ANÁLISIS DEL AUMENTO EN EL HURTO INFORMÁTICO EN EL DEPARTAMENTO DE CÓRDOBA DURANTE LOS AÑOS 2015 Y 2016.

WILLIAM GUILLERMO DEVIA OROZCO CÓDIGO 1.075.218.890
MAURICIO MIGUEL MARTÍNEZ MUÑOZ CÓDIGO 1.067.888.003

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CCAV SAHAGÚN
MARZO 2019

EL AUMENTO EN EL HURTO INFORMÁTICO EN EL DEPARTAMENTO DE CÓRDOBA DURANTE LOS AÑOS 2015 Y 2016.

WILLIAM GUILLERMO DEVIA - CÓDIGO 1.075.218.890
MAURICIO MIGUEL MARTÍNEZ MUÑOZ - CÓDIGO 1.067.888.003

Monografía de Grado
Para optar al título de
Especialista en Seguridad Informática

Director:
Ing. Hernando José Peña Hidalgo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CCAV SAHAGÚN
2019

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Montería, marzo de 2019.

DEDICATORIA

Este proyecto lo dedico a Dios que me ha dado la vida y fortaleza para terminar esta monografía de grado, a mis padres porque gracias a ellos he salido adelante y estoy superándome, poniendo mi dedicación en cuerpo y alma tal y como ellos lo han hecho conmigo, quiero agradecerles por todo el apoyo que me han brindado a lo largo de mi vida, por su paciencia, comprensión y consejos.

A mi esposa, porque gracias a su apoyo incondicional en los momentos más difíciles ha conllevado a que no pierda mi interés en lograr mis objetivos, siendo ella actualmente mi principal apoyo.

De la misma manera lo dedico a los docentes Salomón González, ingeniero Hernando José Peña Hidalgo, ingeniero Luis Fernando Zambrano, porque han sido esas personas que junto con mis padres me han educado para formar a esa persona que fui, que soy y que seré. Agradeciéndoles todo su apoyo, por la orientación que me han dado, por sus consejos que permitieron orientar mí camino**.**

William Guillermo Devia Orozco

DEDICATORIA

Este proyecto lo dedico principalmente a Dios Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos como profesional, además de su infinita bondad y amor.

A mi esposa e hija que han vivido conmigo esas largas noches detrás de un computador y siempre han estado ahí para apoyarme y motivarme a seguir y nunca desfallecer.

A mis padres por los ejemplos de perseverancia y constancia que los han caracterizado y que me han infundado siempre, por el valor mostrado para salir adelante y por su amor.

A los docentes Salomón González, ingeniero Hernando José Peña Hidalgo, ingeniero Luis Fernando Zambrano, por su grandes apoyos y motivaciones para la culminación de nuestros estudios como especialistas y para la elaboración de esta monografía.

Mauricio Miguel Martínez Muñoz

TABLA DE CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

INTRODUCCIÓN

Con ocasión a los avances tecnológicos que desde mediados del siglo XX a la actualidad han traído gran cantidad de beneficios especialmente relacionados con el comercio electrónico entre personas, empresas y/o países; y a su vez el intercambio de información y comunicación a nivel mundial, ha conllevado a que estos avances tecnológicos permitan la aparición de delincuentes informáticos, personas que sin agredir física o verbalmente al ciudadano de bien, afectan su patrimonio económico, y a su vez día tras día perfeccionando su modus operandi, teniendo en cuenta las diferentes actividades de prevención y disuasión que realizan las entidades del estado, con el fin de evitar el aumento de modalidades delictivas, principalmente el delito de hurto por medios informáticos y semejantes tipificado en el artículo 269i de la ley 1273 de enero 05 de 2009 en el departamento de Córdoba.

Teniendo en cuenta el análisis estadístico realizado por el Centro Cibernético Policial DIJIN Policía Nacional, el cual fue desarrollado y basado en la estadística extraída del aplicativo SPOA propiedad de la Fiscalía General de la Nación, se pudo establecer que el departamento de Córdoba es uno de los lugares donde en los últimos años se ha incrementado la denuncia por el delito de hurto por medios informáticos, lo que nos conlleva a establecer las causas, motivos, circunstancias, que conllevaron a que el número de denuncias se aumentaran de una manera desmesurada, hechos entre los que se destaca el cambiazo de tarjeta por medio del cual posteriormente lograr sustraer gran cantidad de dinero de la cuenta de la persona titular de la cuenta bancaria.

Los delitos informáticos surgen con la aparición de todas aquellas operaciones que el ciudadano del común puede realizar para ello utilizando un medio

informático, desde el lugar que desee siempre y cuando cuente con conexión a internet, al igual que la utilización de algún dispositivo tecnológico que soporte la transacción a realizar o de un elemento que permita realizar el pago o compra de algún producto.

En la actualidad la tecnología y el internet han hecho que las personas realicen todo tipo de actividades sin necesidad de salir de su oficina u hogar, es así como se realizan compras de todo tipo de productos, pagos de servicio bancarios y de servicios públicos entre otros, pero esto también con lleva a que las compañías le aporten a sus páginas web la seguridad necesaria para que los usuarios no tengan ningún tipo de problema al momento de realizar estas actividades por medio de sus portales.

La informática y el internet se encuentran presente en casi todos los campos de la vida moderna, Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

Desde el 5 de enero de 2009 en Colombia rige la ley 1273 de la protección y los datos, más conocida como ley de los delitos informáticos, la cual trajo consigo nuevos tipos penales que conllevaron a que el Código Penal se modificara y a su vez legislara normatividad sobre el tema en Colombia, debido a la aparición de nuevas conductas delictivas que no se encontraban tipificadas en la normatividad existente y que conllevaba a que se tipificaran los hechos ocurridos, basados en otra conducta delictiva.

Por todo lo anterior, se desarrolla está investigación la cual busca identificar las modalidades utilizadas por los delincuentes, así como las variables que permitieron el aumento del delito de hurto por medios informáticos en el

departamento de Córdoba durante los años 2015 y 2016, junto con los resultados obtenidos por las autoridades del estado referentes a este delito.

TÍTULO

ANÁLISIS DEL AUMENTO EN EL HURTO INFORMÁTICO EN EL DEPARTAMENTO DE CÓRDOBA DURANTE LOS AÑOS 2015 Y 2016

DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN

Teniendo en cuenta el constante uso de las tecnologías de información y las comunicaciones, la creación del ministerio de las Tecnologías de la Información y las Comunicaciones (TIC), ha traído cambios en la ciudadanía respecto al uso de las tecnologías para la comunicación. No obstante este auge ha conllevado a nuevas modalidades de hurto por parte de los delincuentes en este caso delincuentes informáticos o ciberdelincuentes, quienes con sus diferentes modalidades para atraer a la víctima, robar - extraer información, suplantar páginas web, ha permitido ver la necesidad de implementar medidas de control por parte de los entes del estado con el fin de frenar este desmesurado índice delincuencial, que día tras día aumenta y afecta el bolsillo de las familias colombianas[1] [2].

En el departamento de Córdoba y según la estadística de denuncias instauradas durante los años 2015 y 2016 (ver figura 1) el principal delito denunciado dentro de los consagrados en la ley 1273 de 2009, es el hurto por medios informáticos y semejantes (art. 269i) ya sea por medio de páginas comerciales dedicadas a la venta de productos o a través del cambiazo de tarjetas débito o crédito en los cajeros electrónicos de las diferentes entidades bancarias, modalidad en la cual el delincuente, normalmente dos personas, simulan brindar una ayuda al tarjeta habiente que se encuentra en el cajero y mientras uno le cambia la tarjeta, el otro observa la clave de uso para posteriormente realizar retiros, compras,

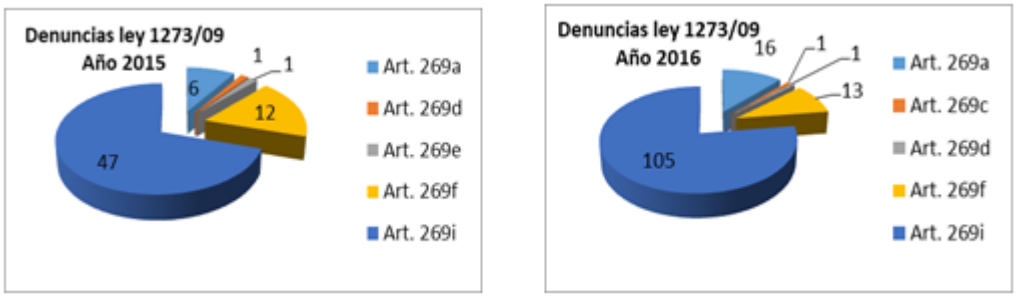
[1] https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

[2] https://www.eltiempo.com/justicia/delitos/denuncias-por-delitos-informaticos-crecieron-en-2017-172294

transacciones, que en su mayoría de casos superan los dos millones de pesos, esto cuando momentos después el cliente se da cuenta, debido a las notificaciones enviadas vía mensajes de texto o correo electrónico por parte de la entidad bancaria con relación a las transacciones efectuadas desde sus cuentas bancarias o tarjetas de crédito.

A pesar que el hurto por medios informáticos sigue incrementando y las victimas en su mayoría de veces son personas de estratos bajos, padeciendo cada una de ellas en su medida graves detrimentos patrimoniales a través de la perdida de sus bienes económicos e información privada a la que acceden de manera ilegal los delincuentes cibernéticos, la cultura de la denuncia ha aumentado, permitiendo así obtener pruebas que permitan cómo mínimo individualizar a los autores de las conductas punibles denunciadas.

Figura 1 Comparativo denuncias año 2015 – 2016 departamento de Córdoba

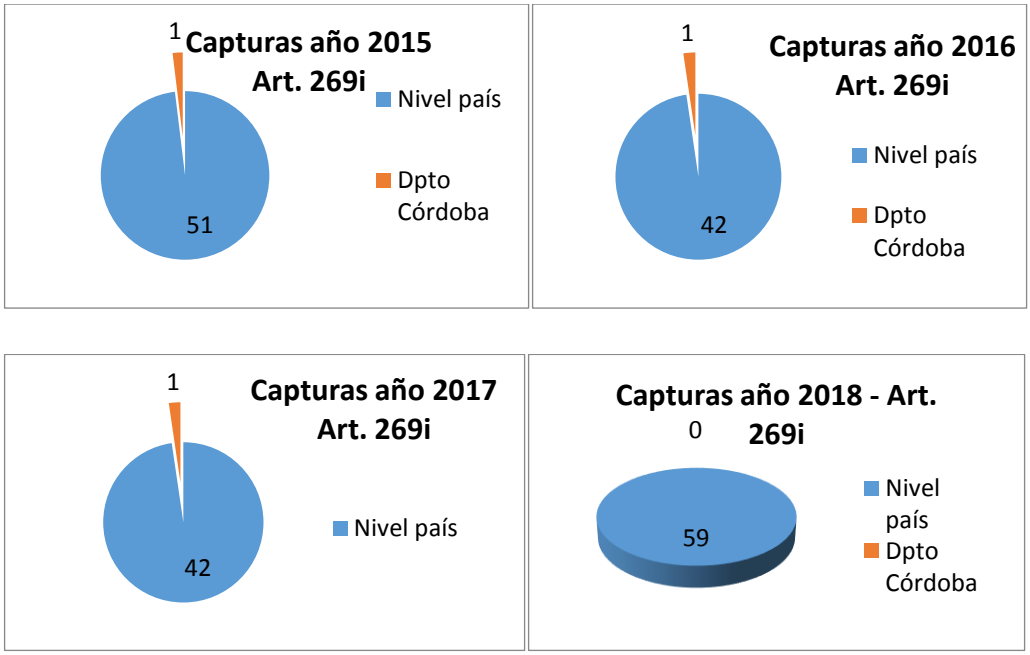


Fuente: El autor, información aportada por Centro Cibernético Policial.

A raíz de lo anteriormente descrito, y mientras el gobierno nacional no realice acciones que conlleven a la reducción del delito, así como mesas de trabajo entre diferentes gremios con lo cual se permita conocer nuevos modus operandi y obtener respuestas oportunas ante solicitudes dentro de procesos penales que se adelanten en esta región del país, las cuales principalmente son radicadas en entidades bancarias, los tiempos de una investigación penal seguirán siendo extensos, lo anterior teniendo en cuenta que mencionadas respuestas son entregadas en los tiempos acordados para el derecho de petición (15 días) y no de una manera ágil y en algunos casos incompleta, lo que conlleva a que la

administración de justicia no pueda recolectar pruebas suficientes que permitan capturar autores de hechos punibles investigados y sea necesario implementar desde los hogares y empresas, medidas preventivas que permitan minimizar riesgos impidiendo así ser víctimas de este flagelo.

Figura 2 Comparativo capturas realizadas años 2015 – 2016 y 2017 – 2018 departamento de Córdoba



Fuente: El autor, información aportada por Centro Cibernético Policial

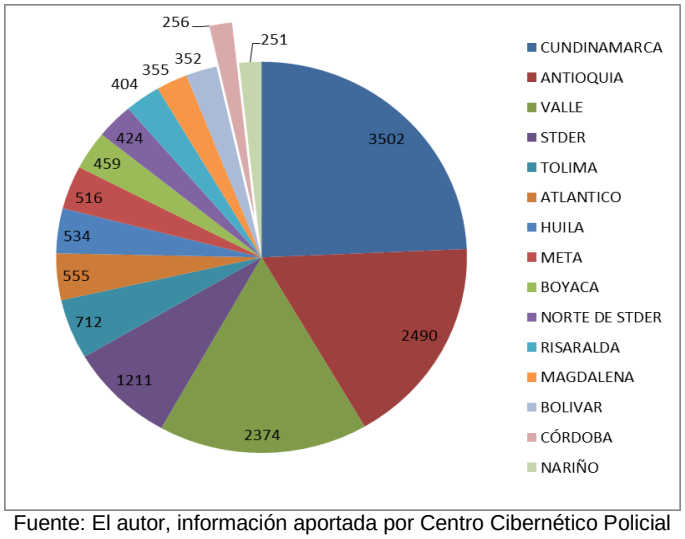
1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo la identificación y análisis de las causas y variables relacionadas con el hurto informático en el departamento de Córdoba durante los años 2015 y 2016, puede ayudar a identificar las causas que conllevaron al aumento de mencionado delito?

JUSTIFICACIÓN

Origina esta investigación la necesidad de identificar las causas por las cuales ha incrementado durante los años 2015 – 2016 el hurto por medios informáticos en el departamento de Córdoba, ubicándolo durante el año 2016 en la posición catorce a nivel nacional de los departamentos donde más se presentaron denuncias por el delito de hurto por medios informáticos, lo anterior según lo informado por parte del Centro Cibernético Policial en la DIJIN de la Policía Nacional, delito el cual sin realizar alguna agresión física, puede afectar más el bolsillo de la comunidad en general, independiente de su estrato, condición social, pues el uso desmesurado de lugares públicos para realizar compras por internet, el pago con tarjeta en diferentes establecimientos comerciales donde se descuida la tarjeta, la asociación de tarjetas de crédito a diferentes aplicaciones de uso celular para pago descontando desde las mismas, entre otras modalidades utilizadas por los delincuentes para obtener información con la cual pueda acceder a portales virtuales bancarios para transferir fondos, conlleva a la necesidad de crear estrategias que permitan frenar el aumento desconsiderado de esta conducta punible.

Figura 3 Comparativo denuncias a nivel nacional año 2015 – 2016



Fuente: El autor, información aportada por Centro Cibernético Policial

Teniendo en cuenta que con el transcurrir de los días, los ciudadanos que realizan desde su lugar de trabajo o vivienda las transacciones bancarias, pago de servicios públicos, compra de elementos de uso masivo, entre otras, se hace necesario realizar un aporte para que el Estado analice la situación que se presenta e implemente medidas que permita combatir las modalidades utilizadas por los delincuentes informáticos y así frenar dicha actividad delictiva, concientizando a la ciudadanía sobre los riesgos a los que están expuestos, permitiéndoles dar a conocer las diferentes modalidades utilizadas, realizando campañas de socialización donde se observe la actividad delincuencial de los ciberdelincuentes, y personas que hayan sido capturadas por participar de conductas delictivas más precisamente hurto por medios informáticos, con lo cual se pueda generar sensación de seguridad a la comunidad del departamento de Córdoba y la comunidad tenga conocimiento sobre actividades que adelantan las autoridades judiciales del estado con el fin de agilizar la investigación de los diferentes casos denunciados de hurto por medios informáticos, por medio de los cuales se pueda identificar las personas dedicadas a la ejecución de estas conductas, y a su vez se puedan judicializar.

La poca actividad preventiva realizada en los diferentes municipios del departamento de Córdoba por parte de las autoridades político administrativas y de Policía, puede conllevar a que muchas personas desconozcan esta nueva modalidad delictiva, por lo cual podría ser pertinente que las acciones preventivas y de disuasión no sean solo en la capital del departamento, si no que sea en toda la jurisdicción.

OBJETIVOS

1.3. OBJETIVOS

Hacer estudio a las diferentes modalidades de ataques utilizados en hurto informático en el departamento de Córdoba, durante los años 2015 y 2016.

1.4. OBJETIVOS ESPECÍFICOS

- Identificar variables que conllevaron al aumento del delito en el departamento.
- Conocer las estrategias implementadas por las autoridades para contrarrestar esta modalidad delictiva.
- Identificar los tipos de hurto informático que existen en el mercado.
- Realizar un estudio sobre el nivel de conocimiento por parte del personal en el departamento, con capacidad para adelantar investigaciones relacionadas con hurto informático.
- Analizar los resultados obtenidos por las autoridades durante la vigencia 2015 – 2016, frente a este delito.
- Identificar el tiempo óptimo o base para identificar el autor de hechos denunciados, de acuerdo a casos propuestos.
- Identificar los recursos tanto físicos como tecnológicos necesarios para contrarrestar delito de hurto informático.

ALCANCE Y DELIMITACIÓN DEL PROYECTO

Identificar las causas que conllevaron a que el hurto por medios informáticos aumentara de manera desmesurada en el departamento de Córdoba, afectando familias de diferentes estratos sociales y empresas privadas, lo anterior teniendo en cuenta el auge que ha tenido el uso de las tecnologías de información y las comunicaciones con las cuales el usuario final realiza sus transacciones vía celular, computador o de manera personal en diferentes establecimientos comerciales, lo que ha permitido que los delincuentes haciendo uso de la buena fe depositada por las personas, se aprovechen y afecten de manera electrónica el bolsillo de los mismos.

Al conocer las conductas delictivas es posible dar a conocer a los habitantes del departamento de Córdoba las modalidades utilizadas por los delincuentes informáticos, por medio de las cuales realizaron hurto por medios informáticos, afectando a un sin número de familias o empresas cordobesas, con el fin de sensibilizarlas frente al riesgo, para que de esta manera tomen conciencia de lo que está ocurriendo y a su vez apliquen medidas de seguridad y precaución al realizar compras o pagos electrónicos en diferentes establecimientos comerciales, presenciales, o a través de internet.

Analizar los horarios utilizados por los delincuentes para cometer esta conducta delictiva, por medio de la cual se puedan generar estrategias para que las autoridades mitiguen el impacto de este delito.

Identificar la población más afectada con esta conducta delictiva, cuyo fin permita sensibilizar al ciudadano para que implemente actividades que conlleven a la protección de su economía.

Establecer las frecuencias horarias en las cuales actúan los delincuentes, misma forma la población que puede verse afectada con esta modalidad delictiva.

MARCO DE REFERENCIA

1.5. ESTADO ACTUAL

El delito en la cibersociedad y la justicia penal internacional.

AUTOR Jarvey Rincón Ríos

FICHA BIBLIOGRÁFICA RINCON RIOS, Jarvey. El delito en la cibersociedad y la justicia penal internacional. Madrid, 2015, 504 p. Tesis doctoral (Derecho). Universidad Complutense de Madrid, facultad de derecho.

PALABRAS CLAVE Fraude, sabotaje, informático, penales, leyes, tecnológico, delito.

PALABRAS DESCONOCIDAS Ubicuo, supraterritoriales, panóptico, adeptos, ascetismo, hedonismo, puritana, mass.

FUENTES 72

CONTENIDO DEL RAE En el documento manifiesta el autor que antiguamente existían muchos controles cuyo fin era evitar la comisión de delitos por parte de cada uno de los ciudadanos, controles que no excedían de actividades normales en el contorno de las ciudades y grandes capitales. Manifiesta que con la transformación del capitalismo en donde el uso dado a la tecnología, guerra y ciencia, conllevó a que el uso de las ideas fuera más importante que el del trabajo. El hombre ya no vive en esa cultura de historias, el hombre ya vive en ese presente y sueña con ese futuro, virtualizado, en el que pueda estar al mismo tiempo en varios lugares, comprar en la distancia, negociar, vender, y realizar contratos en el cibermercado. El hacker y los virus, pasaron a ser los problemas de hoy en día, uno por estar generando problemas en el ciberespacio y el último por ser la enfermedad informática. La historia anterior era llena de controles, la

actual también pero no son lo suficientes para una sociedad que día a día está consumida por el ciberespacio y que por su velocidad, conlleva a que los controles deban ser más estrictos, sin hasta el momento ser efectivos, por lo que ha conllevado a que los diferentes estamentos internacionales, encargados de legislar en cada país y de crear normas internacionales, convenios de trabajo, pactos judiciales, se han visto en la necesidad de implementar medidas que permitan contrarrestar el auge que ha tenido la sociedad, hoy en día consumida por el ciberespacio, para que así como en tierra se controla, virtualmente también se realice. Aduce que para la década de los 50 cuando empezó la introducción de la primera computadora, hoy en día ordenador, y más precisamente para la década de los 60 cuando en Estados Unidos y Alemania salieron a la luz los primeros casos de espionaje, manipulaciones de ordenadores, sasos de saboteo fecha en la cual dichos casos eran tratados como criminalidad y no como casos penales; para la década de los 70 empezaron algunos estudios empíricos de delitos informáticos donde se estudiaron aplicando métodos científicos de investigación criminológica, casos que se encontraban relacionados a la comisión de actos por medio de sistemas informáticos o de su aprovechamiento por lo que con el trascurrir de los días, encontraban otros casos que no habían salido a la luz pública y en los cuales se habían desviado más de mil millones de pesos, principalmente de dineros existentes en cuentas bancarias y que conllevaron a que una de estas entidades bancarias, cerrara sus puertas. Da a conocer que para las décadas de los años 80, y teniendo en cuenta que la prensa y principales medios de comunicación se enteraron de casos relacionados con piratería informática, manipulaciones a cajeros electrónicos para obtención de dinero, virus, y manipulaciones en sistemas de telecomunicación, lo cual dieron a conocer y conllevó a que surgiera la necesidad de implementar estrategias que permitieran el control, prevención y sanción de dicha actividad. En 1983 empezaron a surgir algunos conceptos relacionados con delitos informáticos al igual que en 1990, pero dichos conceptos o estudios no pasaban más allá de la criminalidad informática. A nivel mundial con el transcurrir de los años seguían analizando los

casos presentados, a tal punto que en 1984 en Francia luego de analizar los diferentes y pocos casos presentados, llegaron a la conclusión que los casos presentados en ese país, superaban un 10% el valor de los asaltos tradicionales presentados y que la cifra cada día aumentaría. De esta manera empieza a tomar fuerza el concepto de delito informático no solo por los casos presentados y analizados, sino por que surgió la necesidad de implementar nuevos tipos penales en la normatividad para cada país que pudiera sancionar dichos delitos, y a su vez reorganizar la política de estado dentro de la cual se puedan incluir las estrategias a realizar por parte de las entidades del estado, para contrarrestarlo. De esta manera diferentes abogados empezaron a dar conceptos de lo que es delito informático y empezaron a dar enfoque a lo que se hacía necesario implementar en cada nación y que se trabajara de manera conjunta a nivel mundial, por lo que se realizaron avances significativos en normatividad penal para quienes atenten contra los datos y las telecomunicaciones en la Unión Europea, siendo Alemania y Francia quienes han logrado mejores y mayores resultados con la creación en Alemania el 15 de mayo de 1986 de la segunda ley contra la criminalidad informática, Francia lo hizo el 05 de enero de 1988 con la creación de la ley 88/19 que trata sobre fraude informático; Estados Unidos no se quedó atrás y en 1984 empezó a regular a través de diferentes actos y leyes en las cuales se destaca Acta federal contra el abuso computacional (1994) y Economic Espionaje (1996), misma forma ocurrió en Canadá (1982) y las más reciente 2003. España no pudo quedarse atrás y en su código penal, clasificó los delitos informáticos en cuatro grandes grupos que abarcan delincuencia para ataques informáticos, robo de información, conductas y atentar contra los derechos privados de los procesos de innovación. Prácticamente 23 años después de que en Alemania se sancionara la primera ley que castiga los delitos informáticos, en Colombia se sancionó la ley 1273 de 2009 que es la que actualmente castiga las conductas relacionadas con delitos informáticos., así como las más recientes en Brasil Ley Nº 7.646, de 18 de diciembre de 1987, Argentina Ley 26388 de octubre 10 de 2016, Bolivia Decreto

Supremo No. 27329 del 31 de enero de 2004 y Chile Ley 19799 de Firma Electrónica del 12 de abril de 2002.

CONCLUSIONES A modo de conclusión frente a la posición de los Tribunales españoles, que no se resisten a darle fuerza vinculante a los preceptos contenidos en tratados internacionales asumidos por el Estado Español, y que en la búsqueda inocua de mantener la soberanía desde la administración de justicia no renuncian a ninguna de sus potestades estatales, Núñez se ha manifestado, estableciendo que: “Parece claro, a la vista de lo anterior, que los tribunales españoles se resisten a aceptar que están obligados por las decisiones de los órganos convencionales creados por Tratados internacionales sobre Derechos Humanos de carácter universal, de los que España es Parte. Órganos cuya competencia para aceptar y examinar denuncias individuales respecto a España el Estado español ha aceptado expresamente. A pesar de ello, la jurisprudencia de estos órganos encargados de la supervisión y el control de los Tratados universales de promoción y protección de los Derechos Humanos acaba, más tarde que pronto, teniendo su incidencia tanto en las sentencias dictadas por los tribunales españoles como en la legislación interna que regula el sistema judicial. No obstante, la interpretación que se sigue realizando por parte de la jurisprudencia española, tanto de las decisiones emanadas de los órganos convencionales encargados de la supervisión de los derechos contenidos en los Tratados por los que se crean, como de los mismos derechos contenidos en estos Tratados, se aleja aún de lo deseable desde el punto de vista del Derecho internacional de los Derechos Humanos. Ello es así porque a las primeras les otorga nuestra jurisprudencia una mera «naturaleza política» y a los segundos, a los derechos, sólo les reconoce valor en España en tanto los Derechos fundamentales reconocidos en la Constitución Española han de interpretarse a la luz de aquéllos, según dispone el artículo 10.2. Pero quizá lo más sorprendente no es la peculiar interpretación del Derecho Internacional público que pueden realizar los jueces y

tribunales españoles, obviando a veces la obligatoriedad de aquello a lo que un Estado ha prestado formal y, por supuesto, voluntariamente, su consentimiento en obligarse, requiriendo para ello, en estos casos, la previa autorización de las Cortes Generales en virtud de lo dispuesto en el artículo 94.1 de la Constitución Española. Sino que, además, las resoluciones judiciales españolas han llegado hasta a negarle a estos órganos convencionales de protección de los derechos humanos la facultad de interpretar las disposiciones de aquellos Tratados por los que fueron creados. (NÚÑEZ, P.T., 2009:280)

AUTOR DEL RAE 233006_2

Delincuencia informática: daños informáticos del artículo 264 del código penal y propuesta de reforma.

AUTOR Jorge Alexandre González Hurtado

FICHA BIBLIOGRÁFICA GONZÁLEZ HURTADO, Jorge. Delincuencia Informática: daños informáticos del artículo 264 del código penal y propuesta de reforma. Madrid, 2013, 408 p. Tesis doctoral (Derecho). Universidad Complutense de Madrid, facultad de derecho.

PALABRAS CLAVE Tecnológicos, normatividad, legales, fraude, Unión Europea,

PALABRAS DESCONOCIDAS Hándicaps, taxatividad, incardinada, polisémica.

FUENTES 314

CONTENIDO DEL RAE Con la aparición notoria en la década de los 80 de la evolución informática, también aparecieron algunas conductas ilícita que tal como crecía el uso de estos medios tecnológicos, estas aumentaban consideradamente; es así que con el papel fundamental que han ocupado tanto en la vida de las

personas como en la de la empresas, los estados han empezado a crear diferentes normatividades legales que permitan regular el accionar delictivo de cada una de estas conductas ligándolas a una nueva rama del derecho. la aparición de estas tecnologías, también ha sido sumamente importante para las empresas quienes a pesar de la poca normatividad existente y la gran variedad de riesgos ya conocidos, la utilizan, siendo conocedores que a pesar de la normatividad existente para regirla y castigarla, parece con el pasar de los días no ser suficiente y siempre quedando atrás frente a las nuevas conductas que surgen para la comisión de esta modalidad de delito informático, conllevando a que la normatividad siempre estuviera incompleta frente a este delito. Con ocasión al a trascendencia que ha tomado el daño informático en la vida diaria de las personas y ejercicio de las empresas, el autor decide hacer un análisis sobre la regulación de este delito consagrado en el artículo 264 del Código Penal Español. A pesar que mencionado artículo fuera modificado el pasado 22 de junio de 2010, no dejaran de ser importantes y es por eso que con el pasar de los años, pasarán a un plano más importante por la regularidad con que se presentarán por el tema que existirá para hablar con ocasión a las conductas ilícitas que se ejecutarán, y con la flexibilidad y poco conocimiento que existe en los tribunales, muy pocas serán castigadas. El análisis que quiere realizar el autor dará a conocer que la normatividad existente en el artículo 264 del Código Penal Español, regula las modalidades de delitos informáticos que con menos frecuencia se ejecutan en esa nación por lo que la mayoría de casos no podrán ser castigados bajo esa norma jurídica. Gracias al convenio sobre ciberdelincuencia creado en Budapest el pasado 23 de noviembre de 2001, consolidado como la mejor herramienta para la lucha contra la delincuencia informática junto con la decisión 2005/222/JAI del consejo de la unión europea de fecha 24 de febrero y son las que han motivado para que en España, exista preocupación sobre normatividad que regule las diferentes conductas de delitos informáticos que se presenten. Con su análisis el autor pretende dar a conocer a los ciudadanos las modalidades existentes de delitos informáticos que son reguladas y castigadas mediante el código penal

español, enfocándose precisamente en el daño informático, tipificado en el artículo 264 de dicha Ley; al igual que hacer un contraste de los problemas que se presentan en la aplicación de dicha Ley por parte de los operadores de derecho, fuerzas de la ley y cuerpos de seguridad que hacen parte del estado con las soluciones que puedan tratar de buscar para mitigar el impacto de las conductas delictivas, que se buscan castigar. De esta manera el autor señala que con la aparición del internet, el ciberespacio, a pesar de ser una herramienta fundamental se han convertido en el origen de un montón de situaciones que no solo deben ser tratadas con la normatividad penal, sino también bajo la administrativa, civil, y las demás existentes, pues de una u otra manera están afectando e incumpliendo lo estipulado en ellas. Con ocasión a la introducción de la normatividad que regula los delitos informáticos, en este caso el daño informático, ocurrida en 1995, surgió una prueba para el legislador en el sentido de tipificar de una manera excelente la conducta cometida para que pueda ser encajada en alguna de las modalidades que para ese entonces existía en el Código Penal Español, por lo que el artículo que regula dicha conducta delictiva tuviese qué ser modificado y también gracias al convenio sobre ciberdelincuencia firmado en Budapest en 2001. Antes de la existencia del Código Penal de 1995, no existe antecedente alguno que pueda demostrar cómo se solucionaban las conductas delictivas relacionadas con delitos informáticos, por lo que se presume que se haría por la vida civil. Así mismo a pesar de la existencia de normatividad en otros países de Europa frente al cibercrimen o modalidades de delitos informáticos, las cuales en los años 1986, 1989, 1990 y 1994 fueron dadas a conocer al legislador Español al igual que las modalidades existentes y con antecedente de ejecución en diferentes países, el legislador español solo las tuvo en cuenta para el año 1995 y de una manera incompleta, pues es así como se evidenció al ser incorporadas en el Código penal Español, una década después de haberse hecho en otros países. Es por eso que en el análisis que el autor realizará de la reforma realizada al Código Penal Español en el 2010, dará a conocer los aspectos modificados, los no modificados y los incorporados. Con la reforma realizada al Código Penal Español mediante

LO 5/2010 de 22 de junio, se añadieron nuevas conductas punibles entre esas las relacionadas con punibles de delitos informáticos al igual que de otros preceptos generales para el Código. Es así que para que exista un código penal cargado de diferentes preceptos jurídicos y que sean de efectiva ejecución en territorio español, es necesario realizar un buen anteproyecto de ley (planeación) para que de esta manera y teniendo en cuenta los casos presentados y de los cuales tanto personas como entidades jurídicas y/o del estado se vieron afectadas, puedan tipificarse las conductas que se presentan actualmente, siendo necesaria la presencia de todos los congresistas en los diferentes debates, para que fuera debatido en el congreso y posterior sancionado.

CONCLUSIONES No cabe duda de que en la actualidad tanto las instituciones, sean públicas o privadas, como los particulares, y toda clase de asociaciones, tomen la forma que sea, se ven abocados irremediablemente a la utilización de equipos informáticos y sistemas de información. Es simplemente inevitable. Parece difícil volver a una situación anterior tal y como se ha ido produciendo la evolución de la sociedad. Nos guste o no, este es el camino que se ha decidido seguir. Sin embargo, la introducción en la sociedad de nuevas herramientas pensadas para hacer a las personas la vida más 356 cómodas, supone que puedan ser utilizadas con fines totalmente opuestos para las que fueron creadas, atentas a los cuales deben estar siempre los poderes públicos, tanto en el ámbito nacional como internacional. La conclusión final que se extrae de la elaboración de este trabajo de investigación es la de que se han puesto en funcionamiento las herramientas legales (e incluso policiales) oportunas para proteger a la sociedad de un nuevo tipo de delincuencia, tanto en el concierto internacional, lo cual es esencial, como en nuestro ordenamiento interno. Sin embargo, la regulación que se ha realizado en España respecto a los delitos de daños informáticos, aunque puede resultar suficiente en el momento actual y es acorde a la mayor parte del precepto internacional y semejante a la de los países de nuestro entorno, puede

ser reformulada desde nuevos principios integradores. Las construcciones literales de los tipos arrojan algunas dudas de interpretación, y en la jurisprudencia actual no encontramos respuesta por la escasez de casos planteados ante los Tribunales, pues la existencia de esta clase de delitos que llegan a ser conocidos es todavía escasa. El éxito que supone haber sido conscientes de la nueva problemática aparecida con el desarrollo de las nuevas tecnologías, no debe empañarse por una regulación farragosa, y de difícil interpretación. Si bien se ha comenzado a recorrer el camino para proteger a la sociedad de nuevos tipos de delincuencia, es necesario hacerlo con la máxima efectividad. Por ello, desde el reconocimiento que debemos profesar por la puesta en marcha de medidas concretas tanto en el ámbito nacional como internacional, debe exhortarse a mantener el esfuerzo actual en completar de la mejor forma nuestro ordenamiento jurídico en relación con las nuevas tecnologías, especialmente en el ámbito penal.

AUTOR DEL RAE 233006_2

Daños informáticos contra sistemas: el artículo 264 bis del código penal.

AUTOR Alberto Rodríguez Fernández

FICHA BIBLIOGRÁFICA RODRÍGUEZ FERNÁNDEZ, Alberto. Daños informáticos contra sistemas: el artículo 264 bis del código penal. {En línea}. Fecha de consulta 25 de mayo de 2017. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Rodriguez%20Fernandez,%20Alberto.pdf?idFile=bd78e587-740d-4e30-abe4-ec7d2e0755dd

PALABRAS CLAVE Ciberdelincuencia, ataques, sistemas, seguridad, directiva, Unión Europea, parlamento, Budapest.

PALABRAS DESCONOCIDAS Incipientes.

FUENTES

CONTENIDO DEL RAE Con la introducción del articulo 264bis por medio de la LO 1/2015 del 30 de junio (Ley Orgánica) se dio vida nuevas conductas delictivas asociadas a delitos informáticos y mediante las cuales el gobierno español empezó a hacerle seguimiento y castigar más drasti8camente las modalidades utilizadas por los delincuentes informáticos para hacer sus actividades delincuenciales en donde se vieran afectados ciudadanos españoles, empresas estatales u otro tipo de personas que para ese momento se encontraran en territorio español; lo anterior teniendo en cuenta que el articulo 264 existente en el Código Penal Español no fue realizado de la manera que se esperaba y con la tipicidad necesaria para cada una de las modalidades ya conocidas para la fecha de su creación, por lo que debido a la directiva 2013/40/UE del 12 de agosto del Parlamento y del Consejo relativa a los ataques contra los sistemas de información, y de la Convención sobre Ciberdelincuencia de Budapest, el gobierno español debió nuevamente crear tipos penales para incluir las diferentes modalidades delictivas ya conocidas con las cuales se pudiera castigar toda clase de comportamiento delictivo que no estuviera tipificado en dicho código. Esta reforma afectó de forma importante la normatividad existente en materia de castigar los delitos informáticos ya que introdujo un nuevo artículo, el 264bis. Uno de los motivos que conllevó a añadir mencionado artículo al Código Penal Español, fue la incorporación al ordenamiento jurídico de la Directiva 2013/40/UE del 12 de agosto del Parlamento y del Consejo ya que esta era relativa a los ataques contra los sistemas de información. Mediante esta norma se sustituye la Decisión Marco 2005/222/JAI del consejo con fecha 24 de febrero de 2005, Directiva que hace alusión a las normas mínimas que deben tener todos los estados con relación a las conductas punibles y sanciones a las mismas siempre y cuando se encuentren enmarcadas como delito informático o que sirvan para hacer frente a los ataques informáticos de los cuales algunos de los países que hacen parte de la Unión Europea han venido siendo víctimas y a su vez con el fin

de que sirva como vínculo laboral frente a casos relacionados con alguna de las modalidades existentes en el código penal español y tipificada como delito informático, teniendo en cuenta el auge que está presentando la cibercriminalidad. Es por eso que pese al esfuerzo realizado por las autoridades españolas como europeas por medio del cual permitieron definir nuevos delitos que permitieran acomodarse a la tipicidad de cada una de las modalidades que con la historia se han presentado para de esta manera perseguir de manera grupal y mancomunadamente los delincuentes informáticos, más sin embargo en pleno siglo 21 y donde el auge del comercio electrónico se encuentra en su furor, donde los ciudadanos hacen todo por medios tecnológicos, no se pueden cruzar los brazos sino por el contrario seguir implementando actividades, estrategias y porque no, implementar nuevas conductas delictivas en la normatividad legal, por medio de la cual se puedan castigar la ejecución de conductas delictivas que puedan tener relación con lo estipulado en el Código Penal español pero que por su forma de ejecución no pueda tipificarse como delito, basados en la actualización constante de las normas mínimas que debe tener un estado (Unión Europea) para salvaguardar los diferentes sistemas de información de cada una de las organizaciones, familias, instituciones educativas, entre otras, garantizar su nivel de protección, pues es por medio de estos que se puede dar una respuesta acertada y a tiempo a los diferentes requerimientos existentes en las diferentes empresas. En la actualidad los ataques ya dejaron de ser a un solo computador, por el contrario, ya se hacen a gran escala y principalmente buscan afectar organismos del estado, con el fin de burlar la seguridad que tengan implementada, lo anterior teniendo en cuenta que día a día se crean nuevas modalidades delictivas en las que no pueden permitir verse afectados. La Directiva 2013/40/UE del 12 de agosto del Parlamento y del Consejo no solo insta la creación de normas mínimas para garantizar la seguridad a los sistemas de información y castigar aquellos que no cumplan con la normatividad existente, también contempla implementar sanciones y multas de acuerdo al daño causado, a la conducta ejercida y a la modalidad utilizada; todo con el fin de cumplir con la finalidad

primordial del convenio de Budapest y ratificado por España el pasado 17 de junio de 2010 mediante publicación en el BOE, donde se establecieron 4 puntos que la normatividad de cada nación debe tener y enfocar hacia su cumplimiento con el fin de que todas las naciones integrantes de la Unión Europea tengan armonizados los delitos y sanciones. De esta manera a pesar que no es menester del autor, no queda duda de que para la realización de proyectos de ley que conlleven a la incorporación, modificación o eliminación de conductas penales descritas en el Código penal español, es necesario realizar con mucho tiempo atrás un anteproyecto del que deben participar diferentes entes de la nación, con el fin de exponer los diferentes puntos de vista que sirvan para enfocar los nuevos delitos que se pretenden incorporar a la normatividad, o modificar aquellos existentes, evitando de esta manera que los delincuentes informáticos tengan facilidad para no ser culpados de conductas realizadas principalmente aquellas realizadas bajo la voluntad del propietario o tenedor pero que no se encuentren tipificadas en la normatividad de la nación o en los acuerdos de la Unión Europea.

AUTOR DEL RAE 233006_2

La problemática jurídica en la regulación de los delitos informáticos

AUTOR Alejandro Armando Montaño Álvarez

FICHA BIBLIOGRÁFICA MONTAÑO ÁLVAREZ, Alejandro. La problemática jurídica en la regulación de los delitos informáticos. Ciudad Universitaria, 2013, 381 p. Tesis profesional (Licenciado en derecho). Universidad Nacional Autónoma de México, facultad de derecho.

PALABRAS CLAVE Seguridad, crimen, delincuencia, informático, fraude, extorsión, daño informático.

PALABRAS DESCONOCIDAS GONZÁLEZ HURTADO, Jorge. Delincuencia Informática: daños informáticos del artículo 264 del código penal y propuesta de reforma. Madrid, 2013, 408 p. Tesis doctoral (Derecho). Universidad Complutense de Madrid, facultad de derecho.

FUENTES 109

CONTENIDO DEL RAE Teniendo en cuenta la existencia de múltiples carteles delincuenciales aquellos que obtienen ganancias a través de actividades ilícitas, perseguidas por las autoridades estatales y sus diferentes fuerzas, más precisamente en jurisdicción de Sinaloa, donde la delincuencia ya es organizada conllevando al lavado constante de dinero, lo que conllevó a que las entidades estatales con el fin de frenar dichas actividades, crearan grupos de trabajo mancomunado con diferentes entidades estatales para combatirlos y que sean sometidos bajo la normatividad penal que se rige en dicho estado Mexicano; pero así como se han creado grupos de trabajo para contrarrestar el crimen organizado, fue necesario modificar la normatividad existente, de tal manera que las diferentes conductas realizadas por dichos criminales pudieran tipificarse sin problema alguno, en alguna de las modalidades delictivas existentes en la ley penal del país. Sin duda alguna, los dineros que reciben dichos carteles o grupos delincuenciales organizados provienen de extorsiones, narcotráfico, acciones que no solo afectan el estado, sino el medio ambiente y el ciudadano. Teniendo en cuenta que el trabajo mancomunado sirvió para mitigar de buena forma dicha actividad delictiva; y que con la implementación de tecnologías para frenar la extorsión por medios telefónicos, el uso de internet, y demás herramientas, surgió la necesidad de incorporar a la normatividad legal del país, nuevos modalidades delictivas asociadas a los delitos informáticos, con las cuales no solo controlarían los fraudes informáticos, sino que también podrían generar sistemas de seguridad para proteger la información en los sistemas de información estatales, de empresas privadas, de ciudadanos del común y de todo aquel que hiciera uso del internet, ya que con el auge que tiene es posible que el crimen organizado inicie

acciones delincuenciales informáticas, por medio de las cuales puedan realizar fraudes financieros, extorsiones, amenazas y otras modalidades que día a día fueron surgiendo pero que no eran tipificadas como delito o conducta ilícita. No solo fue necesario incorporar en la normatividad legal un tipo penal que castigara y sancionara a quien incurriera en alguna de las modalidades allí escritas, sino que fue necesario que el legislador se capacitara para que de esta manera tuviera la capacidad de tipificar de una manera adecuada las conductas que estas bandas delincuenciales organizadas pudieran realizar y que no se presentaran situaciones adversas por desconocimiento de la normatividad existente. Por tal razón la regulación de los delitos informáticos surge como necesidad imperiosa de todo estado, pues para nadie es un secreto que muchas familias realizad a diario sus actividades comerciales, financieras, educativas, utilizando internet, lo cual implica un riesgo al realizarla, ya que existe de por medio información, que aparte al dinero depositado en cada una de las cuentas bancarias, también es muy valioso principalmente para aquellas organizaciones que protegen información confidencial o de seguridad para el estado, instituciones educativas, pues con ella en manos ajenas es muy probable la ocurrencia de actividades delincuenciales ya que estos grupos ilegales están utilizando equipos de cómputo con el fin de cometer conductas punibles tipificadas como delitos informáticos, y que les sirven para obtener dinero a través de actividades ilícitas. Es indispensable que el legislador tenga conocimiento de casos delincuenciales vinculados a delitos informáticos que hayan ocurrido en otras naciones, para que sirvan de guía ante casos presentados en la nación y puedan determinar o permitir identificar bandas delincuenciales que estén utilizando la misma modalidad delictiva para cometer actos delincuenciales en la nación. De igual forma es indispensable para el legislador y su equipo de trabajo, orientar la normatividad y enfocarla sobre la normatividad de los países vecinos, para de esta manera no permitir que con el fin de evadir la justica salgan de países que tienen tipificada la conducta como delito para poder ejercer la conducta criminal en países vecinos que no la tipifiquen; es por eso que para la Organización de las naciones Unidad por sus siglas ONU, es

importante regular algunas conductas y darlas a conocer al mundo para su prevención; el grupo G8 (ocho países más industrializados en el mundo)quienes luego de una reunión efectuada en Washington dieron a conocer que en sus principales temas a tratar esta combatir el cibercrimen por medio de las respectivas investigaciones de hechos ocurridos; la comisión de las comunidades europeas quienes firmaron el convenio de Budapest el pasado 23 de noviembre de 2001 y mediante el cual se unificó una política penal para prevenir la criminalidad en el ciberespacio, así como la de prevenir a los aliados sobre el riesgo existente en las redes informáticas y que trabajando de la mano ante estas conductas delictivas puede garantizar la confiabilidad, integridad y disponibilidad de la información existentes en las diferentes bases de datos existentes. Actualmente existen diferentes entes que persiguen delincuentes o trabajan asociadamente para facilitar la cooperación en la investigación de conductas delictivas a nivel mundial, es el ejemplo de la Organización Internacional de Policía, por sus siglas INTERPOL, donde su misión más importante es prevenir o combatir el crimen trasnacional; Oficina Europea de Policía por sus siglas EUROPOL, creada mediante tratado de Maastricht en la Unión Europea el pasado 7 de febrero de 1992 en la Haya, cuya misión es ayudar en la aplicación de la ley de los estados miembros, en el caso de los delitos informáticos, apoya siempre y cuando se trate de estructuras criminales y que sean dos o más naciones las que se encuentren comprometidas y que sean miembros. La división del Departamento de Justicia de los Estados Unidos, Federal Bureau of Investigation por sus siglas FBI, una de las más poderosas e influyentes organizaciones en el mundo, encargada de investigar y suministrar información de diferentes casos que se investiguen, también vela por la seguridad interna del país.

CONCLUSIONES La historia de la Informática se remonta a los años 50s existiendo previamente a ello diversos aparatos que de manera rudimentaria facilitaba las labores del ser humano tales como las calculadoras, la llamada “máquina diferencial”, instrumentos para realizar operaciones a través de tarjetas

perforadas, inclusive hasta llegar al rudimentario ábaco, llegando así hasta las computadoras que han sufrido múltiples modificaciones a través de las denominadas “Generaciones”, en las cuales han reflejado su avance y evolución que han ido teniendo durante cada 5 o 10 años, sin embargo, en la actualidad esos avances aparecen por cada año, inclusive mensualmente, ya que una computadora adquirida en una fecha, al mes siguiente es mejorada. Dicho avance ha implicado también una evolución cotidiana en el número de componentes de las computadoras recibiendo sus correspondientes denominaciones, situaciones que deben ser conocidas por los legisladores tanto para su debida regulación, así como para considerarlas al pretender formare algún tipo penal, ya que existen códigos punitivos en donde se incluyen tales conceptos como lo es el del Estado de Aguascalientes en donde prevé que la transgresión puede efectuarse a un programa de computación o software. La Cibernética difiere a la Informática en que la primera trata de explicar y dar solución a eventos de control y comunicación ya sea de fenómenos acontecidos en la naturaleza, en la sociedad o producto de los hombres, mientras que la Informática pretende desarrollar máquinas capaces para que la Cibernética cumpla con sus objetivos pretendiendo desarrollar lo que se ha conocido como “Inteligencia Artificial”, reflejando un beneficio en las Ciencias Naturales, Sociales, así como en las diversas técnicas y en sí en todas las actividades del ser humano. Las nuevas tecnologías en un mundo globalizado, siempre presentarán nuevos y dinámicos beneficios en cada aspecto de la vida humana pero también implica que nuevas formas delictivas surjan en días, que sin una legislación que prevea o al día en cuestión de estos aspectos, causarán que los nuevos problemas con nuevas tecnologías sean más difíciles de combatir, La Internet ha venido a evolucionar la historia del hombre como lo fue el descubrimiento de la penicilina para la medicina, dándose su aplicación en actividades tales como en la comunicación, en la mensajería, en la información, entre otras más, convirtiéndose este sistema en una herramienta en beneficio del hombre y en cada uno de sus aspectos que lo rodean, pero siempre existirá el lado negativo que es resultado del crecimiento global, la facilidad que lleva su uso,

y las malas intenciones de la personas, en el que una regulación global será un trabajo arduo ya que un país por sí solo no podrá combatir, pero el primer paso para prevenir los delitos informáticos proviene de la educación y conocimientos de los usuarios. La influencia de la Informática en el Derecho ha originado la existencia del denominado Derecho Informático enfocado a la protección de datos informáticos o la información concentrada en medios magnéticos o digitales, teniendo una gran relación con el Derecho a la Información, en el que se pretende regular el acceso a la libre información; siendo el Derecho Informático definido por Julio Téllez Valdez como “una rama de las ciencias jurídicas que consideran a la Informática como instrumento y objeto de estudio”; siendo el análisis de ambas de suma importancia para la regulación de los Delitos Informáticos. Así, la Informática ha servido para facilitar sus variados campos de aplicación de las diversas ramas del Derecho, como sería la Civil, Mercantil, Administrativa, Laboral, Penal, entre otras, por lo que con ello el legislador adquiere una gran responsabilidad para la creación de normas jurídicas en cada uno de esos campos. Al respecto, existe una gran cantidad de operaciones jurídicas que se realizan a través de la Informática, así como facilitar el manejo de bibliografías jurídicas, criterios jurisprudenciales, entre otros productos jurídicos más se han concentrado en discos compactos o inclusive en pequeñas tarjetas de memoria conocidas como “USB”, así como facilitar su consulta a través de la Internet. Se ha dado la existencia de proyectos para la creación de las llamadas “Ciberjusticia y de los “Cibertribunales”, los cuales serían temas importantes para ser tratados en investigaciones por separado, ya que se pudiera “deshumanizar” al Derecho y se le restaría la labor loable a aquellas personas que de alguna manera tienen la tarea de aplicar la ley a los casos concretos, debiéndose reflexionar aún más sobre estos puntos, sobre todo al considerar el origen romano-germánico del Derecho Mexicano, a diferencia de las propuestas hechas en países cuyo Derecho deriva del sistema anglosajón. Dentro del Derecho Informático encontramos la preocupación de la protección jurídica de datos contenidos en los sistemas informáticos, así como de sus sistemas computacionales por lo que han surgido diversos intentos legislativos

para tal efecto, incluyéndose la creación de tipos penales acerca de sus conductas antisociales. De acuerdo a la protección de diversos bienes jurídicos en la regulación jurídica de los delitos informáticos se han encontrado otras leyes con las que pudieran existir algunas contradicciones para su adecuada aplicabilidad; tal es el caso de la protección de los programas de computación (ejemplo el Estado de Sinaloa) , que también son protegidos por el propio Código Penal Federal con los delitos acerca de los derechos de autor, toda vez que son protegidos como obras por la Ley Federal del Derecho de Autor; así como cuando se refiere a la protección de la información contenida en medios informáticos, ya que ésta también se encuentra regulada por la Ley de Propiedad Industrial. La Ley Federal de Transparencia y Acceso a la información Pública Gubernamental también pretende proteger a la información que poseen los Poderes de la Unión, por lo que será considerado una infracción administrativa cuando un servidor público quien la 357 transgreda conforme a las hipótesis señaladas en esa Ley entre las que encontramos usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar total o parcialmente y de manera indebida información que se encuentre bajo su custodia, entre otras conductas más. Sin embargo, la aplicación de esta legislación es independiente de los ordenamientos penales. En México se ha tenido la preocupación de legislar acerca de los Delitos Informáticos tanto a nivel federal como local ya que encontramos entidades federativas tales como la de Sinaloa y de Veracruz en donde se contemplas tipos penales en donde se pretende proteger la información contenida en los medios informáticos, existiendo además Estados como Aguascalientes (que hace referencia a la violación de programas de software o base de datos, así como de programas informáticos), Colima, Chiapas, Estado de México, Durango, Distrito Federal (con las reservas de ser una entidad federativa), Guerrero, Nuevo León, Quinta Roo, Tamaulipas, Morelos, Yucatán, Zacatecas, Tabasco, Jalisco y Baja California que han incluido en sus legislaciones diversas figuras delictivas que pueden ser cometidas a través de los sistemas computacionales, encontrando así ilícitos como el robo, fraude, falsificación de documentos, corrupción de menores, pornografía infantil, en contra

de las vías de comunicación, secuestro, revelación de secretos, contra la moral pública y ambientales. Las legislaciones penales que prevén los Delitos Informáticos y que han servido para realizar un análisis dogmático jurídico-penal son el Código Penal Federal y el Código Penal para el Estado de Sinaloa, contemplándose en el primero la protección a la información, mientras que en el segundo, además de esta protección también lo hace respecto a la integridad de los sistemas de cómputo, así como de ciertos delitos patrimoniales cometidos por medios computacionales. Los Delitos Informáticos previstos en el Código Penal Federal pertenecen al grupo de los delitos referentes a la "revelación de secretos y acceso ilícito a sistemas y equipos de informática", mientras que los contemplados en el Código Penal para el Estado de Sinaloa se encuentran en el título referente a los "delitos contra el patrimonio". La Dogmática Jurídico Penal a través de la Teoría del Delito sirve para estudiar a un delito como es el Informático, ya que se analizan todos y cada uno de sus elementos integradores para llevar a cabo su aplicación a los casos concretos, sobre todo por ser un ilícito de reciente creación. Dentro de los elementos del Delito Informático la Tipicidad y su correspondiente Tipo Penal cobran gran importancia ya que las descripciones que hacen los legisladores Federal y del Estado de Sinaloa encontramos una diversidad de confusiones en sus descripciones que inclusive pudieran contraponerse con otras figuras delictivas como los del Derecho de Autor y los de propiedad industrial. Hasta ahora se han considerado a los Delitos Informáticos como ilícitos no graves, sin embargo, ante la gran problemática en el mundo de los hechos existe la tendencia de que en un futuro no muy lejano el legislador vea la necesidad de considerarlos como delitos graves, a efecto de no permitir a los sujetos activos su libertad provisional, situación que debe de analizarse detenidamente. Los delitos informáticos previstos en la legislación federal son perseguidos de oficio, mientras que los establecidos en el Código Penal para el Estado de Sinaloa su persecución es de querella Con fundamento en los tipos penales federal y del Estado de Sinaloa se realizó en éste trabajo un análisis pormenorizado de sus elementos tanto en su aspecto positivo como negativo, así como la vida de esos delitos

conocida como Iter Criminis y el concurso de delitos y de personas que pueden aparecen en estos ilícitos informáticos que han sido cuestionados en éste trabajo. Si bien es cierto, la delincuencia en todas sus inclinaciones ha avanzado en el uso de medios más modernos para realizar sus fines delictivos como lo es el uso de computadoras, también lo es que se deben modernizar las formas de combatirla, siendo el arma más adecuada el establecimiento de legislaciones acordes con esa problemática, tanto a nivel federal, local, así como internacional, toda vez que se está hablando de una delincuencia que se lleva a cabo en todos los rincones del mundo. La problemática de la Delincuencia Informática ha sido tan complicado ya que como se ha mencionado el avance de la tecnología informática ha sido tan impresionadamente rápido que ese avance se ha reflejado en los medios computacionales utilizados por la delincuencia; avances que han aparecido en los sistemas para guardar información dentro de esos sistemas informáticos con una mayor seguridad utilizando el sistema conocido de “encriptación”, sin embargo la delincuencia se ha asistido de expertos en informática para violar esas seguridad, encontrando así a los denominados Hacker, Lamer, Wracker, Cracker, Phreaker Script-Kiddies, Speaker y Rider; delincuencia informática que ha generado en el mundo desde los años 70s grandes daños a personas en lo particular, a empresas, a entidades financieras y a los propios Estados, al grado tal que han existido posibilidades de conflagraciones internacionales, que h utilizado inclusive la Internet para facilitar sus diversas conductas ilícitas, asistiéndose de los llamados “viru”. Dentro del mundo informático en la Internet ha surgido el llamado “Mundo Virtual” en el que se puede llevar a cabo una multiplicidad de operaciones “imaginarias” en las que el usuario puede ver cumplidos sus deseos que en el mundo real no pudiera llevar a cabo, como comprar inmuebles, barcos, edificios, participar en casinos, etc., sin embargo, lejos de cumplir esos deseos satisfactoriamente pueden ser objetivos de la delincuencia informática o bien participar activamente en ella, a través de operaciones ilícitas relacionadas con robos, fraudes, pornografía infantil, narcotráfico, entre otras muchas más, además de recibir información distorsionada acerca del tabaquismo, medicinas,

desórdenes alimenticios, etc…situaciones que debe considerar el legislador para establecer un adecuado marco jurídico. También ha surgido el llamado "Terrorismo Cibernético" considerado por el Diccionarios de la Real Academia Española como: "la actuación criminal de bandas organizada, que reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos", encontrando ya en nuestra legislación penal federal a la figura del terrorismo. Ese "Ciberterrorismo" a nivel internacional ha servido para realizar actos vandálicos como los suscitados en los ataques a las torres gemelas de Nueva York, en los Estados Unidos de América el 11 de septiembre de 2001, así como el de los trenes en Madrid España, el 11 de marzo de 2004. Los sistemas financieros en todo el mundo se han visto afectados por la delincuencia informática para afectar a la economía mundial. Novena.- Por ser un problema mundial la delincuencia informática ha sido regulada jurídicamente por diversos organismos internacionales entre los que encontramos a la O. N. U., el llamado "Grupo de los Ocho Países" y la Comisión de las Comunidades Europeas, siendo ésta última la que ha tenido mayores logros debido a la consolidación que han tenido los países europeos, creando convenios entre ellos como el de la "Cibercriminalidad", del 23 de noviembre de 2001, que precisa un marco jurídico avanzado en la materia. Dentro de esos países europeos España han establecido también una legislación detallada en cuanto al marco jurídico de los delitos informáticos. Uno de los grandes problemas de toda clase de delincuencia es el de detectar el modus vivendi y operando del delincuente para así poderlo detener, por lo que una de las ciencias auxiliares del Derecho Penal para llevar a cabo esa finalidad encontramos a la Criminalística que enfocada a Los Delitos Informáticos va a ser indispensable para lograr la aprehensión del delincuente informático que utiliza los grandes avances tecnológicos para sus fines delictivos y que se oculta y huye a través de las líneas alámbricas e inalámbricas de esos sistemas computacionales. Las investigaciones de los Delitos Informáticos han enfrentado grandes problemas de origen técnico de la Informática, así como en su grado de conocimiento de las personas de los diversos sectores en donde se comete esta

clase de ilícitos, así como de quienes se encargan de la procuración y administración de justicia, y de quienes establecen su marco normativo. Décima.- La Policía es de gran importancia para la investigación de los delitos, y los informáticos no son la excepción, por lo que surge a nivel internacional en diferentes países la “Policía Cibernética”, que deberá utilizar todos los conocimientos en Informática para localizar y detener al delincuente informático. En México encontramos la existencia de la “Policía Cibernética” en la estructura de la Policía Federal Preventiva a partir del año 2000 que dentro de sus objetivos es combatir a la corrupción de menores y a la delincuencia informática, coordinándose con otras corporaciones policiales en los Estados de la República Mexicana, así como a nivel internacional. A nivel internacional destacan grupos policiales en contra de la delincuencia informática tales como: la INTERPOL, la EUROPOL y el FBI. Las políticas en la Criminalística Informática se encuentran siempre avanzando y van dirigidas principalmente a cubrir las vertientes legal y técnica. En México, la Procuraduría General de la República y las procuradurías de cada uno de los Estados que de alguna manera contemplan en sus legislaciones a los Delitos Informáticos en los diversos enfoques que se han señalado durante la presente investigación acordes a los bienes jurídicos que se pretende proteger (integridad de los sistemas informáticos o ilícitos cometidos por medios informáticos), han venido realizando sus actividades para integrar tales ilícitos en áreas especialidades como: la de delitos de derechos de autor, financieros, patrimoniales, delitos no violentos, e inclusive en la propia Subprocuraduría de Investigación Especializada en Delincuencia Organizada, enfrentándose a las problemáticas jurídicas y técnicas que se han comentado; sin existir concretamente un área a nivel federal encargada de los Delitos Informáticos cuando el bien jurídico es la confidencialidad de la información.

AUTOR DEL RAE 233006_2

Delitos informáticos-caso de estudio

AUTOR Alicia Rubí Guerra Valdivia

FICHA BIBLIOGRÁFICA GUERRA VALDIVIA, Alicia. Delitos informáticos – caso de estudio. México, 2011, 144 p. Tesis de maestría (Tesis de grado (Maestro en ingeniería en seguridad y tecnologías de la información). Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica.

PALABRAS CLAVE

PALABRAS DESCONOCIDAS Jactarse, lindar, discrimen, soslayado, apologético.

FUENTES 81

CONTENIDO DEL RAE Con el desmesurado avance tecnológico, que en ocasiones ha superado las estadísticas propuestas y que ha conllevado a que el activo más valioso pase a ser la información, fue necesario implementar acciones, políticas, estrategias, que nos permitan tener un control total sobre el mismo, aquel que nos garantice que la información contenida en bases de datos, servidores, y otros medios de almacenamientos, esté segura y no pueda ser modificada por parte de terceros, porque a pesar de que pueda ser castigada y sancionada la acción contraria a lo dispuesto en la normatividad legal de cada país, esa acción no permitirá que la información vuelva a nuestro poder, tal cómo se encontraba antes de ser modificada o encriptada. En algunos países existen reglas, leyes, acuerdos, tratados, convenios, por medio de los cuales se crearon algunas conductas que pueden tipificarse como delitos, en este caso delitos informáticos, existiendo siempre una brecha que en la mayoría de los casos permite que aquel delincuente informático, no pueda ser juzgado adecuadamente según la conducta delictiva cometida porque existen vacíos en la norma o el desconocimiento de su aplicabilidad en algunos casos, conlleva a esto. Por eso es indispensable que antes de sancionar o permitir que entre en aplicabilidad nuevas

leyes, existan comisiones que se encarguen de verificar que dichos proyectos de ley cubran las necesidades que exigen la justicia y por medio de las que se puedan castigar todas aquellas acciones que ocurran, puedan ocurrir y se eviten vacíos, útiles para los defensores de justicia. Hoy en día las acciones delincuenciales están enfocadas a atacar los sistemas de información, principalmente de grandes empresas, es por eso que existe la necesidad inmediata de vincular de manera efectiva la legislación penal con la tecnología, debe pensarse en la creación, y ejecución de una legislación eficaz, aquella que no permita que existan vacíos legales, debido a la atipicidad de algunas conductas que en los estrados no pueden ser avalados y que de esta manera no permita la persecución penal de aquellas estructuras delincuenciales dedicadas a la ejecución de delitos informáticos, también por el continuo avance de las diferentes modalidades utilizadas que conllevan a que la normatividad existente, no esté actualizada jurídicamente para castigar cualesquiera de fraudes informáticos que ocurra. Con las razones anteriormente expuestas es que se centra el objetivo de la tesis, por medio de la que se dará a conocer un panorama respecto a la ejecución de la normatividad existente en México con la implementación de la legislación ante esas conductas punibles, ya que entre menos acciones penales existan por parte de las autoridades del orden, mayor será la ejecución de las modalidades de delitos informáticos en la nación y en las diferentes territorialidades del mundo, siendo esta la peor tarjeta de presentación por parte de los que administran justicia y los legisladores de un país. Mas sin embargo es de aclarar y teniendo en cuenta todos los casos conocidos, donde por mal uso dado a los avances tecnológicos sobre los que el hombre puede tener dominio, no se puede decir que los avances tecnológicos sean los mismos culpables de afectar en problemática la vida de las organizaciones y/o personas, sino de la mala manipulación realizada por parte del hombre con intenciones ilícitas, a los sistemas. Así mismo y basados en que día a día ligado al avance tecnológico surgen nuevas modalidades delictivas, no es preciso culpar al legislador y su grupo de trabajo por no implementar e incorporar nuevas conductas delictivas en el Código penal, sino por

el contrario centrar los objetivos sobre los motivos que conlleva a aquellas personas a realizar dichas conductas delictivas, pues los delitos informáticos siempre son acciones realizadas por el hombre, de ahí que surge el binomio informática – derecho; porque de nada sirve tener una sociedad culturalmente reconstruida, con importantes mejoras en su calidad de vida, cuando a la par con estos cambios y mejoras trae consigo conceptos de involución que jurídicamente son tutelados y permite lesionar bienes o el buen nombre de las personas. Con el planteamiento anterior podemos observar que a pesar de los avances tecnológicos que han surgido al igual que sus repercusiones en nuestros días nos ha incitado a la búsqueda de soluciones inmediatas que llevan a no diferenciar las conductas cometidas. Pero también encontramos situaciones en algunos países los cuales han incorporado normatividad que castigue estas modalidades delictivas relacionadas con delitos informáticos, así como existen países donde no existe normatividad que regule esa actividad delictiva y por el contrario permiten congresos de hackers, quienes motivan el derecho a ejercer su conocimiento, más aun cuando existen monopolios de la información y contra los que no cuentan con la capacidad de proteger información confidencial, evidenciando que dejan a un lado la responsabilidad que les embarga como estado y que a su vez puede convertirse en apologías peligrosas frente a la actividad realizada por los hackers. Con razón a esta situación y a otros casos presentados y teniendo en cuenta que es responsabilidad como nación velar por la protección a los Derechos Humanos DDHH, México hace parte de la cumbre mundial sobre la sociedad de la información; misma forma ocurre en la convención de Budapest en la cual se señala una política penal común para la protección de la sociedad con relación a la ciberdelincuencia y en la que se señala la protección de los estados en la participación para la protección de los intereses comunes, notando de esta manera que ya existe una cooperación internacional frente al castigo de los delitos informáticos.

CONCLUSIONES La influencia de la globalización en la evolución de las sociedades, así como el desarrollo de nuevas tecnologías trae aparejado el surgimiento de nuevas conductas que no siempre se encontrarán dentro del marco de la legalidad y la seguridad social. La problemática central aparece entonces como resultado del progreso cada día más importante y sostenido de los sistemas computacionales, que en la actualidad posibilitan procesar y poner a disposición de la sociedad en general una cantidad creciente de información de toda índole, que aparece entonces al alcance de millones usuarios de un servicio basado en tecnología a nivel internacional. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, y prácticamente sin limitaciones, cede con facilidad a todo aquel que lo desee un conjunto de datos que, al menos hasta hace algunos años, sólo podían obtenerse luego de prolongadas búsquedas y selecciones, en la que el individuo representaba un papel determinante y las máquinas existentes tenían el rango exclusivo de equipos auxiliares para dicha labor. En la actualidad, en cambio, ese enorme caudal de información puede adquirirse de manera casi inmediata, transmitirse incluso documentalmente y llegar al usuario mediante sistemas sencillos de operar, confiables y capaces de responder casi ante toda la gama de interrogantes que se planteen a los archivos informáticos. La manipulación fraudulenta de los sistemas informáticos con ánimo de lucro, la destrucción de programas o datos, así como el acceso y la utilización indebida de la información que posee la potencialidad de afectar el ámbito de lo privado, son sólo algunos de los múltiples procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos, así como causar importantes daños materiales y/o morales. Se debe considerar entonces la importancia de que la magnitud de los perjuicios así ocasionados es a menudo importantemente superior a la que es usual en la delincuencia tradicional, así como el hecho de que existen muchas más posibilidades de que este tipo de delitos no lleguen a descubrirse. Se trata, entonces, de una delincuencia de

especialistas en tecnologías de la información, con tal pericia que en muchas ocasiones saben cómo borrar toda huella de los hechos. Ante la problemática anterior, resulta evidente la importancia del papel que tiene el Derecho ante el avance y aparición de novedades tecnológicas para servir como elemento disciplinado y regulador del proceso. He ahí la importancia de gestionar una legislación específica y concreta en materia de delitos informáticos. A lo largo de esta tesis, se han venido identificando problemas de diversa índole, entre los cuales, a mi parecer, una adecuada definición con respecto a lo que es un “delito informático”. Resulta imposible cubrir la gran gama que hay con respecto a los mismos, debido a que las tecnologías día a día avanzan. Resulta ilógico tener en cuenta la temporalidad a que se sujeta en determinado momento la sociedad. El concepto de esta conducta delictiva debe englobar que no solamente se puede hacer uso de la tecnología como medio para delinquir, es decir, no solamente es un medio, podría ser un fin; independientemente de cuáles sean los de mayor recursión. Se podría definir un delito informático como una conducta delictiva que afecte a un tercero, la cual puede ser realizada mediante cualquier medio que implique la tecnología. Dicha conducta delictiva, independientemente si es usada como medio o como fin, tendrá que sancionarse. Los delitos informáticos, no suceden únicamente en determinadas regiones del mundo, si bien es de notarse que ciertos países son los más atacados, también lo es que ninguno está exento de tales conductas delictivas. Las implicaciones jurídicas y políticas de las posibles búsquedas transfronterizas, se están convirtiendo en una preocupación para las agencias de aplicación de la ley en todo el mundo, que día a día emprenden una luchan contra los nuevos desafíos planteados por las comunicaciones en red y las nuevas tecnologías. Los procedimientos tradicionales de investigación (y en particular los procedimientos a menudo engorrosos que rigen las investigaciones a nivel internacional) puede no ser adecuados para satisfacer las necesidades en casos de delincuencia informática, esto para una acción inmediata y aplicación de la ley que va más allá de las fronteras nacionales. La globalización de la actividad delictiva ha creado problemas molestos que, en algunos casos, desafían las

soluciones simples. Es decir, se pueden tener varios escenarios al respecto. Un delincuente puede utilizar una computadora para cometer un delito tradicional, como el fraude o el robo (por ejemplo, la promoción de inversiones falsas en una página web), así mismo, también el equipo mismo es el que puede contener elementos que funjan como prueba del delito (por ejemplo un traficante de drogas, que en resguardo de sus contactos lo tenga en su equipo. Una de las grandes desventajas para sancionar este tipo de delincuencia es la distancia y la ubicación de quien comete el delito. No se pretende demeritar algún otro tipo de delincuencia, sin embargo, un delincuente informático (por ejemplo) no necesitaría de altos recursos monetarios para transportar determinada mercancía, simplemente el hecho de saber explotar su conocimiento bastará para que inclusive adopte la identidad de un tercero. Es el caso que en Estados Unidos de Norteamérica el Juez Harold Baker dictaminó un fallo histórico al decir que “no somos direcciones IP”. Lo anterior va relacionado al robo de identidad, si se parte del conocimiento que debe de tener el juzgador al identificar lo que es una dirección IP y que hoy en día tienen el criterio para hacer alusión a una falsa alegoría de suponer que una dirección IP equivale a una persona. Los tratados internacionales que hay con respecto a los delitos informáticos, son un recordatorio de que cada país, debe de contar con una legislación adecuada para sancionar los mismos; así como una cooperación entre los diversos países para combatir con los delitos informáticos, que hoy en día es asunto mundial. Los delitos informáticos en México, no son exclusivos de la competencia en materia penal, la diversidad de delitos variará con respecto a las ideas que tengan las personas que hagan uso de medios tecnológicos para delinquir. Los delitos informáticos no pueden ser una actividad que se someta al capricho temporal que vive día a día la sociedad y que está en constante crecimiento; por ende, se debe de aspirar a la creación de una ley más eficaz y amplia. México no puede permanecer en el caso de que se tengan que sufrir consecuencias para dar resultados, la jurisprudencia debe de ayudar a una mejor legislación en cuanto a vacíos legales, sin embargo, resulta complicado que haya resoluciones al

respecto, sin antes existir una ley que los regule. No es posible seguirse apegando a figuras típicas que no resuelvan una problemática específica, pues desde su formación se puede apreciar si estas figuras cumplirán con el objeto primordial del derecho: lograr una correcta relación entre los miembros de la sociedad. Se tiene que se puede contemplar el delito sólo si se accede a un sistema informático protegido por un mecanismo de seguridad, lo cual me atrevería a señalar que podría ser absurdo. Esta problemática es planteada por el Dr. Nava Garcés que nos da un ejemplo claro al decir que para que se diera el delito de allanamiento de morada es necesario que la casa habitada cuente con un candado, llave, portón o cadena protectora. La justicia no puede reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad o que en todo caso hayan tenido un descuido (y no se pretende justificar la falta de precaución); esto podría ser que en todo caso, el que una computadora esté conectada a Internet significa que cualquiera puede justificadamente borrar o destruir archivos, sólo porque no está protegida por algún mecanismo de seguridad, o en su caso, no encuadraría con el delito como lo estipula la ley, dejando desprotegido a cierto sector de la sociedad. Es decir, la ley no solamente debe de proteger a un nicho de ciudadanos que sean cuidadosos, la legislación mexicana debe de proteger a cualquiera que esté dentro de su ámbito y por consecuente no esperar hasta el momento en que un juzgador deba de dar interpretación a ello. Como se planteó en esta tesis, una de las desventajas principales, es que la legislación no es específica en cuanto a determinados términos que la misma plantea, como: “mecanismo de seguridad”; y, no hace referencia a los mismos. Consecuentemente, en estos casos se deja a criterio del juzgador darle interpretación al mismo, es aquí donde entra la importancia de que los juzgadores tengan conocimiento al respecto, las periciales, es decir, todos los resultados de una ardua investigación, serán entregadas a ellos, y éstos son los que tendrán que dar resolución. Ahora bien, no es algo nuevo para ellos esta decisión, sin embargo, el tema de las TIC’s va a la vanguardia y tan rápido como va avanzando la tecnología, irán avanzando la diversidad de delitos que se

pueden cometer al respecto, independientemente de que los métodos varíen, los resultados, si bien no serán iguales, van encaminados a una comisión delictiva que, como es de esperarse, afecta a alguien más. Remembrando una frase en una obra literaria versa de la siguiente manera: (…) “Vamos despacio, que juez que mal se informa, mal sentencia”, si bien a primera lectura, esta simple frase puede resultar algo muy lógico, es ya una necesidad que los juzgadores estén informados al respecto y sepan cómo se cometen este tipo de delitos, aclarando que, no con esto se quiere dar a entender que sean especialistas en el tema, sino que conozcan e identifiquen la gran variedad que existe hoy en día para cometerlos; y, de esta forma, tengan en cuenta que no solamente ya son computadoras las que se usan para delinquir, sino también algún dispositivo móvil, que en manos de alguien que lo sepa usar, será de la misma utilidad que una computadora. Es momento de que haya una reacción colectiva ante la incuestionable realidad que estamos viviendo con respecto a la tecnología.

Inclusión de los delitos informáticos, que se cometen en internet, dentro del código penal guatemalteco.

AUTOR Elmer Yovany López García

FICHA BIBLIOGRÁFICA LÓPEZ GARCÍA, Elmer. Inclusión de los delitos informáticos, que se cometen en internet, dentro del Código Penal guatemalteco. Guatemala, 2011, 118 p. Tesis de grado (licenciado en ciencias jurídicas y sociales). Universidad de San Carlos de Guatemala. Facultad de ciencias jurídicas y sociales.

PALABRAS CLAVE Código penal, delito informático, informática, historia, Convenio.

PALABRAS DESCONOCIDAS Descuellan, talión, laguna legal.

FUENTES 25

CONTENIDO DEL RAE En el presente documento el autor quiere dar a conocer la importancia de la inclusión de los delitos informáticos en la legislación Guatemalteca mediante cuatro capítulos en los que explicará los aspectos generales, la teoría general del delito, informática e internet y la inclusión del delito informático en el código penal español. El derecho penal surgió a raíz del nacimiento del hombre, pues es por medio de este que se evalúan las acciones realizadas por él y a través del mismo se determina si se pueden castigar y/o sancionar o por el contrario son aceptadas para la sociedad, funcionando solamente en caso de vulnerar a la sociedad, evitando de esta manera que cada quien tome justicia por sus propias manos, tal como ocurría con nuestros ancestros. A través del derecho penal existen normas y disposiciones jurídicas que permiten regular las conductas delictivas cometidas por ciudadanos y a su vez castigar y/o sancionar a quien la ejecutó o participo de ella; es por medio de esta que las diferentes naciones deben regular las conductas delictivas relacionadas con delitos informáticos y por lo cual en Budapest se firmó un convenio mediante el cual se fijaron algunas pautas básicas que deben cumplir los países que hacen parte de el con los cuales permitan brindar condiciones de seguridad a los ciudadanos que hacen uso de los medios tecnológicos, ya sea por ocio, académico, laboral, comercial, entre otros. A pesar de la informática ser una ciencia nueva en el contexto humano, es una de las que más avances ha tenido desde su aparición y es por eso la necesidad que debe haber en cada nación, ya que, así como hay avances tecnológicos, existen individuos que, de una manera u otra, pueden causar daño al ciudadano y a grandes organizaciones. Manifiesta el autor que Guatemala no puede ser ajeno a este tipo de conductas ya que en el código penal no existe normatividad que regule, castigue, sancione a quienes incurran en algunas de esas conductas, siendo las más conocidas la manipulación de datos de entrada, fraude, sabotaje, virus informático, entre otras. El crecimiento tecnológico, así como los grandes avances que se han presentado, la reducción

del tamaño de grandes equipos de cómputo, anteriormente llamados ordenadores, así como la reducción de los chips, conlleva a que existan modalidades delincuenciales por medios informáticos en nuestro país, tal como se evidencia haberse presentado en otros países, principalmente de Europa, y que no solamente puede afectar la información de empresas, sino también la de personas, permitiendo que de esta manera con esa información confidencial que pudo verse afectada, pueda surgir nuevos tipos delincuenciales, como lo es la extorsión, el sabotaje informático, permitiendo que de esta manera se puedan causar grandes pérdidas económicas. Existen empresas que administran bastante información valiosa, confidencial y de no existir parámetros para protegerla, normatividad para castigar y sancionar a quien incurra en los delitos, es posible decir que el hombre no se desvela por la informática, sino la utilización que el hombre le puede dar a la informática, así mismo con los sistemas de información que administren información privada de las personas o de empresas dedicadas al almacenamiento, así como de las bases de datos de las imágenes de los diferentes programas para dispositivos móviles (celulares). Un delito informático es cualquier comportamiento contrario a lo descrito en la normatividad jurídico legal existente para cada país y que sea realizado utilizando redes informáticas, pueden ser activos o pasivos. La inclusión de normatividad que regule los delitos informáticos, debe ser ajustada y regulada para todos los países, independiente si existe antecedentes o no, de casos conocidos cometidos por vía informática, lo anterior teniendo en cuenta que nuestro país no tiene en su código penal normatividad que proteja al ciudadano de bien, a las organizaciones y que permita judicializar a los delincuentes dedicados a esta actividad ilegal; pues de esta manera a pesar de ser conocedores de la modalidad que se presente, no será posible tipificar de manera acertada al conducta a quien la esté o haya cometido, ya que en el código penal en su primer artículo se establece el principio de legalidad, por medio del cual nadie puede ser juzgado por hechos que no se encuentren calificados como delitos o faltas en el marco del Código y también existe lo denominado y conocido en doctrina como laguna legal, que no es más

que la ausencia de normas positivas aplicables a relaciones o casos jurídicos determinados. Es muy importante que el gobierno nacional tome cartas en el asunto a fin de implementar, incorporar o crear nuevas conductas por medio del os cuales los delincuentes informáticos puedan ser perseguidos, castigados, sancionados, y no se sigan amparando en la laguna legal o en al artículo primero del Código Penal; la nación debe estar avante ante cualquier delito informático que se pueda presentar y no solo de ciudadanos, sino también ante empresas del estado, que administran diferentes bases de datos en las cuales se encuentra información confidencial de todos los que habitamos en Guatemala como también de las diferentes actividades que hacen las fuerzas del estado, entidades del estado, lo cual al caer en manos de personas inescrupulosas puede ser un peligro para la seguridad pública de la nación; también es indispensable que antes de promulgar nuevas leyes o modificarlas, se reúnan los legisladores con sus grupos de trabajo, invitando asesores de otros países que ya tengan conocimiento sobre las modalidades utilizadas por los delincuentes informáticos, para que sirvan de guía ante la creación e implementación de leyes que permitan combatir los delitos informáticos y castigar sus autores.

CONCLUSIONES El derecho penal, establece reglas para el lineamiento de la conducta del ser humano en la sociedad, pero al avance de la tecnología y su utilización en la informática han generado muchas formas de delinquir sin poder tener una consecuencia jurídica para lograr establecer una violación de un orden jurídico y de la pena como reintegración de ese orden al no limitar la conducta humana.

La carencia de tipicidad del delito, en una legislación penal conlleva al ser humano a actuar fuera de los límites que establece el derecho penal ejerciendo una manifestación de voluntad delictiva no penado por la ley, pero la falta de acción

penal, ausencia de tipo, falta de condición objetiva es lo que actualmente carece la legislación y como consecuencia no nace el delito y menos se obtendrá una pena. La informática, la Internet, los sistemas de datos de cómputo y en general todo lo relacionado con el software se han convertido en el objetivo de los delincuentes informáticos, que por su nivel de conocimiento realizan hasta el espionaje industrial y el personal introduciéndose sin autorización violando un derecho de la sociedad civil, empresas privadas, como de instituciones públicas.

Los delitos informáticos en cuanto a su comisión, son relativamente fáciles de realizar con resultados altamente satisfactorios sin ser descubiertos, pero sin estar ninguno regulado, por consiguiente, no constituyen delito y deja en libertad a quienes los cometen con total impunidad para satisfacer sus intereses quedando el ordenamiento jurídico nacional rezagado a nivel de sistemas operativos.

AUTOR DEL RAE 233006_2

Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica

AUTOR Andrés Bolaños Díaz & Teresa De Jesús Narváez Narváez

FICHA BIBLIOGRÁFICA Bolaño, Andrés. Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica San Juan de Pasto, 2014, 100 p. Monografía (Especialización en Seguridad Informática). Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas Tecnología e Ingeniería.

PALABRAS CLAVE Ley, Legislación, Ciberdelincuencia, Delito Informático, Sanciones legislativas, falencias, normativa.

PALABRAS DESCONOCIDAS Mobbing

FUENTES 63

CONTENIDO DEL RAE En esta monografía se realizó un análisis comparativo sobre delitos informáticos teniendo en cuenta la legislación encontrada sobre este tema en Colombia, primeramente, Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela. Se confrontan las leyes de Delitos Informáticos de los países seleccionados con los delitos informáticos contemplados en el Convenio de Ciberdelincuencia de Budapest 8 que se acordó en el 2001 por la ONU (Organización de Naciones Unidas) de ese entonces, hoy ratificado por más de 100 países. Después de esto se realizó una confrontación de cada artículo de la Legislación Colombiana Ley 1273 de 2009 comparada con las leyes que contemplan características similares de los 6 países seleccionados para el estudio: Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela; mediante esta comparación se determinaron las fortalezas, debilidades y falencias de la legislación Colombiana en cuanto a los delitos informáticos, Los delitos informáticos fueron catalogados internacionalmente mediante el convenio de Ciberdelincuencia y Colombia no ha ratificado su participación activa de este Convenio, aunque se tomó como pilar en la formulación de la Ley 1273 de 2009, no se lo adoptó en su totalidad, por esta causa es necesario volver a retomarlo para actualizar la caracterización de los delitos e identificarlos con el mismo nombre como se conocen a nivel internacional. La Ley 1273 del 05 de Enero de 2009 de la República de Colombia necesita encontrar un contraste con la legislación afín en países que tienen similares condiciones como: que hablen el mismo idioma, que tengan similitud en la economía, el poder militar, estabilidad, población, desarrollo y el papel en el mundo ,como Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela, para crear un ambiente balanceado en el que se pueda establecer una comparación beneficiosa que enriquezca la formulación de las nuevas normas. El mismo entorno tecnológico cambiante obliga a los entes legislativos a evaluar su sistema legal, es necesario determinar las falencias existentes en la norma sobre delitos informáticos a la luz de otras legislaciones y

de tratados internacionales, que permitan proyectar leyes adecuadas y efectivas que cumplan con su misión de proteger. Y estos entes buscan puntos de vista que favorezcan o amplíen su visión de la problemática, y la buscarán en las fuentes que se especializan en el estudio de estas áreas temáticas, en este caso, entre los estudiosos de los sistemas informáticos, es un deber de los profesionales del área poner a disposición documentos que faciliten esas consultas. En Colombia se ha creado un marco jurídico que abarca determinados delitos informáticos, pero es necesario que se hagan aportes críticos que puedan motivar la creación de nuevos artículos legislativos que incorporen los delitos que aún no han sido contemplados en la legislación nacional. La norma se mantiene en un ambiente dinámico que permite su renovación y reforma, de modo que es posible argumentar la inclusión de normas que castiguen los nuevos delitos al identificarlos, con el fin de propender por la defensa de la integridad de los datos y la información de la sociedad en general. Cabe destacar que la Ley Colombiana se ha constituido en un punto de referencia para otros países, porque a nivel internacional ha sido uno de los primeros en elevar a bien jurídico la Información y el dato, como lo explica su autor, es decir, la información y el dato se convierten en bienes protegidos por el derecho. Aunque se aprobaron exitosamente 10 Artículos, se pueden mejorar aún más, como lo expuso el Doctor Díaz García en su Proyecto de Ley de Delitos Informáticos, en la cual expresaba con palabras más claras la tipificación de cada delito informático sobre el cual se legisla, al igual se dejaron por fuera tres artículos que el autor proponía que son de gran importancia sobre los cuales se podría argumentar legalmente: Falsedad Informática, Espionaje Informático, Spam (correo no deseado) Y no solamente estos delitos, sino todos aquellos que se van tipificando por el constante crecimiento de nuevas formas de delinquir en contra de la seguridad informática, como por ejemplo: El Bullying Informático, El Mobbing Informático Pero la idea propuesta a través de este estudio es la concientización de la importancia de incluir en la legislación colombiana políticas de Seguridad Informática como lo hizo el país con Legislación más reciente, Perú, la Ley Peruana en cuanto a Delitos

Informáticos es muy completa, gran parte de su estudio se basa en el Convenio de Ciberdelincuencia del 2001, y se fortalece mucho más cuando establece una disposición que particularmente promueve el uso de Medidas de Seguridad para la protección de los datos y su integridad, y las buenas prácticas. Se requiere plantear una mejora a la ley 1273 en la legislación nacional Estas mejoras se plantean con el fin de manifestar un punto de vista de los autores basados en el conocimiento adquirido en la Especialización de Seguridad Informática y para exponer teóricamente la necesidad de modificar la Ley sobre Delitos Informáticos en Colombia, para que los artículos sean más específicos, se pueden plantear las siguientes mejoras: Modifíquese el título del Artículo 269B como Extorción Informática. Y adiciónese a la definición del delito el texto con el fin de lucro personal. En el Artículo 269D, adiciónese a la definición del delito el texto o altere, sustraiga, destruya o inutilice los objetos que puedan servir de prueba ante la autoridad competente. En el Artículo 269G, adiciónese a la definición del delito, el texto La misma sanción será aplicada al que suplante identidad en redes sociales o sitios de internet, Incorpórese el Artículo 269M: Espionaje Informático. El que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado, incurrirá en prisión de seis (6) a diez (10) años y multa de 500 a 2.500 salarios legales mínimos mensuales vigentes

CONCLUSIONES Se concluye que a la Legislación Colombiana le hace falta el tratamiento de algunos delitos que han sido establecidos en el Convenio de Ciberdelincuencia de las Naciones Unidas, como son: Abuso de dispositivos y Falsificación de Información. Se concluye que Colombia al no hacer parte activa del Convenio de Ciberdelincuencia provoca que tenga falencias en su normativa jurídica ya que no asocia las definiciones de delitos informáticos con los términos que ya se han definido a nivel internacional. También se concluye que no existe

un organismo de control especializado que se haya establecido desde la Legislación Colombiana encargado de asegurar el tratamiento de los Delitos Informáticos. De acuerdo a la búsqueda de información realizada, se concluye que en Colombia se han cometido muchos delitos informáticos que no han sido castigados de la forma adecuada porque no se encuentran bien tipificados en la norma. Se concluye que las mejoras mostradas como resultado de este estudio pueden servir como base para formular proyectos de Ley de futuras legislaciones en cuanto a la tipificación de delitos informáticos. Mediante el estudio realizado se concluye que las falencias principales de la Ley 1273 de 2009 se encuentran: - En su contenido, porque existen delitos que deberían contemplarse. En las definiciones de los delitos, porque existiendo definiciones en tratados internacionales no se los utiliza plenamente - En la tipificación específica de los delitos, porque los títulos como se los conoce no son comprensibles a todo lector.

AUTOR DEL RAE 233006_2

Caracterización de los delitos informáticos en Colombia.

AUTOR Iván Manjarrés Bolaño & Farid Jiménez Tarriba

FICHA BIBLIOGRÁFICA MANJARRÉS, I & JIMÉNEZ, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82. {En línea}. Fecha de consulta 25 de mayo de 2017. Disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

PALABRAS CLAVE Delitos, Tecnologías, Internet, Información, Seguridad.

PALABRAS DESCONOCIDAS

FUENTES 15

CONTENIDO DEL RAE Para nadie es un secreto, que los avances tecnológicos demuestran la evolución del hombre y las capacidades que tienen, ya que gracias a estos avances han permitido que desde sus hogares todas los ciudadanos que

tienen acceso a internet, puedan realizar, consultar, llamar, opinar, de temas académicos, comerciales, de amor, y hasta aprobar o reprobar pensamientos de política; pero así como estas redes nos permiten realizar un sin número de actividades también es posible que se ejecuten actividades ilegales según lo descrito en nuestra normatividad legal vigente que abarca los delitos informáticos con sus respectivas modalidades o formas de ejecución, las cuales pueden poner en riesgo nuestra información, economía y hasta nuestra integridad personal o de nuestras familias. Es por eso que mi objetivo al elaborar este documento, es consultar, analizar y compartir con ustedes los resultados obtenidos en base a las investigaciones que han adelantado con relación a las modalidades delictivas de delitos informáticos que se conocen en el país. Así mismo es muy cierto que la nueva reglamentación implementada en Colombia relacionada con la persecución a quienes ejecuten conductas relacionadas con delitos informáticos y tipificadas en los artículos 269a al 269j del Código Penal colombiano es un complemento a lo que ya existía en la misma norma, con la diferencia que esta hace alusión a las realizadas sobre medios informáticos, haciendo uso de redes de telecomunicaciones, entre otras, conllevando a que en los tribunales su enfoque jurisprudencial se haga desde un enfoque anterior y no basado en lo tipificado en la conducta imputada al delincuente, obteniendo pocos resultados dentro de las investigaciones. Es por eso que así como el estado colombiano sancionó y puso en ejecución desde el pasado 5 de enero de 2009 la ley 1273 más conocida como el de delitos informáticos, es necesario que tanto jueces, como fiscales y a su vez los investigadores de estos delitos, sean capacitados para así poder dar un enfoque judicial a la conducta incurrida permitiendo que de esta manera exista involución por parte de los delincuentes informáticos y se evite que sigan aumentando ataques informáticos y a su vez perjuicios económicos y morales. Para la ocurrencia de un delito informático y comparando con la violencia que hemos vivido en nuestro país, y que por ser un delito en algunos casos vía administrativa no se requiere utilizar arma de fuego, pero en este caso si podemos decir que cada vez que un delincuente informático acciona el clic, es como si

hubiese accionado un arma de fuego, ya que, por medio de ingeniería social, es que normalmente se inicial los delitos, principalmente informáticos. A pesar de que las autoridades tienen conocimiento de las modalidades tipificadas en el Código Penal Colombiano y de las utilizadas por los delincuentes, no es suficiente pues en un gran porcentaje las víctimas no son las autoridades sino el ciudadano de a pie, lo anterior basado en que las estrategias implementadas por las autoridades, en su mayoría de casos no son dadas a conocer a toda la ciudadanía, también porque la ciudadanía las conoce pero no sabe aplicarlas, y en la mayoría de casos ciudadanos que no toman las medidas de precaución necesarias argumentando que a ellos no les pasará. Dice la historia que la aparición del primer ordenador fue para la década de los 50 y que el primer conocimiento que se tuvo de algún fraude informático hoy en día delito informático, fue para la década de los 60, en Alemania y Estados Unidos; así mismo que los primeros estudios respecto a actividades delincuenciales vía informática se hicieron a mediados de los años 70 y fue utilizando el método científico por medio de investigaciones criminológicas. A raíz de los resultados obtenidos en dichas investigaciones, tiempo después salió a la luz pública un sin número de casos presentados en donde la sumatoria de cifras de dólares hurtados o desviados, y marcos alemanes, superó la barrera de los mil millones. Posteriormente a finales de los 90 y con ocasión a la migración de algunas modalidades delincuenciales a internet, surgió un grupo denominado G8 con el fin de estudiar los problemas emergentes de criminalidad migrados a dicha plataforma. Para la realización de un delito informático es necesaria la participación de dos sujetos, uno activo y el otro pasivo, el primero de los mencionados es aquel que realiza o participa de la acción delincuencial, el otro es la persona propietaria del bien jurídico tutelado, conocida penalmente como la victima de los hechos. El sujeto pasivo es sumamente importante en un proceso investigativo inicialmente para que denuncie el caso ocurrido y segundo para obtener a través de su relato, información de cómo ocurrió la conducta para de esta manera el ente investigador tener conocimiento del modus operandi utilizado y así mismo saber las acciones a iniciar para establecer el autor de la conducta

ejecutada. Con base en las denuncias instauradas la Comisión de regulación de las Telecomunicaciones por sus siglas CRT, dio a conocer que en el primer trimestre del año 2008 los suscriptores del servicio de internet aumentaron en un 13.6%, lo que conlleva a que con la masificación del servicio de internet ha permitido mayores avances y también nuevas modalidades utilizando esta herramienta de telecomunicaciones. El ente de la Policía colombiana encargada de adelantar este tipo de investigaciones lo realiza mediante tres aspectos importantes, el primero preventivo a través de campañas por medio de su portal web, investigativo por medio de la coordinación llevada por parte de la Fiscalía general de la nación, gerente de los procesos investigativos y político, participando en la promulgación y elaboración de proyectos de ley que permitan tipificar las nuevas conductas conocidas.

CONCLUSIONES Del presente proyecto hemos sacado las siguientes conclusiones: El continuo avance de las Tecnologías de la información, está ocasionando, además de múltiples beneficios para la sociedad, la proliferación de los denominados delitos informáticos. La delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países latinoamericanos, conllevan también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales. La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones. Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que, a

nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

AUTOR DEL RAE 233006_2

Modalidades, participación y sanción en la comisión de delitos informáticos en Colombia a partir de la ley 1273 de 2009.

AUTOR Eberzon Manuel Ortiz Muñoz

FICHA BIBLIOGRÁFICA ORTIZ MUÑOZ, Eberzon. Modalidades, participación y sanción en la comisión de delitos informáticos en Colombia a partir de la ley 1273 de 2009. Pereira, 2012, 71 p. Tesis de grado (Especialización en Derecho Penal y Criminología). Universidad Libre de Colombia, facultad de derecho.

PALABRAS CLAVE Delito, ley 1273 de 2009, tecnología, fraude, denuncia, ciberdelincuente.

PALABRAS DESCONOCIDAS Contera, concomitante.

FUENTES 11

CONTENIDO DEL RAE En el presente documento, el autor quiere explicar las modalidades existentes para incurrir en delitos informáticos, al igual que diferenciar entre autor y coautor, en ambos casos participes de la conducta punible. Conocedores de la existencia de la ley 1273 de enero de 2009, conocida como Ley de delitos informáticos, no es menester entrar en detalles sobre cada uno de sus aspectos jurídicos y la discriminación de cada uno de sus artículos, más sin embargo si es indispensable dar a conocer al lector, como puede incurrir en una conducta ilícita descrita en mencionada ley, de la cual muchas personas desconocen su existencia. Podemos afirmar que para el aumento que existe en

cuestión al número de denuncias instauradas por alguno de los delitos descritos en la ley 1273 de 2009 deben existir causas que permitan al ejecución de la conducta punible, podemos determinar que en un estado donde no exista regulación precisa que permita frenar la actividad delincuencial ejecutada por los ciberdelincuentes, los avances tecnológicos no tendrán como objetivo contrarrestar las modalidades utilizadas, y no podrá existir persecución contra ese crimen tecnológico. Entrando ya al objetivo del presente documento, nos enfocamos a lo descrito en el artículo 30 del código penal colombiano en el cual nos define al determinador y al cómplice, siendo el primero de estos quien instiga al segundo para cometer la conducta y por ende la pena es mayor para el primero. De esta forma es posible determinar que, si se puede presentar la coautoría en la ejecución de un delito informático, pues un empleado de una empresa, puede ser inducido por otro, para que realice alguna acción por medios informáticos, permitiendo de esta manera tener estatus frente al grupo delincuencial del cual quiere hacer parte. También encontramos el cómplice, que no es más que aquella persona que sin ser partícipe de la conducta punible ejecutada, tiene conocimiento de la misma y accede a la contribución del delito principal; existen 3 tipos de cómplice: previo, aquel que participa antes de la ocurrencia de la conducta ilícita; concomitante, aquel que participa durante la ejecución de la conducta ilícita; y posterior, aquel que participa posterior a la ejecución de los hechos, modalidad que también puede presentarse ante la ocurrencia de un delito informático, como por ejemplo al momento de acceder a una base de datos por parte de un ex funcionario de una empresa, conlleva a que un empleado le preste el usuario. Entrando en detalle con el proceso investigativo, respecto a la recolección de pruebas y por medio de las cuales se puede demostrar la participación de una o más personas en una conducta punible, encontramos en la Constitución nacional el artículo 15, derecho a la intimidad, si bien es cierto que todo ciudadano tiene unos derechos (inviolables) y deberes, el legislador debió incorporar normatividad que bajo circunstancias necesarias, permita vulnerar derechos fundamentales, en este caso la intimidad, por tal motivo para poder acceder a información existente

en bases de datos (bancos) y con la cual sea posible demostrar la participación de esa persona en una conducta punible investigada, el ente investigador deberá coordinar previamente con un juez con control de garantías, se autorice el acceso a dicha base de datos y una vez se obtenga la información, deberá informarse la recepción de la misma, dentro del os términos autorizados. Misma forma existen diferentes normas internacionales que en materia de seguridad de la información crearon estándares que permiten poner en ejercicio las mejores prácticas con las cuales se puedan desarrollar, implementar y mantener especificaciones para la seguridad de la información, entre esas normas tenemos: ISO/IEC 27000, ISO/IEC27001, esta última es una certificación que acredita el cumplimiento de los requisitos para la implementación de un sistema de gestión para la seguridad de la información en una organización, y mediante esta se promueve la mejora continua de los procesos de la organización. Y como país hacemos parte de los países que pertenecen al convenio de Budapest firmado en noviembre de 2001, mediante el cual se hicieron unas precisiones en materia criminal y que los países deben tener como referente para la aplicación de normas y estrategias de seguridad. Y como ya se ha dicho, la única ley que regula, castiga y sanciona los delitos informáticos y algunas de sus modalidades, es la ley 1273 de enero 05 de 2009, dentro de la cual tenemos 10 artículos, uno de los cuales tiene circunstancias de agravación punitiva y permite que, por la modalidad de ejecución de la conducta, la pena pueda aumentar, evitando de esta manera que el delincuente informático pueda quedar en libertad por la pena impuesta. Dicha ley está dividida en dos capítulos el primero con 8 artículos y protege la información y los datos, en los delitos existentes en dicho capitulo encontramos algunos cuya tasa de condena es igual o inferior a los 3 años por lo cual sería posible como medida de detención la vivienda y otros cuya condena puede ser superior a los 4 años, así mismo en el capítulo II de la misma ley tenemos el hurto por medios informáticos y la transferencia no consentida de activos, siendo estos dos artículos, de los que más pena de prisión pueden aplicar, recurriendo a las circunstancias de agravación punitiva, las cuales según la modalidad utilizada puede aumentar la condena. Es

de anotar que el hurto por medios informáticos y semejantes, tipificado en el artículo 269i, es la conducta que a nivel nacional más casos tiene denunciados, teniendo en cuenta que los delincuentes informáticos, normalmente buscan obtener dinero ilícito, y esta es una de las formas más rápidas para obtenerlo, con la modalidad del cambiazo o clonación de tarjetas.

CONCLUSIONES A lo largo del trabajo, en materia de delitos informáticos se pudo concluir que en Colombia se encuentran tipificadas algunas modalidades o técnicas para la realización material del delito, que afectan las bases de datos y la información, sin embargo existen ciertas técnicas que son de mucha tecnología que son de difícil comprensión en materia de ciberdelincuencia, es decir su tipificación positiva en una norma es ardua, inclusive su desvaloración jurídica de resultado en una norma que comprenda y sancione de manera específica un tipo de conductas que ponga en peligro los bienes jurídicos tutelados, es muy compleja, por el mismo sentido de ser algo novedoso en la actualidad, que se sale de las conductas tradicionales, utilizadas por los delincuentes. De la misma forma, cabe mencionar que a pesar de su tipificación y sanción de las conductas que afecten las bases de datos y la información, el estado en materia de política criminal ha procurado compilar las diferentes técnicas utilizadas por los delincuentes, con el fin de agrupar y proteger todo tipo de afectación a los derechos fundamentales como lo son la intimidad, la dignidad, la honra, el patrimonio y todos aquellos derechos que son potencialmente vulnerables a través de las herramientas tecnológicas, tal como vio a lo largo del trabajo. En el mismo orden de ideas, por tratarse de conductas relacionadas con instrumentos tecnológicos para cometer ilícitos, se concluye que la apreciación de estas técnicas y la imputación de aquellas es más compleja por el desconocimiento y falta de preparación por parte de los actores de la justicia penal. Es necesario que a nivel nacional, se procure con la inversión y preparación de políticas que instruyan a los funcionarios en materia de delitos informáticos, porque éstos

pueden ser más peligrosos, habida cuenta que su materialización es a través de estos medios, imposibilitando significantemente la individualización de la participación de la conducta penal. De lo anteriormente planteado, se puede concluir que las formas de participación en la comisión de un hecho punible es de mayor cuidado, toda vez que hay que presumir si se hace en la calidad de autor o participe en los delitos informáticos y su calificación jurídica es el tema En efecto, el problema principal es el poco conocimiento frente a estos temas, el desarrollo social, el cambio constante de la sociedad, el avance tecnológico sin medida, el cambio de generaciones y la actualización permanente de las normas al desarrollo inquebrantable, por parte de los actores jurídicos. La escena virtual es una de las más apetecidas en la actualidad para cometer sus actividades delictivas, pues la delincuencia va en aumento, toda vez que es una modalidad de mayor facilidad para perpetrar sus cometidos, sin ser encontrados de manera inmediata y por ende pensaría que se torna más complicada la flagrancia de un ciberdelincuente, por el modus operandi en que operan, entonces se puede concluir que en materia de delitos informáticos va en aumento, y necesita un cuidado muy detenido por parte de la política criminal del estado, inclusive un consenso con los demás países.

AUTOR DEL RAE 233006_2

Delitos informáticos y entorno jurídico vigente en Colombia

AUTOR Jorge Eliécer Ojeda-Pérez-Miguel Eugenio Arias-Flórez-Fernando Rincón-Rodríguez & Libardo Alberto Daza-Martínez

FICHA BIBLIOGRÁFICA OJEDA, Jorge – ARIAS, Miguel – RINCÓN, Fernando & DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. No 11 (28) (Ene – Jun 2010); p. 41 – 66.

PALABRAS CLAVE Seguridad informática, delitos informáticos, cibercrimen, sistemas de información, entorno jurídico.

PALABRAS DESCONOCIDAS

FUENTES 33

CONTENIDO DEL RAE El documento describe y analiza la evolución y el marco conceptual de los delitos informáticos planteados por diferentes autores nacionales e internacionales, y establece la relación con la reciente Ley 1273 de 2009, mediante la cual la legislación colombiana se equipara con la de otros países en cuanto a la normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales. El ciberdelito, como tendencia que incide no sólo en el campo tecnológico sino también en el económico, político y social, debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de nuestras organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática. Con mayor frecuencia y mayor impacto, los dispositivos de almacenamiento y procesamiento de información llámense servidores, estaciones de trabajo o simplemente PC son vulnerados en sus elementos más sensibles, dejando expuestos no sólo múltiples y significativos datos de distinto valor (financiero, crediticio, estratégico, productivos), sino los mismos patrimonios reales de personas y organizaciones y, aún más, su dignidad, su honra y su vida. Con el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social y empresarial, han surgido comportamientos ilícitos llamados de manera genérica delitos informáticos, que han abierto un amplio campo de riesgos y también de estudio e investigación, en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática. En este documento se describen los antecedentes y el origen del fenómeno en su dimensión delictiva, junto con el concepto de diversos autores y autoridades nacionales e internacionales que han estudiado y enfrentado el tema y que hoy sirven de apoyo para contextualizar su impacto en el ámbito informático y jurídico y, por supuesto,

en el social y económico. A partir del acelerado incremento en las posibilidades de interrelación global por el uso de la comunicación satelital (la internet, el correo electrónico, los teléfonos celulares, las redes sociales), las personas y las organizaciones privadas y públicas han quedado expuestas, por las vulnerabilidades de los sistemas de intercomunicación y manejo de la información y por la falta de preparación y de cuidado en su uso, al progresivo y peligroso impacto de la ciberdelincuencia, con los sistemas informáticos ha ocurrido algo similar a lo observado en la historia. El hombre vive cada vez más interesado y condicionado por la informática, debido a su vertiginoso desarrollo y a la enorme influencia que ha alcanzado en muchas de las actividades diarias de las personas y las organizaciones. Pocas personas, en la actualidad, pueden abstraerse del contacto directo o indirecto con un sistema de cómputo, lo cual muestra de distintas maneras el poder y alcance de la tecnología informática en las sociedades del mundo. Así como la tecnología y su desarrollo han incidido en prácticamente todas las actividades del ser humano a lo largo de su historia, en la actualidad, la dependencia tecnológica ha venido concentrándose cada vez más en el fenómeno de la tecnología informática, la información y la comunicación. Con efecto retardado, se descubrió luego que ese desarrollo venía acompañado de distintos y también novedosos riesgos. La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la Ley de Delitos Informáticos, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas. Las herramientas de los ciberdelincuentes han evolucionado si no más rápido, por lo menos paralelamente al desarrollo tecnológico, como ha venido sucediendo con los virus informáticos.

En un comienzo, los ciberdelincuentes infectaban los equipos de sus víctimas al transportar mano a mano los virus desarrollados, en los medios de almacenamiento de información disponibles en ese momento: los disquetes. Más tarde, utilizaron las redes de datos al aprovechar la internet, pero encontraron la barrera de las restricciones de acceso para evitar contagios. De nuevo, regresaron a la difusión contaminante mano a mano al emplear las memorias móviles con puerto USB y arreciaron los bombardeos de malware1 en el internet. De igual manera, los ciberdelincuentes han utilizado el correo electrónico y los chat rooms o salas de conversación virtual de internet para buscar presas vulnerables. Pero además de los delincuentes informáticos, otros tipos de delincuentes han encontrado espacios propicios en los distintos medios de comunicación electrónica, para desarrollar sus crímenes, como los pedófilos que buscan generar relaciones de confianza online con niños inocentes, para luego aprovecharse de ellos y hasta secuestrarlos o asesinarlos. Estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, de drogas, de personas, de pornografía, de información, sicarios y terroristas se agregan a esta tenebrosa lista que utiliza el ciberespacio y la red para multiplicar sus negocios, sus ilícitas ganancias y sus manifestaciones criminales. Con ese antecedente, las entidades que desarrollaban o trabajaban en los escenarios informáticos del mundo, comenzaron a generar instrumentos de control y sanción a quienes en forma inescrupulosa utilizaban la informática para delinquir. Sin embargo, se encontró que los entes encargados de sancionar a quienes hacían uso ilegal y delictivo de las herramientas informáticas, no tenían cómo judicializar a los nuevos delincuentes. La ley inglesa sirvió para que otros países en especial aquellos donde el internet tenía más desarrollo se sumaran al esfuerzo de discutir y promulgar leyes orientadas a proteger y sancionar la violación de la información.

CONCLUSIONES Los acelerados procesos de globalización con sus innumerables y cada vez más sorprendentes atractivos y posibilidades para la

humanidad entera, impulsados todos por el avance tecnológico de las comunicaciones y la informática se han convertido en el nuevo paradigma de las relaciones personales, organizacionales, locales e internacionales, del conocimiento y el desarrollo. Pero tan importante y dinámico cambio que ha condicionado los nuevos comportamientos sociales, económicos, políticos y éticos de las personas y los pueblos, ha venido acompañado de un no menos dinámico y, a la vez, peligroso proceso de una nueva delincuencia que, al utilizar o impactar los sistemas de información y comunicación de las organizaciones y el mundo, ha llegado a posicionarse como uno de los cada vez mayores peligros para la seguridad, la honra, vida y bienes de las personas y las organizaciones de todos los países. Frente a esos dos fenómenos: el positivo o neutro de la globalización por la tecnología, la información y las comunicaciones, y el negativo de la ciberdelincuencia, las organizaciones y algunos gobiernos del mundo han venido tomando conciencia de la perspectiva de futuro y la subyacente amenaza, para actuar mancomunadamente y construir barreras no sólo tecnológicas, sino también jurídicas y sociales que permitan enfrentar con probabilidades de éxito ese gran mapa de riesgos generado por los delitos informáticos. Como consecuencia, se han diseñado, divulgado y aplicado no sólo modelos, sistemas, herramientas y procedimientos de seguridad informática, sino también el necesario complemento legal para combatir el delito, además de la capacitación y preparación especializada para manejar estos componentes de seguridad, de manera integrada y cada vez más generalizada entre la sociedad. En Colombia, con algunos antecedentes de carácter jurídico (sobre la base de los derechos de autor) y alguna normatividad complementaria (Código Penal y circulares de la Superintendencia Financiera), en 2009 se logró expedir la Ley 1273, con la cual pudo acceder al grupo de países que se han preparado con herramientas más eficaces para contrarrestar las acciones delictivas del cibercrimen, en sectores claves de la sociedad como el financiero, cuyas condiciones de vulnerabilidad son las más estudiadas e investigadas por los delincuentes informáticos. En el contexto mundial observado, las tendencias del cambio caracterizadas y

aceleradas por las tecnologías de la información y la comunicación han venido aparejadas con las tendencias delictivas, ahora caracterizadas como ciberdelito entre cuyos gestores y dinamizadores en el mundo, se encuentra gente preparada, estudiosa, investigativa y con gran poder de mimetización en el ciberespacio. Frente a eso, los países más afectados, en general, y Colombia, en particular, han desarrollado distintos mecanismos tecnológicos y también jurídicos para actuar en los escenarios del cibercrimen, entre los cuales el sector financiero es uno de los más amenazados. Por esta misma razón, sus condiciones de vulnerabilidad y gestión del riesgo informático pueden señalar un derrotero para orientar las normas, políticas, estrategias y procedimientos que permitan enfrentar tal amenaza y velar por la seguridad de toda la sociedad, puesto que ella no sólo va dirigida a un sector en particular, sino a todas las actividades del mundo en las que se muevan recursos financieros. En una primera observación general, puede decirse que las condiciones de seguridad del sistema financiero, visto por los resultados de las 17 entidades encuestadas, presentan distintas condiciones de riesgo que llevan a concluir que la confiabilidad no está plenamente demostrada, bien porque no se ha generalizado una conciencia integral del fenómeno y su negativo impacto, o porque los riesgos y amenazas, por el medio en el cual se desarrollan, siguen sin estar identificados en todo su espectro, o porque ha faltado coherencia en el aparejamiento de los sistemas de seguridad a los riesgos previstos, o porque los instrumentos apropiados también permanecen desconocidos, o porque se mantiene la pobre noción de las herramientas técnicas, jurídicas y sociales para enfrentarlos, en fin, entre otras muchas razones, porque las estrategias diseñadas siguen limitadas o son insuficientes para generar cultura de la seguridad informática en las instituciones, en las organizaciones y en la sociedad. Si bien el sector analizado reconoce la importancia de la planificación de la seguridad informática, tal reconocimiento no es suficientemente coherente con las técnicas, herramientas y procedimientos aplicados y menos con la preparación del talento humano para garantizarla, ni con la inversión destinada al efecto. No basta con planear y nombrar responsables si en el direccionamiento no se

incorpora el desarrollo integral del sistema de seguridad que genere una cultura apoyada desde las propias capacidades y fortalezas internas: las existentes y las que es necesario preparar y consolidar, junto con el conocimiento, la conciencia clara y el aprovechamiento efectivo del apoyo existente en las fuerzas externas del Estado, de la Ley y de la sociedad misma, además de las entidades que internacionalmente trabajan el tema. Éste es un reto colectivo. No es solamente para las organizaciones o las personas que están en la mira permanente de los ciberdelincuentes. Es un desafío para la sociedad y el Estado, para los jueces y los administradores de justicia, que deben estar preparados no sólo en el conocimiento de la Ley y la jurisprudencia, sino en el apropiado conocimiento del contexto tecnológico, informático y de sus proyecciones delictivas. No obstante, las observaciones corresponden a una muestra de un sector específico, por las condiciones de ese sector y su impacto en toda la sociedad, no es exagerado destacar que el reto del cibercrimen, ante las condiciones para enfrentarlo (vistas en el sector tal vez más significativo para observarlo), implican un reto a las propias condiciones de supervivencia y desarrollo de las personas, las organizaciones y las instituciones del país y del mundo. No se puede subestimar su poder, complejidad y alcance que puede llegar no sólo a los recursos, propiedades y derechos, sino de las posibilidades de vida. No basta con formar grupos de defensa o ataque al cibercrimen, si no se construye la conciencia organizacional y ciudadana de la seguridad informática, como parte integral de la cultura de mejoramiento de las condiciones de vida de la gente.

AUTOR DEL RAE 233006_2

El delito de acceso abusivo a sistema informático

AUTOR Ricardo Posada Maya

FICHA BIBLIOGRÁFICA POSADA, Ricardo. El delito de acceso abusivo a sistema informático. En: Revista de derecho comunicaciones y nuevas tecnologías. No 9 (Jun. 2013); p. 1-31.

PALABRAS CLAVE Acceso abusivo, sistemas informáticos, medidas de seguridad informáticas, intimidad personal informática, delitos contra la seguridad de los sistemas informáticos, los datos y la información.

PALABRAS DESCONOCIDAS Demoliberal.

FUENTES 55

CONTENIDO DEL RAE En el Código Penal colombiano prevé en el artículo 269A el delito de acceso abusivo a sistema informático que, además de proteger directamente la seguridad integridad y disponibilidad de los sistemas informáticos e indirectamente los datos y la información informatizada, como bien jurídico colectivo, también resguarda el derecho constitucional fundamental a la intimidad personal informática (CN, art. 15). En este artículo académico se realizó un análisis breve de esta importante figura criminal, estudio los bienes jurídicos protegidos por la norma citada y precisa los elementos objetivos y subjetivos que la estructuran en el CP vigente.

Una de las figuras ampliamente modificadas por ley 1273 fue el delito de acceso abusivo a sistema informático. Tipo penal pionero en nuestro medio jurídico que inicialmente fue regulado por el art. 195 del CP4 —dentro del capítulo VII, título III, dirigido a castigar La violación de la intimidad, reserva e interceptación de comunicaciones—, y que en esta oportunidad fue incluido en el art. 269A, dentro de las figuras que castigan especialmente “Los atentados contra la confidencialidad, la integridad y la disponibilidad delos datos y de los sistemas informáticos” que los contienen, procesan o transmiten en forma automática. Con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques

cibercriminales, como figuras autónomas frente a los tipos penales tradicionales. Sin embargo, la evolución del mencionado art. 269A no ha sido pacífica. En efecto, el cinco de marzo de 2009, esto es, dos meses después de entrar en vigencia la “ciber-reforma”, el Gobierno Nacional sancionó la L. 12886 —mediante la cual se expidieron normas para fortalecer el marco legal que permite garantizar la reserva de la información derivada de acciones de “inteligencia y contrainteligencia”— que, con evidente falta de planeación legislativa, revivió y modificó, en el art. 25, el invalidado art. 195 CP7 y derogó los arts. 4° y 269A adicionados por la reciente L. 1273 de 2009. Para completar el diagnóstico, debe decirse que la L. 1288 de 2009 fue declarada inexequible por la Corte Constitucional mediante sentencia C-913 de 2010, debido a evidentes vicios de procedimiento en su formación (reserva de ley estatutaria), que de nuevo dejaron vigentes los arts. 4° y 269A de la “ciberreforma”.

La cibercriminalidad cubre aquellas conductas punibles realizadas con fines ilícitos, no consentidas (facultadas) por el titular de la información o los datos, o abusivas de este consentimiento (facultad), que se orientan a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática de programas de datos o información informatizada reservada o secreta de naturaleza personal (privada o semiprivada), empresarial, comercial o pública, que pongan en peligro o lesionen (CP/art. 11) la seguridad de las funciones informáticas en sentido estricto, esto es, la confiabilidad (calidad, pureza, idoneidad y corrección), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de la programación de los equipos informáticos o de los programas operativos o aplicativos (software). Por consiguiente, no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos.

Según el Informe de ataques contra sistemas informáticos comparado 2011-2012, identificado: OFPLA-DIPON-109, consultado en: www.policia.gov.co, del 17 de octubre de 2012, la Policía Nacional reportó que, en Colombia, durante este período, fueron presentadas 1985 denuncias penales por cibercrímenes, de los cuales 1191 fueron realizados utilizando la Internet; siendo las ciudades más afectadas: Bogotá, Cali y Barranquilla. Los delitos más cometidos fueron los hurtos por medios informáticos y semejantes, y el acceso abusivo a sistemas informáticos (delitos propiamente informáticos). Las tendencias del informe también señalan que, de las 1985 denuncias, 311 fueron accesos abusivos a sistemas informáticos, y produjeron 26 capturas.

En el ordenamiento penal colombiano, a diferencia de otros ordenamientos penales como el español, el italiano o el alemán, el delito de acceso abusivo a un sistema informático no se clasifica como una modalidad de espionaje informático (porque no se exige de lege data el conocimiento o la disposición de datos: 'cracking malicioso') ni del delito de violación de habitación ajena, por más que, en el último caso, se trate de equiparar los conceptos de sistema informático y domicilio, con el argumento —por cierto muy dudoso— de que se busca proteger el domicilio informático del titular del bien jurídico. No es claro que tal cosa sea posible en el ámbito virtual, como un concepto distinto a la noción de dominio informático, una vez identificado los aspectos de la ley de delitos informáticos es impórtate aclarar los siguientes conceptos: sujeto activo cualquier persona natural que realice la acción propia del tipo penal de acceso abusivo a sistema informático, sin que este requiera alguna calificación especial. Dicho en otras palabras, el sujeto no tiene por qué ser un hacker o un cracker profesional, basta que sea un "intruso" y se cumplan las exigencias jurídicas para ser calificado como autor. Sujeto pasivo: solo pueden ser sujetos pasivos de este tipo penal aquellas

personas que sean, por una parte, el titular del medio informático que resulta objeto del acceso o mantenimiento abusivo, que incluso puede ser una persona jurídica, y, por la otra, el titular de los datos personales, sensibles o secretos almacenados en archivos o bases de datos, y cuya intimidad personal se pone en peligro, Objeto jurídico: el objeto jurídico del tipo penal de acceso abusivo a sistema informático consiste en proteger, en concreto, el derecho o facultad de control del titular sobre la integridad y seguridad del sistema informático, el derecho personalísimo a la autodeterminación informática, y a ejercer, de aptitud, apreciable también en concreto, para desvelar esos aspectos de la vida de una persona.

CONCLUSIONES El delito de acceso abusivo a sistema informático previsto en el CP, art. 269A, no es un delito común sino un cibercrimen caracterizado por exigir especiales formas y métodos de ejecución propiamente informáticos, contra objetos medio inmateriales (sistemas informáticos), realizado por sujetos que usualmente tienen perfiles criminológicos muy precisos. Su interpretación siempre gravita en torno de un bien jurídico autónomo (colectivo-individual) definido como la seguridad, integridad y disponibilidad de la información, los datos y los sistemas informáticos. Actuación que puede vulnerar otros bienes jurídicos, como sucede con la intimidad personal informática (Boix Reig & otros, 2010, p. 457). El legislador penal colombiano ha empleado una técnica legislativa muy discutible al consagrar los delitos de intrusión informática, al menos por tres razones. En primer lugar, porque la norma se aparta de dos aspectos sugeridos por la doctrina en esta materia, lo que refuerza la desventajosa naturaleza de la descripción típica como un delito de mera conducta, lesión contra el sistema informático y peligro potencial para los datos y la autodeterminación informática. En segundo lugar, la eliminación de las medidas de seguridad informáticas dispuestas para limitar el acceso de terceros al sistema informático. Aspecto que resquebraja el principio de autorresponsabilidad del titular del sistema y condiciona la aplicación de figuras

como la autopuesta en peligro, cuando se trata de estudiar la imputación objetiva, tal y como ha quedado dicho a lo largo del texto. Desde un punto de vista subjetivo, el tipo penal parece configurar una cláusula general, toda vez que no exige la ejecución del acceso o del mantenimiento abusivo con una finalidad ilícita ulterior, como lo sería, por ejemplo, el ánimo de lucro, el propósito de violar, interceptar, borrar, copiar o sustraer datos personales del sujeto pasivo o de terceros que se encuentren almacenados en el sistema informático. De algún modo, la precisión de dichos elementos subjetivos permitiría acotar la clase de peligro típico requerido contra el bien jurídico en su aspecto individual, es decir, la intimidad y autodeterminación informáticas. Del mismo modo, el poder sancionar actuaciones sin alguna finalidad específica permite tipificar los casos, en principio inofensivos, de hacking blanco realizados por adolescentes o por personas que solo buscan, por motivos intelectuales o por el simple reto, desafiar las seguridades de un sistema informático determinado. Lo que comporta una extravagante anticipación de la barrera de protección del bien jurídico protegido. En tercer lugar, el tipo penal fue diseñado como una conducta de lesión frente a la integridad del sistema informático y de peligro en abstracto para la intimidad informática. Peligro que se puede interpretar, en los términos del art. 11 Ricardo Posada Maya Junio de 2013 - Universidad de los Andes - Facultad de Derecho - Revista de Derecho, Comunicaciones y nuevas tecnologías. GECTI N° 28 9 del CP, como un peligro concreto contra la reserva o intimidad informática del sujeto pasivo, cuando la intrusión suponga la posibilidad fáctica —al menos un instante— de obtener servicios, causar daño o disponer de la información sensible existente y retirarla de aquel. De todas maneras, este tipo de regulaciones quiebra el andamiaje demo liberal dispuesto por el CP y por los sistemas de juzgamiento en nuestro medio, que se basan en la posibilidad de discutir la imputación, su ofensividad y la culpabilidad por la realización del hecho.

El delito de transferencia no consentida de activos

AUTOR Ricardo Posada Maya

FICHA BIBLIOGRÁFICA POSADA, Ricardo. El delito de transferencia no consentida de activos. En: Revista de derecho comunicaciones y nuevas tecnologías. No 8 (Dic. 2012); p. 1-27.

PALABRAS CLAVE Fraudes informáticos, delito informático, trasferencia no consentida de activos, delitos contra la seguridad de la información.

PALABRAS DESCONOCIDAS Insider.

FUENTES 49

CONTENIDO DEL RAE Mediante el presente documento, el autor hace un análisis del artículo 269j tipificado en el capítulo II de la Ley 1273 de enero 05 de 2009. Con la añadidura realizada al Código penal Colombiano mediante el cual le adicionaron nuevos tipos penales, relacionados con delitos informáticos y los cuales se ejecutan mediante redes de telecomunicaciones, la nación aplicó las recomendaciones realizadas en el convenio de Budapest, mediante el cual se consideró la inclusión de normas sancionatorias a las acciones realizadas utilizando los medios informáticos, permitiendo de esta manera que no solo se proteja la información reposada en diferentes bases de datos de las organizaciones o unidades familiares, uno también el dinero existente en cada una de las cuentas bancarias. Dicha ley surge mucho tiempo después de que en la Unión Europea se diera a conocer normatividad existente para castigar dichas actividades delincuenciales. La doctrina especializada tiene dos conceptos que en ningún momento pueden confundirse, uno de ellos es la criminalidad informática y el otro es la cibercriminalidad. El primero hace relación a aquellas conductas que con ocasión a su ejecución, circunstancialmente hicieron uso de alguna red de telecomunicaciones, por lo que también existe un agravante en la ley 1273 en el cual establece que la pena aumentará si la conducta es realizada utilizando un medio informático, electrónico o telemático. Mientras que la cibercriminalidad si enfoca todas aquellas actividades delictivas que sean utilizadas y pongan en peligro la seguridad de las funciones informáticas de algún sistema, esto es la

confidencialidad, integridad y disponibilidad de la información; estas conductas delictivas no podemos llamarlas delitos comunes, pues si bien es cierto para su realización es necesario realizar algún procedimiento informáticos con cierta riqueza técnica, que no cualquiera puede tener. Penalmente existen algunos términos que la ciudadanía no entiende, por eso en este documento se los explicaré y daré a conocer el enfoque que tiene cada uno de ellos en el ámbito jurídico. Bien Jurídico Protegido, es el bien que protege el artículo en este caso la protección de la información y de los datos, lo que permite proteger la seguridad, disponibilidad, control, autenticidad, integridad de la información y los datos. Teniendo en cuenta lo descrito anteriormente y que el objetivo del documento es realizar un análisis al artículo 269j de la Ley 1273 de 2009, es un delito tipificado como ataque informático, cuya pena puede estar entre los 4 y 10 años y una multa de 200 a 500 salarios mensuales vigentes. Sujeto activo: es aquella persona capaz de realizar la acción delincuencial sin requerir o poseer conocimientos técnicos en este caso en materia informática; en algunas ocasiones el sujeto activo puede llegar a ser el administrador de una red de comunicaciones. Teniendo en cuenta que el artículo 269h agrava las modalidades delictivas y en ejemplo expuesto anteriormente, si el administrador hace parte de una empresa del estado y se le encuentra participación activa en el delito, su pena podría aumentar, al igual que como sanción se le impediría ejercer labores sobre sistemas de información procesados con equipos informáticos. Sujeto Pasivo, en este caso el sujeto pasivo es la persona titular del bien jurídico o a quien se le autorice mediante poder y también la persona titular del medio informático que resultara afectado con la acción, normalmente son personas jurídicas, entidades bancarias. Bien jurídico, descritos anteriormente y tal como lo exige el tipo penal. Objeto jurídico, la facultad que tiene el sujeto pasivo para acceder, disponer, sobre sus datos e información que se encuentre informatizada. Objeto sobre el cual recae la acción, los datos que pueden representar activo patrimonial ya sean bienes o derechos con valor propietario, que se reflejen en la contabilidad de una empresa. Verbo rector simple, acción efectuada por el sujeto activo de la conducta

y que se encuentre tipificada en el artículo que describe la conducta ilícita realizada. Resultado, en este caso pasa a ser la transferencia no autorizada, no consentida por su titular. Es importante aclarar que la transferencia no puede ser consentida y su efecto conlleva al a despatrimonialización efectiva del sujeto pasivo (victima); al igual que la ley no protege al sujeto pasivo frente a fallas del sistema, ya que estas resultarían siendo atípicas por no estar descritas en ningún artículo. De esta manera y luego de explicar algunos conceptos jurídicos y que tiene bastante relación con la aplicabilidad de la ley 1273 de 2009 frente las diversas conductas, modalidades y tipos que existen en la actualidad, es posible encontrar que luego de realizada una transferencia con consentida de activos, puede surgir un nuevo delito asociado al anterior, pues teniendo en cuenta que la acción de la transferencia culmina cuando por ejemplo, el dinero es transferido a una cuenta bancaria sin autorización del titular y/o cuando es ejecutada mediante fraudes (phishing); cuando ese dinero es retirado o utilizado para cualquier tipo de gastos, aplica una modalidad delictiva existente en la Ley 1273 de 2009 conocida como hurto por medios informáticos y semejantes, tipificadas en el artículo 269i y que por su pena ser superior a la tipificada en el 269j, ya que por la modalidad utilizada ser agravada según lo contemplado en el numeral 17 del artículo 58 del Código Penal Colombiano, su pena aumenta y al ser superior a lo dispuesto para el artículo 269j, la de mayor pena es la que el ente judicial debe tipificar ya que la pena menor cede ante la mayor, en el caso que el dinero no sea utilizado, el hurto por medios informáticos quedaría en modalidad tentativa.

CONCLUSIONES Los delitos informáticos de naturaleza económica están a la orden del día. El legislador de 2009 los consagró con el fin de evitar transferencias o apropiaciones masivas de fondos y activos de cuentahabientes, dada la precariedad dogmática de los tipos penales tradicionales para castigar esta clase de comportamientos delictivos. Actuaciones cuya ocurrencia genera una creciente desconfianza en los sistemas legales y de seguridad vigentes para proteger el

patrimonio económico en el tráfico automático de pagos o transacciones financieras. Por ello, no se trata de tipos delictivos comunes. Su naturaleza y el bien jurídico protegido permiten interpretarlos como verdaderos tipos penales autónomos que protegen la seguridad de la información informatizada (bien jurídico colectivo e intermedio) y, en particular, las funciones informáticas referidas a la protección de ciertos bienes personales o personalísimos. El legislador penal colombiano ha empleado una técnica legislativa muy discutible al consagrar los tipos penales que buscan proteger la seguridad de la información y el patrimonio económico. Por una parte, resulta cuestionable el empleo excesivo de elementos normativos a la hora de crear los tipos penales, cuya interpretación es objeto de una viva polémica por parte de la doctrina dominante. Es justamente lo que sucede con los conceptos de “manipulación”, “artificio semejante” y “transferencia”, que no encuentran un sentido y unos efectos unívocos cuando se trata de acotar el alcance del tipo penal de transferencia no consentida de activos. Todo ello en franca violación del principio de taxatividad penal (CP/art. 10). Por la otra, es claro que no está justificada la implantación típica hecha por el legislador, que ha copiado sin mayores reflexiones dogmáticas y político criminales la norma penal vigente en el CP español (ref. 1999), prevista en el art. 248.2, con todos los problemas que ella tiene, que ahora quedan reflejados en nuestro ordenamiento jurídico. Por ello, para una mejor protección de los bienes jurídicos, en el texto se opta por acoger un concepto amplio de manipulación informática, que permita incluir aquellos actos defraudatorios que, con claridad, no quedan cubiertos por el alcance normativo de tipos penales ordinarios o especiales como la estafa, el hurto por medios informáticos o el hurto calificado. En el mismo sentido, se defiende una noción mercantil o contable del concepto de transferencia, sin desconocer que esta es una noción imperfecta para hipótesis límite, cuando el momento de la anotación contable no coincida con el momento de la operación comercial o financiera. Igualmente, para el autor resulta muy difícil defender la hipótesis de Tenencia de elementos peligrosos prevista en el mismo CP/art. 269J, pues no solo resulta de peligro en abstracto y pura peligrosidad objetiva y

presunta, lo que contradice el CP/art. 11, sino también porque su prueba es muy difícil, dada la redacción de la figura típica. Se trata, pues, de una norma expansiva e ilegítima, que contradice los principios liberales de nuestro ordenamiento jurídico penal, por lo que puede tacharse de inconstitucional (CN/art. 4°).

AUTOR DEL RAE 233006_2

Comisión de conductas punibles en el internet en Colombia.

AUTOR Sandra Patricia Suarez León

FICHA BIBLIOGRÁFICA SUAREZ LEÓN, Sandra. Comisión de conductas punibles en el internet en Colombia. Bogotá, 2012, 53 p. Tesis de pregrado (Derecho). Universidad Militar Nueva Granada, facultad de derecho.

PALABRAS CLAVE La Internet, Fraude, Tecnología, Conductas Penales.

PALABRAS DESCONOCIDAS

FUENTES 43

CONTENIDO DEL RAE Con ocasión al desmesurado avance tecnológico y sus repercusiones en todo el mundo, en Colombia fue necesario incorporar a la normatividad que existía nuevas conductas penales que permitieran que los casos presentados a nivel mundial y en el país, pudieran ser castigados de acuerdo a la conducta tipificada según su ocurrencia y modus operandi y no como sanciones o delitos clásicos; es así que al ser considerados los delitos informáticos como crímenes informáticos pues tienen su origen en los computadores, los cuales ya es común que sean utilizados para todo tipo de actividades personales, familiares, académicas, comerciales, laborales, conlleva a que por ser tan indispensables en las actividades diarias tanto de personas como de organizaciones, sea una herramienta de apoyo para la ejecución de conductas delictivas, ya que quien lo usa normalmente no toma las medidas de seguridad necesarias ya sea por

desconocimiento de las mismas o porque no sabe los riesgos a los que puede estar expuesto cada vez que utiliza un medio informático. Con el presente documento el autor busca explicar las nuevas conductas utilizadas por los delincuentes informáticos, cuyo fin sea delimitarlas en las diferentes líneas de investigación en Colombia y el análisis del convenio del consejo de Europa sobre el cibercrimen. El pasado noviembre de 2001, los países que hacen parte de la unión Europea, aprobaron el convenio conocido como convenio de Budapest, mediante el cual se regularon algunos parámetros que debían tener los países participes de él, para regular las conductas delictivas asociadas a los delitos informáticos, y el apoyo que deben prestar entre países; es así que varios integrantes de las diferentes ramas del derecho a nivel mundial, hicieron sus aportes en cuestión a la definición, pero de ese punto no pasaba al tema de normatividad. En Colombia a pesar del caso ocurrido en mayo de 1983 donde lograron transferir de cuentas del Banco de la republica más de 13 millones de pesos, no existía normatividad que regulara las actividades ilícitas realizadas utilizando los sistemas informáticos o que afectaran a los mismos, a pesar que en ese entonces solo dicho delito podía ser tipificado por el delito de violación a los derechos de autor, según lo tipificado en el artículo 51-4 de la ley 44 de 1993. Con ocasión al caso mencionado, surgió jurisprudencia mediante la cual se pronunciaban frente a algunos artículos existentes en leyes que podían tener incidencia alguna con algunas modalidades delictivas, pero no realizadas por medios informáticos, pues así lo decía la norma. En la Constitución Nacional de 1991, vigente hoy en día, tipificaron algunos artículos mediante los cuales buscaron frenar el poder informático para esa fecha, mediante la acción de tutela, lo que permite que toda información que se encuentre en bases de datos y le pertenezca a una persona, pueda ser actualizada, rectificada o cancelada. Fue tiempo después en el 2009, cuando entró a regular la Ley 1273 de 2009 por medio de la cual el gobierno empezó a perseguir los delincuentes informáticos y a castigar y sancionar sus acciones, pero así como surgió esta ley, surgieron nuevas modalidades delictivas que con relación a lo estipulado en dicha ley, quedaron en

el aire, pues existen muchos vacíos para su aplicación, representando esto un reto de mayores dimensiones para los organismos del estado principalmente aquellos que hacen parte de la rama judicial. Estas modalidades delictivas provocaron preocupación en el mundo, que conllevó a que varios países se unieran y firmara el ya mencionado Convenio de Budapest. La legislación colombiana protege la información y los datos y también de los atentados informáticos, norma que se dividió en dos capítulos, existiendo 8 en el primero y 2 en el último, estos actualmente los que mayor daño pueden causar, en términos económicos, pues están sumamente relacionados. Un delincuente informático posee unas características, y la más común es ser aquella acostumbrada a desafíos tecnológicos. El convenio de Budapest del cual hace parte Colombia, es una norma que regula como los países deben afrontar el delito informático, surgió como respuesta a todos los casos presentados en Europa y con ocasión al vacío jurídico que existía, pues estos delitos por ser informáticos, pueden pasar de lo local a lo transnacional; en él se incluyen tratados de asistencia internacional para apoyo mutuo en investigaciones, pero no son el punto final para parar estos delitos, ya que aún existen naciones en donde no existe normatividad que persiga, castigue y sanciones los delitos informáticos. Actualmente la Ley 1273 de 2009, tiene tipificados una serie de delitos que cuentan con muchos vacíos jurídicos y a su vez sus sanciones o penas son muy mínimas en cuestión de la conducta que pueda ejecutarse y del valor que se represente en la acción punible. Es por eso que se plantea de manera muy urgente, incorporar nuevas modalidades delictivas en dicha normatividad que permita perseguir cuanta clase delictiva exista y que sea realizada por redes de telecomunicaciones, con el fin de castigar y sancionar a quienes incurran en ellas; así mismo capacitar e incorporar más recurso humanos, capacitándolo primero, con el fin de agilizar los ´procesos investigativos, que desde el 2009 a la fecha, no son muchos los procesos sacados adelante (condenados), permitiendo de esta manera que el delincuente informático siga haciendo de las suyas, se incrementen las estadísticas, al igual que las cifras

negras, de aquellos casos ocurridos y que no aparecen en las estadísticas de la Fiscalía General de la nación y Policía Nacional.

CONCLUSIONES La primera observación que surge de esta investigación es que era necesaria una reglamentación más amplia de la temática, como sí se ha hecho en otras legislaciones del mundo, proporcionándole la debida y verdadera trascendencia normativa en sus países, ya que ese acceso al que se refiere la medida está introducido en el interés económico, pero también es importante porque vulnera la fe pública, como ejemplo se puede nombrar la modificación de una escritura pública electrónica, conducta punible que no tarda en consumarse, puesto que ya se legalizó el manejo del documento electrónico y solo faltaría reglamentar el trámite de esta clase de instrumentos con el registro civil. 2º. De la misma forma y mediante un análisis de las legislaciones que se han decretado en diversos países se demuestra que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras. También se establece que desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos, pero también es evidente que es difícil elaborar estadísticas sobre los diversos tipos de delitos. 4º. En relación con lo anterior, se puede afirmar que la cifra de delitos de esta naturaleza es elevada y es evidente que no es fácil descubrir sus autores y por lo tanto sancionarlos, en parte gracias al poder económico que tienen y que aprovechan para que a través de los actos que desarrollan mediante los delitos informáticos originar daños económicos incalculables, los cuales son indiferentes para la opinión pública. 5º. Se agrava además con el problema que quienes cometen este tipo de conductas no se asumen como delincuentes, no se les segrega, desprecia, ni desvalora, por el contrario, el autor o autores de este tipo

de delitos se consideran a sí mismos como "respetables" y enfrentan castigos como " objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad". En síntesis, se puede afirmar que la delincuencia informática se apoya en el delito organizado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aclarando que este no es el único medio por el cual se desarrolla. Las ventajas y las necesidades del flujo nacional e internacional de datos, aumenta incluso en países latinoamericanos, favoreciendo también la posibilidad que se incrementen estos delitos. Por lo mismo se caracteriza que la criminalidad informática constituye un reto desmedido tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

AUTOR DEL RAE 233006_2

Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación

AUTOR Juan David Rodríguez Arbeláez

FICHA BIBLIOGRÁFICA RODRÍGUEZ ÁLVAREZ, Juan. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. {En línea}. Fecha. {26 de mayo de 2017}. Disponible en http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

PALABRAS CLAVE Redes sociales, delitos informáticos, sistemas de información, entorno jurídico, vulneración de derechos.

PALABRAS DESCONOCIDAS Friendster, myspace.

FUENTES 8

CONTENIDO DEL RAE El desarrollo de las Tecnologías de la Información y de las Comunicaciones en nuestro país, ha traído consigo una serie de avances tecnológicos por medio de los cuales cada individuo puede realizar sus actividades por medio de dispositivos tecnológicos, actividades relacionadas con comercialización de productos, consultas académicas, entre otras, no solo en el ámbito local, regional o nacional, también puede hacerse con ámbito internacional. Cada quien es responsable de su comportamiento, a pesar que desde el 5 de enero de 2009 en Colombia entró en rigor la aplicabilidad de la Ley 1273 de 2009 más conocida como ley de delitos informáticos, mediante la cual se modificaron e incorporaron algunos nuevos delitos al Código Penal Colombiano y mediante los cuales se buscó castigar y sancionar a todo aquel que no cumpliera con lo estipulado en la normatividad. Con motivo de la integración que existe de la tecnología con el comportamiento humano, surgieron diversas paginas por medio de las cuales se puede estar en contacto con esos excompañeros de clase, de trabajo, y porque no de barrio, inicialmente conocidas como círculo de amigos, hoy en día conocidas como redes sociales. Mencionadas páginas surgieron en el año 1995 y se hicieron con el fin de encontrar esos viejos amigos tal como se explicó anteriormente, mencionadas paginas o redes sociales fueron mejorando a tal punto que para el año 2003 ya eran tendencia a nivel mundial y existían algunas ya llamadas redes sociales como por ejemplo Friendster, Myspace. Con la utilización masiva de estas redes sociales, inicialmente empezó a cumplirse el objetivo con el cual había sido creadas, encontrar viejos amigos, excompañeros, etc., empezaron a expandirse desmesuradamente pues día a día había mayor número de personas utilizándolas pues no existía distinción entre estratos sociales, religión, raza y que aparte de encontrar esos viejos amigos, ya se empezaba a compartir contenido, en muchas ocasiones académico. Hoy en día se han podido identificar tres grandes tipos de redes sociales, el primero de ellos enfocado a crear grupos de amigos, quienes anteriormente tuvieron algún acercamiento ya sea por índole académica, social, familiar; el segundo enfocados a un tema en particular como por ejemplo aquellas que comparten información de

algún tipo de deporte y el tercero con el fin de dar a conocer un trabajo o vender sus conocimientos profesionales. Teniendo en cuenta que por medio de las redes sociales, se realizaban actividades en donde existía intercambio de información, de conocimientos, se compartía información personal, de ubicación, de actividades realizada a diario, empezaron a surgir individuos que aprovecharon toda esta información compartida por los usuarios de las redes sociales permitiendo que surgieran acciones que atentaban contra la moral de sus integrantes, lo cual para ese entonces no se llamaría delito; ocurriendo que tal como se conoce de la historia nuestros antepasados, cuando descubrieron la utilidad que tenía el cuchillo en sus labores diarias, principalmente de caza o en el hogar, no faltó quien le dio un uso diferente que muy seguramente afectó a muchos de los pobladores de ese entonces. Hoy en día y con el aumento que ha presentado la tecnología en nuestras familias, ya existe una relación muy cercana con aquellos dispositivos (computador, celulares) que nos permiten tener contacto en tiempo real con aquellas personas que se encuentren en otro lugar y porque no en otro país, al igual que nos permiten obtener o compartir información en un momento dado. Existen herramientas que a medida que los avances tecnológicos han sido divulgados, también han creado y mejorado utilidades que permiten proteger al internauta de alguna acción delincuencia (delito informático), pero así como existen estas mejoras para la protección del ser humano, también el delincuente informático valiéndose de su conocimiento adquirido, ha ido creando nuevas modalidades con las que puede causar daño a quien haga uso de las tecnologías de información, en este caso redes sociales. Es así como empezó la difusión de software malicioso por medio de las redes sociales, correos electrónicos, o afectando lo equipos de cómputo existentes en las salas de internet, siendo los usuarios de estas últimas personas las presas más fáciles para aquellos delincuentes. Con esta modalidad el delincuente empezó a robar información confidencial de los internautas con el fin de empezar a generar extorsiones, estafas, por medio de las cuales pudieran obtener dinero para el sustento de sus actividades ilícitas; o también tráfico de armas, de drogas, de personas y porque

no, venta de información de posibles víctimas. Con ocasión a los problemas que ya se estaban generando por medio de las redes sociales, las entidades del estado empezaron a crear escenarios por medio de los cuales pudieran identificar a aquellas personas que utilizaran de forma equivocada los diferentes sitios informáticos, pero no contaban con las herramientas necesarias para castigar y sancionar estos delincuentes. De esta manera el estado colombiano empezó a fijarse en las leyes que existían en la Unión Europea pues no contaban con leyes que permitieran sancionar y castigar las acciones delincuenciales realizadas por los delincuentes informáticos, hoy en día conocidas como delitos informáticos, ya que a pesar de existir normatividad en la Constitución Nacional por medio de la cual el estado se encontrara en la obligación de proteger la intimidad de las personas, la libertad de las personas y para expresarse, la solución fue tardía para promulgar leyes que castigaran estas acciones. El pasado 5 de enero de 2009 entró en aplicabilidad la Ley 1273 en Colombia, por medio de la cual se sancionan algunas actividades delincuenciales realizadas por medios informáticos, lo anterior teniendo en cuenta que fue incluida en el convenio firmado en Budapest y que tiene vigencia desde julio de 2004, primer tratado internacional mediante el cual se busca hacer frente a los delitos informáticos de las naciones que pertenecen a él.

CONCLUSIONES En Colombia no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en Colombia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa. En nuestro país se deben diseñar políticas criminales encaminadas a prevenir la realización de estos delitos, políticas que tengan como base la enseñanza a la comunidad del correcto uso y manejo de las redes sociales para de esta forma minimizar los riesgos existentes en ellas. Los delitos informáticos son conductas que día a día se presentan en mayor cantidad en las redes sociales afectando gravemente derechos constitucionales prácticamente de todos los miembros de la sociedad. La

seguridad en las redes sociales y el suministro de información personal debe hacerse con todas las precauciones necesarias, y para que los usuarios de las redes tengan esta conciencia, los mecanismos y organismos del estado deben ayudar a crear una nueva cultura que conlleve a las personas a protegerse en este espacio digital que puede afectar fácilmente la vida e integridad de cada ciudadano. Las nuevas tecnologías de información y comunicación como las redes sociales además de ser el medio donde se presentan delitos como bullying, phishing, perfiles falsos, pornografía infantil, y toda clase de daños, fraudes y robos informáticos, también es el medio que están utilizando delincuentes comunes para llegar a la realización de delitos clásicos que se comenten personalmente como; secuestros, amenazas, estafas, acosos, hurtos, entre otros. El constante avance tecnológico y el avance de los delitos a la par de las nuevas formas de comunicación en el mundo no deben estar separadas de las correspondientes reformas y creaciones legales, nuevas normas que abarquen y contemplen las posibles vulneraciones a los derechos constitucionales para que las personas puedan tener opciones y medios dónde acudir para denunciar y protegerse frente a cualquier delito en las redes sociales.

AUTOR DEL RAE 233006_2

AUTOR DEL RAE 233006_2

La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio.

AUTOR Rodrigo Cortés Borrero, Jhon Alexander Ballén Rojas y Juan José Duque Montes.

FICHA BIBLIOGRÁFICA CORTÉS, Rodrigo - BALLÉN, Jhon & DUQUE Juan. La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. En: Revista de derecho comunicaciones y nuevas tecnologías. No 14 (Jul-Dic. 2015); p. 1-25.

PALABRAS CLAVE Criminología crítica, delitos informáticos, derecho penal especial, información y datos, Ley 1273 de 2009.

PALABRAS DESCONOCIDAS Asidero, rampante, albores, ínfimo,

FUENTES 39

CONTENIDO DEL RAE Mediante el presente artículo de revista, los autores quieren dar a conocer la persecución contra los delitos informáticos en el distrito judicial de Villavicencio. Teniendo en cuenta las conductas delictivas que empezaron a presentarse desde la década de los 80, el mundo empezó a enfrentarse a una nueva modalidad delictiva, los delitos informáticos; es por eso que, en Colombia, con más de dos décadas después de la primera alerta de conductas criminales relacionadas con delitos informáticos se sancionó una ley que castigue dicha modalidad delictiva. Tal como se indicó anteriormente, a mediados de la década de los 80 se consolidó el primer paso frente a una política penal que persiguiera los delitos informáticos, pero en Colombia solo se logró proteger en el año 1989, la propiedad de software, conocido como derechos de autor. Internacionalmente en el año 1992 se hizo una recomendación en Alemania, para que se promulgara nuevos tipos penales que pudieran perseguir los que no existieran en la Ley; años después en nuestro país y después de 2 intentos, se logró que fuera aprobado un proyecto de ley mediante el cual se logró incorporar nuevos tipos penales al Código Penal Colombiano, que permitieran perseguir la delincuencia informática, la cual protege al ciudadano la información y los datos y los ataques informáticos, quedando de esta manera a la altura de los países que para esa fecha hacían parte de la Unión Europea, ya que años atrás mediante el convenio firmado en Budapest, noviembre 2001, se dictaron normas

básicas que debían tener los países que hicieran parte de esa Unión, con el fin de protegerse de las modalidades existentes de delitos informáticos. La ley 1273 de 2009 fue un gran avance en materia de Ley para Colombia, pues transcurridos más de cinco años desde que se firmó el convenio de Budapest, no existía en el país normatividad jurídica que permitiera perseguir estas modalidades delictivas, al igual que existiera pisos jurídicos para la protección de la información existente en las diferentes bases de datos públicas o privadas. El delincuente informático surgió en paralelo con el desarrollo tecnológico, computador; pero sus herramientas si han avanzado más rápido que la tecnología, inicialmente sus actividades ilegales consistían en difundir virus a través de redes de datos y utilizando para ello disquetes, posterior empezaron a utilizar las memorias USB y con ellas a difundir software malicioso en las redes, al igual que encontrar victimas por medio de las salas de chat; también hay otra clase de delincuentes, pero en esta ocasión son aquellos que utilizando los medios de comunicación electrónica, encontraron lugar para su actividad ilegal, en este caso estafas, fraudes, proxenetismo, drogadicción, etc. Seis años después y teniendo en cuenta el desmesurado aumento de las diferentes conductas criminales asociadas a los delitos informáticos, el gobierno por medio del documento CONPES 3701 de 2011 (Política Publica de Ciberseguridad) y en coordinación del ministerio de las TIC, empezó a capacitar a entidades privadas sobre Ciberseguridad y seguridad de la información, al igual que dispuso la creación de tres grupos para la orientación ciudadana, siendo estos: COLCERT, Comando Conjunto Cibernético de las Fuerzas Militares y el Centro Cibernético Policial del cual depende el CAI virtual. Con el fin de lograr el objetivo principal de mi documento, la dirección de la Fiscalía seccional Villavicencio suministró una información previamente solicitada y en la cual me daban a conocer los procesos existentes, las personas condenadas, entre otras, por lo cual someramente se dan a conocer algunos puntos importantes de dicha respuesta. Durante el tiempo comprendido entre 2011 y 2012, se recibieron 114 denuncias, de las cuales solo fueron condenadas 6 personas, 32 procesos fueron archivados y 7 personas fueron imputadas o

acusadas. Con relación a los juzgados penales, se obtuvo información que 18 personas fueron condenadas por delitos informáticos, destacándose el hurto por medios informáticos y semejantes]; así mismo nos dieron a conocer que el delito más denunciado es el hurto por medios informáticos y semejantes mediante la modalidad de clonación de tarjetas, phishing y/o cambiazo de tarjetas. Con relación a la capacidad que tiene el CTI para enfrentar estas modalidades delictivas, de oficio nos respondieron que tiene un grupo especializado de fiscales para perseguir ese delito, la investigación de estos delitos requiere de personal profesional y capacitado y que los investigadores han sido capacitados por el gobierno de estados unidos, entidades privadas y por ellos en el manejo de herramientas forenses. Ahora, saliendo de las respuestas documentales, se le hizo una entrevista a la Directora Seccional de Fiscalía Villavicencio, quien nos manifestó que: el grupo de fiscales específicos no existe, pero si hay una unidad específica para ese tipo de delitos, el grupo de investigadores que investigan estos delitos, está compuesto por dos unidades, un ingeniero y un tecnólogo y que los investigadores de la unidad, también son peritos, lo cual conlleva a que tengan más carga laboral. Así mismo dio a conocer que no hay convenio con ninguna entidad ya que cada entidad bancaria es autónoma de dar su respuesta dentro de los términos legales y previa orden judicial. Analizando estadística suministrada por diferentes entidades del nivel público, es fácil decir que en Colombia existe una cultura de la no denuncia, lo que conlleva a que un sin número de casos ocurridos, no lleguen a las bases de datos y queden en la impunidad, permitiendo que de esta manera el delincuente siga invisible a la persecución penal. Lo que permite determinar que la ley 1273 de 2009 fue creada sin una perspectiva de largo plazo que tuviera en cuenta la inversión económica necesaria para la capacitación y actualización constante de quienes investigan estos delitos, o para herramientas forenses necesarias en la investigación.

CONCLUSIONES En el área penal del Distrito Judicial de Villavicencio existe una cifra negra que no está ampliamente registrada en las denuncias y sentencias. Esto se sustenta en la información suministrada por la Fiscalía General de la Nación, Seccional Villavicencio, y la obtenida del CTI, que denota que las personas tienen una negativa concientización de denuncia respecto a las conductas referidas a los delitos informáticos, situación que contrasta con las estadísticas a nivel nacional de empresas de seguridad privada. En el Distrito Judicial de Villavicencio es muy inferior el rango de denuncia frente a otros flagelos. Durante los dos años objeto de investigación se interpusieron 95 denuncias referidas a delitos informáticos: 65 en el 2011 con 19 archivos y 30 en el 2012 con solamente 5 archivos. De las denuncias interpuestas solo 9 terminaron en condena, es decir, existe una gran brecha que ha dificultado el proceso desde la denuncia hasta su terminación, y del mínimo número de investigaciones que culmina con una condena, esta por lo general no es privativa de la libertad, sino cualquiera otra sanción distinta. Muestra de ello es que en la mayoría de las judicializaciones los ciberdelincuentes siempre gozaron del beneficio de un subrogado penal. A la fecha de publicación de este informe, en el Distrito Judicial de Villavicencio solo hay una persona privada de la libertad en establecimiento carcelario. Frente a los anteriores datos, podemos afirmar que existe una serie de dificultades en el procedimiento judicial, que impiden una mayor efectividad de la norma penal sobre los ciberdelincuentes. A lo anterior se suman circunstancias como: - Los juzgados penales de conocimiento en Villavicencio sobre estos delitos son solo cuatro de categoría municipal. - El CTI carece de talento humano suficiente para adelantar una adecuada investigación referida a los delitos informáticos, en la totalidad del Distrito Judicial. - Cabe resaltar que se cuenta con una adecuada capacitación para el poco personal asignado a la investigación de estos delitos, dado que la unidad especializada está compuesta solamente por dos investigadores. Sin embargo, como bien nos fue expuesto por parte de la Unidad Especializada del CTI en cuanto a delitos informáticos, es compleja la investigación de algunos de los punibles

referenciados en la Ley 1273 de 2009 en cuanto al trámite que sugiere la norma en materia de acceso a las bases de datos, pues la exigencia de previa orden judicial impide una eficaz investigación debido a que los proveedores de servicios de bases de datos solo mantienen esta información por tres meses y luego no se asegura que aparezca. Este trámite tan garantista termina beneficiando al delincuente y obstaculizando el accionar del ente investigador. - En cuanto a la recolección de medios probatorios debe haber una mayor coordinación entre las dependencias de policía y organismos judiciales en los distintos operativos que se despliegan, ya que por la mala práctica en la recolección se pierden datos e informaciones vitales, y la equívoca manipulación de estos por parte de investigadores ajenos a la unidad especializada impide que se obtengan elementos que coadyuven a la investigación de estos delitos y de otros flagelos que tengan relación con la evidencia informática. - Los fiscales asignados a estos delitos carecen de una formación específica en cuanto a conocimientos técnicos y particulares en materia de delitos informáticos. Esta es una de las principales dificultades debido a que la unidad especializada del CTI tiene que hacer un mayor esfuerzo para apoyarlos en la investigación de estos punibles. Acogiéndonos a lo expuesto, debería existir una mayor inversión en capacitación y en la designación de fiscales especializados, con conocimientos técnicos en áreas informáticas y similares, que les permitan conjugar el derecho con las tecnologías. - Los jueces tampoco han sido lo suficientemente capacitados para el juzgamiento de estos delitos. Debido a que es toda una cadena en la que los eslabones van de investigador a fiscal y juez, deben entender los criterios tan innovadores de la norma que castiga los delitos informáticos. Esto se obtiene brindando capacitaciones que permitan a los operadores jurídicos comprender los tecnicismos y variables que estos delitos presentan, que por lo general son entendibles a la luz de conocimientos de ingenieros de sistemas y profesiones afines. Esta es una debilidad de nuestra administración de justicia, al no consolidar esfuerzos suficientes para que los jueces tengan todas las herramientas suficientes. Sin embargo, esta era una circunstancia que se preveía al momento

de entrar en vigencia la norma, y que expertos como los citados en la parte inicial del trabajo señalaron en cuanto a que se requería una reforma estructural, y preparación adecuada para que los operadores jurídicos y todos los agentes que intervienen en la investigación y desarrollo de un proceso judicial estuviesen lo suficientemente preparados para confrontar estos delitos. Al responder la pregunta inicial se averiguó que la persecución de los delitos informáticos durante el periodo 2011-2012 fue insuficiente por la naturaleza de las conductas, la falta de denuncias, el perfil de los delincuentes y la incipiente capacidad técnica y humana de la Fiscalía General de la Nación y el CTI, y lo restringido que se encuentra el juez de conocimiento frente a estos flagelos. La persecución judicial de estos delitos en Colombia es algo sumamente nuevo. Hasta la fecha se está empezando a invertir en una política nacional criminal, creando organismos especializados e invirtiendo partidas presupuestales que fomenten, fortalezcan y consoliden organismos judiciales, fiscales y jueces lo suficientemente capacitados, con recursos adecuados para generar eficacia de la norma y lograr un menor grado de impunidad frente a estos delitos, que cada vez más la sociedad colombiana sufre en su cotidianidad. La realidad de la comunidad asentada dentro del Distrito Judicial de Villavicencio no es ajena a este diagnóstico crítico de cifra negra de los delitos informáticos, por lo cual esperamos que cada vez sea mayor la capacidad de reacción de nuestro aparato de administración de justicia frente a la persecución de los delitos informáticos, que es lo que el Gobierno nacional ha tratado de consolidar y dirigir en los últimos tres años.

AUTOR DEL RAE 233006_2

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.

AUTOR Astrid Carolina Parra Rojas & Ricardo Granados Ramírez

FICHA BIBLIOGRÁFICA PARRA ROJAS, Astrid & GRANADOS RAMÍREZ, Ricardo. 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. Cúcuta, 2016, 77 p. Tesis de pregrado (abogado). Universidad Libre de Colombia, facultad de derecho, ciencias políticas y sociales.

PALABRAS CLAVE Seguridad, cambiazo, clonación, hurto informático, sistemas, fraude, recomendaciones.

PALABRAS DESCONOCIDAS

FUENTES 49

CONTENIDO DEL RAE Mediante el presente documento, el autor va a hacer un análisis de la aplicabilidad de la ley 1273 de 2009 en el distrito judicial de Cúcuta en el periodo 2012 – 2014. Con ocasión a la revolución informática a la fecha, los avances tecnológicos que con su aparición ha traído son innumerables, de tal manera que, así como tiene sus cosas positivas, también tiene las negativas, como por ejemplo la aparición de delincuentes informáticos y que con su aparición conllevaron a que en Colombia se promulgara por parte del ente legislador y se sancionara la Ley descrita inicialmente, más conocida como Ley de delitos informáticos. Dichos delitos informáticos y modalidades castigadas mediante la Ley 1273, en este caso especial el autor hace referencia al hurto por medios informáticos y semejantes, que es aquella conducta que se hace por sistemas protegidos por parte de personas que con conocimientos en sistemas o por la confianza depositada en ellos, obstaculizan, impiden el normal desarrollo, desvían, transfieren, retiran, acceden, etc., dinero a donde no se les ha autorizado, en la mayoría de casos, el bien jurídico tutelado es la economía del ciudadano, de aquel que depositando la buena fe en terceros en busca de ayuda, pasa a ser el sujeto pasivo, victima. Antes de haber sido sancionada la ley 1273 de 2009, en Colombia el hurto por medios informáticos era castigado bajo el artículo 239 de la ley 599 del 2000, Código Penal Colombiano, pero con la aparición de la ley 1273 pasó a ser

castigada bajo los preceptos del artículo 240, ya que esta modalidad por ser a través de un sistema informático, electrónico o de telecomunicaciones, se convierte en agravado, según lo descrito en la normatividad existente. Es por eso que con ocasión al aumento desmesurado de las conductas criminales asociadas al delito informático, y teniendo en cuenta que en otros países ya existía normatividad jurídica al respecto, Convenio de Budapest, en Colombia surgieron propuestas de Ley que luego de dos intentos por fin tuvo cabida en el Congreso y es ahí cuando fue aprobado el contenido de la Ley 1273 de 2009 la cual incorporo nuevos tipos penales al Código Penal Colombiano, unos a proteger la confidencialidad, disponibilidad e integridad de la información y los datos y otros a proteger de los ataques informáticos, entre esos el hurto por medios informáticos y semejantes, articulo 269i. Como el objetivo de este documento es analizar la aplicabilidad de mencionado artículo en el distrito judicial de Cúcuta durante el periodo comprendido entre 2012 y 2014, les daré a conocer las modalidades más recurrentes en dicha ciudad, según información aportada por la Fiscalía general de la nación y su unidad encargada de adelantar este tipo de investigaciones, Unidad Estructura de Apoyo EDA. Inicialmente se tiene que la modalidad más utilizada en ese lapso de tiempo, fue la utilización de tarjeta falsa en cajero automático, la cual es realizada luego de sustraer la información existente en la banda magnética de tarjetas extraviadas y que el cliente nunca reporta como perdidas ante la entidad bancaria para su respectivo bloqueo, sino cuando se entera de que le han sustraído dinero de su cuenta bancaria o también por confianza de los clientes, al realizar transacciones con ella y descuidar o perder de vista su tarjeta al momento del pago, conllevando a que pueda ser deslizada en lectores de tarjeta ajenos al del establecimiento público, con lo cual la información existente en la banda magnética puede sustraerse. Así mismo existe la modalidad del cambiazo de tarjeta, aquella que cuando el tarjetahabiente se encuentra realizando un retiro por cajero electrónico, permite que un tercero desconocido, le ayude en el procedimiento y en un descuido del cliente, le es cambiada su tarjeta, entregándole una con las mismas características y a su vez visualizada y

memorizada la clave de la misma, lo que conlleva a que una vez la tarjeta débito o crédito está en manos del delincuente, pueda realizar transacciones en otro cajero o establecimiento público y empiece a debitarse el dinero existente en la cuenta de la víctima. Junto con estas modalidades también se han presentado la denominada Phishing, en la cual el delincuente envía correos spam suplantando en la mayoría de casos ser enviados desde entidades bancarias y en las que normalmente piden actualizar información personal y confidencial del tarjetahabiente, por lo que una vez el cliente sigue instrucciones e ingresa a las URL adjuntadas en el correo, es dirigido a una página que simula ser la de la entidad bancaria y empieza a actualizar los datos que le piden, los cuales son dirigidos al delincuente informático, quien posteriormente los va a utilizar para realizar su conducta ilícita. En otras modalidades utilizadas fueron relacionados el software espía y keylogger. Con el fin de disminuir la ocurrencia de estas modalidades delictivas en el distrito judicial de Cúcuta, las autoridades municipales y de Policía, han implementado estrategias que permitan sensibilizar al ciudadano de bien respecto a las modalidades utilizadas por los delincuentes, generando para ellos algunas recomendaciones de seguridad al momento de realizar transacciones, principalmente con tarjeta, al utilizar los cajeros electrónicos en caso de no saber utilizarlos pedir ayuda a un funcionario del banco o en su defecto ir acompañado de otra persona que si sepa utilizarlo, no permitir la ayuda por parte de extraños, no descuidar ni perder de vista al momento de pagar con tarjeta en establecimientos, como lo son estaciones de gasolina y/o restaurantes, cambiar de manera constante la contraseña de la tarjeta, no realizar transacciones por internet desde sitios públicos, verificar que la pagina visitada del banco y por medio de la cual realizaran la transacción empiece en https, entre otras.

CONCLUSIONES La revolución informática surgida desde mediados del siglo XX hasta la actualidad, ha traído consigo un sinnúmero de beneficios, especialmente relacionados con la facilidad para el intercambio de información y comunicación a

nivel mundial; sin embargo, así como esta ha evolucionado y tiene importantes ventajas, también ésta tiene sus desventajas, y es que a la par con ella han surgido los delincuentes informáticos, quienes han venido perfeccionando sus modus operandi en los delitos informáticos, siendo uno de los más frecuentes el delito de hurto por medios informáticos, consagrado en la Ley 1273 de 2009 (Artículo 269I). La Ley 1273 en su artículo 269I, consagró el delito de hurto por medios informáticos, en aras de proteger el patrimonio económico de los ciudadanos, estableciendo que quien superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 (hurto) manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. Antes de la expedición de la Ley 1273 del 2009, el Código Penal (Ley 599 de 2000), en varias normas, hacía referencia a la descripción de conductas punibles cometidas utilizando medios informáticos, no expresamente dentro de un título como tal, sino que estas se encontraban diseminadas por varios de ellos; y el tratamiento penal que se otorgaba al mismo, era el de hurto simple (artículo 239); situación que cambio con la entrada en vigencia de esta nueva ley, pues en ella se consagra el tratamiento penal, como el de un hurto calificado, consagrado en el artículo 240 de la Ley 599 de 2000, y tendrá una pena de prisión de seis (6) a catorce (14) años, si el hurto se cometiere: 1. Con violencia sobre las cosas; 2. Colocando a la víctima en condiciones de indefensión o inferioridad o aprovechándose de tales condiciones; 3. Mediante penetración o permanencia arbitraria, engañosa o clandestina en lugar habitado o en sus dependencias inmediatas, aunque allí no se encuentren sus moradores; 4. Con escalonamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes. Por su parte, el mismo artículo 240 del Código Penal (Ley 599 de 2000), establece que la pena será de prisión de ocho (8) a dieciséis (16) años cuando se cometiere con violencia sobre las personas. Además, las mismas penas se aplicarán cuando la

violencia tenga lugar inmediatamente después del apoderamiento de la cosa y haya sido empleada por el autor o partícipe con el fin de asegurar su producto o la impunidad. Por otra parte, la pena será de siete (7) a quince (15) años de prisión cuando el hurto se cometiere sobre medio motorizado, o sus partes esenciales, o sobre mercancía o combustible que se lleve en ellos. Si la conducta fuere realizada por el encargado de la custodia material de estos bienes, la pena se incrementará de la sexta parte a la mitad; y finalmente, la pena será de cinco (5) a doce (12) años de prisión cuando el hurto se cometiere sobre elementos destinados a comunicaciones telefónicas, telegráficas, informáticas, telemáticas y satelitales, o a la generación, transmisión o distribución de energía eléctrica y gas domiciliario, o a la prestación de los servicios de acueducto y alcantarillado. El sujeto activo en el delito de hurto por medios informáticos, puede ser: cualquier persona, un indeterminado singular, cualquier persona, o la persona encargada de la custodia material de los bienes. Por su parte el sujeto pasivo en dicho delito, es la persona natural o jurídica titular del derecho de propiedad; o la persona en estado de indefensión o inferioridad. El bien jurídico tutelado es el de delitos contra el patrimonio, que se encuentra en el TÍTULO VII – Ley 599 de 2000. Las modalidades de hurtos que se han generado a través de medios informáticos en el Municipio de San José de Cúcuta en el período 2012-2014, según la información consultada en la Fiscalía General de la Nación, Unidad de Estructura de Apoyo EDA, son: la utilización de tarjeta falsa en cajero automático, el cambiazo de tarjeta, la clonación de tarjetas, el phishing, el Software espía – Spyware, y el Key Logger, los cuales afectan el patrimonio económico, y, principalmente a los tarjetahabientes de las diferentes Entidades Bancarias. En relación con las estrategias orientadas a evitar ser víctima del delito de hurto a través de medios informáticos en el Municipio de San José de Cúcuta, de acuerdo a las situaciones más frecuentes que se presentan frente a este delito en medios informáticos, se recomienda a los tarjetahabientes, clientes bancarios, y a quienes realizan transacciones a través de internet: 1. Cambiar frecuentemente la clave personal; 2. No perder de vista la tarjeta, ni permitir que la deslicen en dispositivos diferentes

a datafonos, cajeros electrónicos o PIN PAD; 3. No prestar su tarjeta a terceros; 4. No aceptar ayuda de extraños al hacer operaciones en cajeros, datafonos o medios electrónicos; 5. No escribir, la clave en ninguna parte, esta debe ser memorizada; 6. Tapar el teclado cuando digite la clave, para evitar que alguien pueda verla; 7. Al momento de efectuar alguna transacción o compra con tarjeta revisar que la tarjeta que le sea entregada o devuelta sea la suya; 8. No ingresar a las páginas de los bancos a través de links (enlaces) o correos electrónicos; 9. No entregar información y datos personales por correo electrónico de sus cuentas de ahorro o corrientes; 10. No acceder a las páginas de los bancos a través de enlaces, sino tecleando la dirección; 11. Mantener actualizado su computador personal con mecanismos de seguridad tales como: antivirus, antispyware, firewall personal, parches de seguridad entre otros; 12 No realizar transacciones desde computadores públicos. Finalmente, es importante resaltar que los bancos en general restituyen el dinero hurtado cuando la modalidad usada es desconocida por los clientes y no se han tomado medidas para sensibilizar a los clientes sobre las precauciones que debe tener para no caer en la trampa; pero devolver el dinero al cliente es decisión de cada banco, de acuerdo con el resultado de la investigación que surta y de sus políticas internas. En algunos productos o casos, estas pérdidas están aseguradas, sin embargo, no la totalidad; pues algunos productos y en determinados Bancos, se cuenta con pólizas de seguros para cubrir riesgos de ataques informáticos o ciberseguridad. Para que el Banco revise el caso es necesario acudir al defensor del cliente bancario, que tiene cada Entidad.

AUTOR DEL RAE 233006_2

En el ámbito local y luego de realizar búsqueda en diferentes repositorios de universidades de esta zona del país, como Universidad del Sinú, Universidad de Córdoba, Universidad Pontificia Bolivariana, no se encontraron análisis realizados

al aumento del delito de hurto por medios informáticos y semejantes en esta región del país.

1.6. MARCO DE ANTECEDENTES

- Bolaño, Andrés. Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica San Juan de Pasto, 2014, 100 p. Monografía (Especialización en Seguridad Informática). Universidad nacional Abierta y a Distancia, escuela de Ciencias Básicas Tecnología e Ingeniería.

- PARRA ROJAS, Astrid & GRANADOS RAMÍREZ, Ricardo. 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. Cúcuta, 2016, 77 p. Tesis de pregrado (abogado). Universidad Libre de Colombia, facultad de derecho, ciencias políticas y sociales.

- RODRÍGUEZ ÁLVAREZ, Juan. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. {En línea}. Fecha. {26 de mayo de 2017}. Disponible en http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

- CORTÉS, Rodrigo - BALLÉN, Jhon & DUQUE Juan. La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. En: Revista de derecho comunicaciones y nuevas tecnologías. No 14 (Jul-Dic. 2015); p. 1-25.

1.7. MARCO CONTEXTUAL

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. (2013). Elaborado por: Giovanni Stalin Grisales Pérez. Universidad EAFIT, Medellín, Antioquia.

La razón de este documento, surge del incremento desmesurado de los delitos informáticos a nivel mundial, conductas como el hurto por medios informáticos y la Transferencia no consentida de activos, afectan en nuestro país, tanto a personas naturales como jurídicas, padeciendo cada una de ellas en su medida, graves detrimentos patrimoniales a través de la perdida de sus bienes económicos e información privada a la que acceden de manera ilegal los delincuentes cibernéticos. Esa razón, llevó a que se hiciera un estudio dogmático de ambas conductas punibles, tomando como referencia los cientos de casos que mes a mes ingresan a los despachos de las Fiscalías de Medellín y que fueron muchos de ellos analizados con el fin de ilustrar de una manera clara, sencilla y comprensible a Jueces, Fiscales, funcionarios de Policía Judicial, abogados, estudiantes de derechos y todos aquellos que quieran conocer desde lo jurídico el amplio y complicado mundo de los delitos informáticos en Colombia.

Los delitos en las redes sociales: aproximación a su estudio y clasificación. (2012). Elaborado por: Andrea de Cea Jiménez. Universidad de Salamanca, España. Este trabajo desarrolla un estudio y elabora una clasificación de los delitos que se pueden cometer las redes sociales en línea. Para ello se realiza un estudio del estado de la cuestión tanto de la definición como de las características del delito informático y de las redes sociales.

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. Cúcuta, 2016, 77 p. Tesis de pregrado (abogado). Universidad Libre de Colombia, facultad de derecho, ciencias políticas y sociales. A través del presente documento se dan a conocer las modalidades utilizadas por los delincuentes en la ciudad de Cúcuta y por medio de las cuales obtienen para su bien o de un tercero, el dinero existente en las cuentas de ahorro, tarjetas débito, crédito, de personas del común y que deambulan en esa ciudad, modalidades a través de las cuales infringen el articulo 269i de la ley 1273 de 2009.

1.8. MARCO TEÓRICO.

Con el paso de los días, el acceso a las tecnologías de la información y las comunicaciones es un medio utilizado por las personas, razón por la que con su uso y los diferentes retos que la tecnología impone surgen riesgos en la red los cuales en la mayoría de casos tienen como víctima al usuario, que en este caso es el ciudadano de a pie, pueden ser riesgos mínimos como algo muy considerado; por lo cual se hace necesario preocuparnos por los sistemas de seguridad para evitar que nuestros clientes/usuarios permitan que estos riesgos se materialicen, buscando para esto estrategias contra este tipo de acciones, hoy en día sancionadas penalmente. Se considera un delito informático toda conducta ilícita que puede ser sancionada a la luz del Derecho Penal, por hacer uso indebido de la información y de cualquier medio informático empleado para su manejo, o de la tecnología electrónica o computarizada, como método, como medio o como fin, en perjuicio de la libertad de las personas y organizaciones, o de su patrimonio, o propiedad (activos), o de su derecho a la vida, a la intimidad, al crédito y buen nombre.

Julio Téllez-Valdés (2007), en su libro Derecho Informático, enfoca el delito informático desde el punto de vista típico y atípico y lo define como "actitud contraria a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".

Alberto Suárez-Sánchez (2009), por su parte, señala: "En conclusión, el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información per se cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales".

Luis Camacho-Losa (1987), de otro lado, había dicho: "Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas".

En el mismo sentido Castillo y Ramallo, expresan que el delito informático es “toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas”. (Huerta & Líbano, 1996, p. 114).

Carrasco (s/a), define el hurto como “el apoderamiento de objetos ajenos con violencia”, también habla sobre las diferentes modalidades de hurto: robo ordinario simple y calificado, y, los delitos que incumplen las personas que lo cometen.

Teniendo en cuenta que para poder ejecutarse una actividad delictiva deben participar mínimo dos personas, penalmente se clasifican de la siguiente manera:

Sujeto Activo: Persona del común cuyo interés está fundamentado en obtener ilícitamente un bien, con el fin de obtener provecho para sí mismo o para un tercero; independiente de su estatus económico, no existe motivo para la realización de la conducta.

Sujeto Pasivo: es aquella persona sobre la cual el sujeto activo (víctima del hecho), ejerce alguna acción con el fin de apoderarse del bien que le va a generar provecho y la cual desconoce el modus operandi del delincuente o en algunas ocasiones son víctimas ya que abusan de la buena fe que ha depositado en el sujeto activo.

El cambiazo de Tarjeta: es una modalidad que generalmente sucede cuando una persona se encuentra haciendo fila en un cajero electrónico y se ofrece a brindar ayuda a algún tarjetahabiente que está realizando alguna transacción en el cajero de una Entidad Bancaria. Esta persona porta una tarjeta con las mismas características que la que tiene el usuario (victima); en medio de la ayuda brindada el delincuente cambia su tarjeta y así mismo es posible que observe la clave digitada por el usuario o por parte de un segundo delincuente, con lo cual ya pueden realizar retiros u otras transacciones con la tarjeta, llegando al punto de utilizar la totalidad del saldo existente en la cuenta.

La clonación de tarjetas: en este caso el cliente puede haber sido víctima del cambiazo de tarjeta o al momento de pagar algún bien con su tarjeta, la pierde de vista y es el momento en que la tarjeta es deslizada por un dispositivo que copia la información alojada en la banda magnética de la misma; posteriormente esa información es transferida a otra tarjeta con la cual empiezan a realizar

transacciones, de las cuales el cliente normalmente se da cuenta al momento en que recibe su extracto mensual.

1.9. MARCO CONCEPTUAL

Adware: (kaspersky, 2017) es un software, generalmente no deseado, que permite el envío de contenido publicitario a un equipo.

Amenaza: (EPN, 2017) Cualquier acción o evento que puede ocasionar consecuencias adversas.

Análisis de impacto al negocio: (seguridad pc, s/f)evaluar los resultados y las consecuencias de la inestabilidad.

Análisis de riesgos: (wikipedia, 2017) consiste en identificar los activos de información de una empresa, vulnerabilidades, amenazas, para así saber los riesgos a los cuales se encuentran expuestos junto a su probabilidad de ocurrencia y el impacto que ocasionará, con el fin de determinar lo controles necesarios para mitigar o evitar la ocurrencia o daño del mismo.

Antispam: (kaspersky, 2017) es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios.

Antivirus: (kaspersky, 2017) software de seguridad utilizado normalmente para proteger equipos de virus, ya sea en tiempo real o mediante análisis, los pone en cuarentena y/o los elimina.

Arquitectura: el diseño de la estructura y las relaciones de sus elementos.

Ataques: tipos y naturaleza de inestabilidad en la seguridad.

Ataques Web: es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Auditabilidad: permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Autenticación: Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Autorización: Lo que se permite cuando se ha otorgado acceso

Blacklisting o Lista Negra: es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos.

Cambiazo: Acción ejecutada por una persona quien brindando ayuda a un tarjeta-habiente, aprovecha un descuido de este último, para cambiarle la tarjeta, entregándole una con las mismas características.

Clasificación de datos: (MINTIC, 2009) El proceso de determinar la sensibilidad y Criticidad de la información.

Clonación: (EPN, 2017)Acción realizada por delincuentes de pasar información existente en la banda magnética de una tarjeta débito o crédito a otra.

Confidencialidad: (EPN, 2017) pilar que debe tener la información debe ser accesible solo a aquellas personas autorizadas.

Control de Acceso: limitar el acceso autorizado solo a entidades autenticadas.

Métricas de Seguridad, monitoreo: Medición de actividades de seguridad.

Cracker: aquel que rompe con la seguridad de un sistema.

Criticidad: La importancia que tiene un recurso para el negocio.

Contra medidas: Cualquier acción o proceso que reduce la vulnerabilidad.

Controles: Cualquier acción o proceso que se utiliza para mitigar el riesgo.

Disponibilidad: (EPN, 2017)Pilar que debe tener de manera ininterrumpida la información y servicios accesibles y utilizables cuando se les requiera.

Hacker: persona que profundiza el funcionamiento de los sistemas con el fin de usarlos al máximo.

Estrategia: los pasos que se requieren para alcanzar un objetivo.

Exposiciones: Áreas que son vulnerables a un impacto por parte de una amenaza.

Gerencia: Vigilar las actividades para garantizar que se alcancen los objetivos.

Gobierno: proporcionar control y dirección a las actividades.

Identificación: verificación de una persona o cosa; reconocimiento.

Impacto: los resultados y consecuencias de que se materialice un riesgo.

Ingeniería social: practica de obtener información confidencial a través de múltiples formas.

Integridad: debe tenerla la información para que siempre sea protegida y exacta.

Keylogger: dispositivo hardware encargado de registrar las pulsaciones de tecla, para posteriormente enviarlas por medio de un correo.

No repudio: no se puede negar un evento o una transacción.

Normas: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

Pharming: (Avast, s/f)método de ataque que redirige el tráfico a sitios web falsos, previamente diseñados y que imitan el real; su principal objetivo es obtener información personal, principalmente bancaria.

Phishing: (Avast, s/f) consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. En esta modalidad incluyen un enlace supuestamente de la página web de la entidad bancaria el cual lleva a páginas web falsificadas, de esta manera el cliente creyendo que está en una página segura, digita sus datos de acceso los cuales son enviados al delincuente.

Políticas: declaración de alto nivel sobre la intención y la dirección de la gerencia.

Riesgo: la explotación de una vulnerabilidad por parte de una amenaza.

Riesgo residual: (Wikipedia, s/f)El riesgo que permanece después de que se han implementado contra medidas y controles.

Sensibilidad: el nivel de impacto que tendría una divulgación no autorizada.

Seguridad en capas: La defensa a profundidad que contenga la inestabilidad.

Software espía – Spyware: malware encargado de recopilar información de un ordenador, con el fin de transmitir a una entidad externa sin conocimiento y autorización del propietario.

Virus: Programa que puede alterar o destruir el funcionamiento del computador. Normalmente funciona sin el permiso o conocimiento del usuario.

Vishing: (MINTIC, 2009) conducta similar al phishing, pero con teléfonos. Consiste en hacer llamadas telefónicas a las víctimas, En las que por medio de una voz computarizada, muy similar a las utilizadas por los bancos, se solicita verificar algunos datos personales e información bancaria.

Vulnerabilidades: deficiencias que pueden ser explotadas por amenazas.

1.10. MARCO LEGAL

- Constitución Política de Colombia
- Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”
- Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”
- Ley 1621 de 2013 “Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones”
- Ley 1712 de 2014“Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones

- Decreto 1727 de 2009 “Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información”

- Decreto 2952 de 2010 “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”

- Decreto 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”

- Decreto 886 de 2014 “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”

- Código Penal Colombiano. Ley 599 de 2000.

- Documento CONPES 3854 de 11 abril 2016 Política Nacional de Seguridad Digital.

- Ley 1826 de enero 2 de 2017 “por medio de la cual se establece un procedimiento penal especial abreviado y se regula la figura del acusador privado”.

- Ley 1928 de julio 20 de 2018 “por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest”

DISEÑO METODOLOGÍCO

1.11. TIPO DE INVESTIGACIÓN

La metodología a realizar en esta monografía es de tipo descriptiva, documental y jurídica, ya que el objetivo principal de este tipo de investigación busca llegar a conocer actitudes o situaciones que se han presentado, en nuestro caso el hurto informático en el departamento de Córdoba durante los años 2015 y 2016.

Descriptiva porque con ella se va a dar a conocer las modalidades utilizadas por los delincuentes para concurrir en el delito de hurto informático en el departamento de Córdoba durante los años 2015 y 2016.

Documental ya que es basada en la estadística existente en bases de datos de empresas del estado, en las que se analizaran la modalidad realizada en cada caso denunciado.

Jurídica ya que pretende demostrar el aumento de denuncias por el delito de hurto informático en el departamento de Córdoba, tipificado en el artículo 269i de la Ley 1273 de 2009 la cual aumentó tipos penales en la ley 599 de 2000.

1.12. POBLACIÓN Y MUESTRA

Este trabajo de investigación tomará como ejemplo la población del departamento de Córdoba quienes durante los años 2015 y 2016 han sido víctimas del hurto por medios informáticos.

1.13. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las técnicas empleadas para desarrollar la investigación, así como las fuentes de información para la elaboración de esta se realizarán a través de un análisis y

revisión de documentos en internet, libros, artículos, leyes nacionales todas relacionados con delitos informáticos, número de capturas por violación al artículo 269i del Código Penal Colombiano efectuadas durante los años 2015 al 2016 a nivel nacional, número de denuncias y reporte estadístico delictivo de casos ocurridos a nivel nacional, información que fue aportada por el Centro Cibernético de la Policía Nacional y otra extraída desde el sitio web de la Policía Nacional de Colombia,[3] la cual previamente fue solicitada, textos históricos, informes policiales, imágenes, videos que nos permita tener información relacionada con el tema de estudio y que permita establecer modus operandi del delincuente.

1.14. PRODUCTO RESULTADO A ENTREGAR

Con la realización de esta monografía mediante la cual se va a analizar el porqué del aumento del hurto informático en el departamento de Córdoba durante los años 2015 y 2016, los habitantes del departamento de Córdoba principalmente los residentes en las cabeceras municipales se beneficiarán al conocer las modalidades utilizadas por los delincuentes para incurrir en el delito tipificado en el artículo 269i del Código Penal Colombiano como hurto por medios informáticos y semejantes, permitiendo de esta manera no caer en manos de los delincuentes.

[3] https://www.policia.gov.co/grupo-informaci%C3%B3n-criminalidad/resultados-operativos

RESULTADO Y DISCUSIÓN

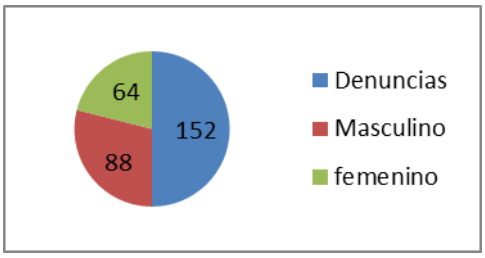
1.15. ANÁLISIS DE VARIABLES QUE CONLLEVAN AL AUMENTO DEL DELITO INFORMÁTICO EN EL DEPARTAMENTO DE CÓRDOBA DURANTE LOS AÑOS 2015 - 2016.

Teniendo en cuenta el número de denuncias realizadas durante los años 2015 y 2016 cuyo delito es el hurto por medios informáticos y semejantes tipificado en el artículo 269i del Código Penal Colombiano, las siguientes son algunas de las variables que por medio de las denuncias podemos describir.

Género

Se puede diferir que basados en la estadística aportada por el Centro Cibernético de la Policía Nacional, durante los años 2015 y 2016, se instauraron 152 denuncias por el delito de hurto por medios informáticos y semejantes, de las cuales en 88 denuncias la víctima es una persona de sexo masculino (57,9 % del total de denuncias). Por lo cual, y teniendo en cuenta las hipótesis que se puedan generar, es válido afirmar que para entablar diálogo por parte de una mujer con una persona desconocida es más difícil que cuando un hombre lo hace.

Figura 4 Comparativo de sexo según denuncias radicadas, años 2015 - 2016

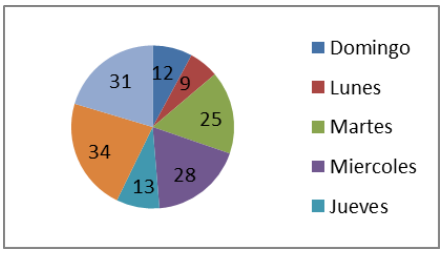


Fuente: El autor, información aportada por Centro Cibernético Policial.

Día de la semana

De las denuncias instauradas en el periodo comprendido entre los años 2015 – 2016, un total de 53 denuncias fueron realizadas durante los días sábado y domingo, es decir un 28,2% del total de denuncias instauradas.

Figura 5 Comparativo de días según denuncias radicadas, años 2015 - 2016

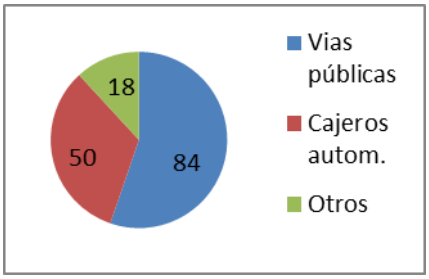


Fuente: El autor, información aportada por Centro Cibernético Policial

Sitio

Evidenciamos también en la estadística, que la ocurrencia de las denuncias en algunos casos puede ser en sitios concurridos, vías públicas y hasta en cajeros electrónicos, donde vías públicas tiene un 55.2 % de casos contra 32.8 % de casos ocurridos en cajeros automáticos.

Figura 6 Lugar hecho según denuncias radicadas, años 2015 - 2016

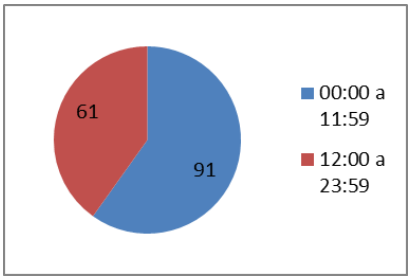


Fuente: El autor, información aportada por Centro Cibernético Policial

Horario

Se puede evidenciar que 91 casos (59.8 %) ocurrieron en las primeras 12 horas del día, por tal motivo es probable deducir que el delincuente actúa mayoritariamente en horas de la mañana.

Figura 7 Lugar hecho según denuncias radicadas, años 2015 - 2016

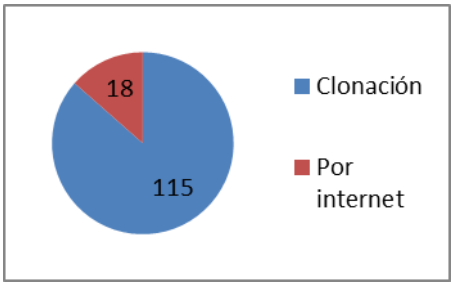


Fuente: El autor, información aportada por Centro Cibernético Policial

Modalidad

Misma forma ocurre en esta variable, ya que la más conocida, rápida, y eficiente para tener dinero efectivo a la mano es la clonación de tarjeta con 115 casos (75.6 %), pero también podemos encontrarnos con las ejecutadas por internet, 18 casos para un 11.8 %, que pueden ser compras o transferencias entre cuentas, que, a pesar de su complejidad, pueden aumentar el daño económico al bolsillo del afectado.

Figura 8 modalidad utilizada según denuncias radicadas, años 2015 - 2016



Fuente: El autor, información aportada por Centro Cibernético Policial

1.16. ESTRATEGIAS REALIZADAS POR LOS ENTES DEL ESTADO PARA CONTRARRESTAR LA ACCIÓN DELINCUENCIAL.

Teniendo en cuenta que los delitos informáticos y precisamente esta modalidad es realizada por medios informáticos o a través de sistemas informáticos, las

autoridades se limitan a realizar campañas de sensibilización en entidades bancarias, centros comerciales y difundirlas por redes sociales, a continuación, un ejemplo de ello.

En la siguiente imagen podemos visualizar la campaña preventiva realizada por los funcionarios de Policía en la ciudad de Montería, más precisamente a las afueras de las entidades bancarias Davivienda y BBVA, por medio de la cual se da a conocer al cliente bancario las modalidades delictivas utilizadas por los delincuentes informáticos para realizar el cambiazo de tarjeta.

Figura 9 Campaña preventiva Policía Montería

Fuente: Twitter @PoliciaMonteria

En la imagen que continúa observamos que a través de la red social Twitter la Policía Metropolitana de Montería da a conocer correos electrónicos por medio de los cuales se puede suministrar información de personas dedicadas a la ejecución de conductas ilícitas, entre ellas los delitos informáticos.

Figura 10 Campaña preventiva Policía Montería

Fuente: Twitter @PoliciaMonteria

Observamos en la siguiente imagen actividades de disuasión al interior de las entidades bancarias con las cuales se da a conocer a los tarjeta habientes no aceptar ayudas de personas desconocidas ya que es una de las modalidades utilizadas por los delincuentes informáticos para obtener información confidencial y con la cual pueden afectar vía internet el patrimonio de las personas.

Figura 11 Campaña preventiva Policía Montería

Fuente: Twitter @PoliciaMonteria

En la siguiente imagen los funcionarios de Policía realizan verificación de antecedentes y requisa a personas que se encuentran de manera sospechosa a las afueras de entidades bancarias, lo anterior en fin de disuadir al delincuente, así mismo dicha actividad es difundida a través de redes sociales.

Figura 12 Campaña preventiva Policía Montería

Fuente: Twitter @PoliciaMonteria

En la siguiente imagen observamos que se realizan charlas de sensibilización por funcionarios de la SIJIN al personal que hace parte del gremio hotelero, con el fin de darles a conocer las diferentes modalidades delictivas utilizadas por los delincuentes para afectar el patrimonio económico de las personas de manera virtual, entre esas el phishing.

Figura 13 Campaña preventiva Policía Montería

Fuente: Twitter @PoliciaMonteria

En la siguiente imagen podemos visualizar que se realizan charlas de sensibilización por funcionarios de la SIJIN y GAULA a los comerciantes, con el fin de darles a conocer las diferentes modalidades delictivas utilizadas por los delincuentes para afectar el patrimonio económico de las personas de manera virtual.

Figura 14 Campaña preventiva Policía Montería

Fuente: Twitter @PoliciaMonteria

En la siguiente imagen observamos que se realizan campañas por medio de redes sociales con el fin de recordarle al tarjeta habiente no permitir la ayuda de extraños al momento de utilizar los cajeros electrónicos, ya que puede ser víctima del cambiazo, modalidad con la cual el delincuente informático puede obtener la clave de la tarjeta y realizar el cambio de la misma, permitiéndole de esta manera poder retirar y transferir el dinero existente en la cuenta.

Figura 15 Campaña preventiva Policía Córdoba

Fuente: Twitter @PoliciaDecor

En la siguiente imagen se realiza charla de sensibilización a los estudiantes de universidades a fin de darles a conocer las modalidades utilizadas por los delincuentes informáticos para afectar de manera virtual el patrimonio de las personas u organizaciones.

Figura 16 Campaña preventiva Policía Córdoba

Fuente: Twitter @PoliciaDecor

1.17. MODALIDADES DE HURTO INFORMÁTICO UTILIZADAS POR LOS DELINCUENTES INFORMÁTICOS.

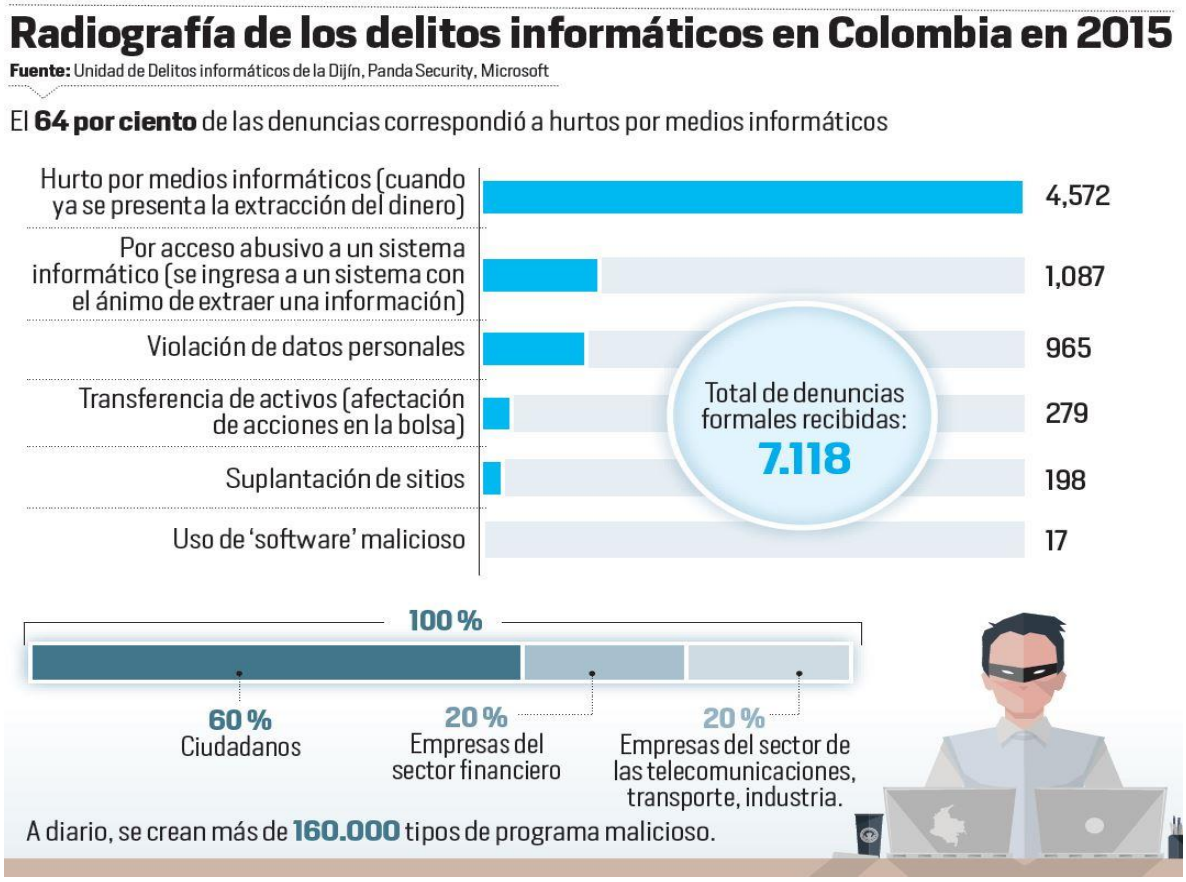
Los delitos informáticos representan el 15% de los ilícitos cometidos a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares en el último año, reveló Intel Security, La cifra es calculada con base en el tiempo en que las compañías afectadas cesan su operación debido a ataques informáticos, los puntos débiles de las compañías es el bajo presupuesto que destinan a seguridad informática. "No supera el 10 por ciento en el mejor de los casos. Entretanto, las amenazas cibernéticas se incrementan entre 50 y 60 por ciento cada año"

El Coronel Freddy Bautista, jefe de la Unidad de Delitos Informáticos de la DIJIN, reveló que en Colombia se formalizaron 7.118 denuncias por delitos informáticos durante el 2015, más de 40 por ciento más que en 2014.

De esta cifra, 4.572 casos (64 por ciento) se relacionaron con hurto por medios informáticos. Más de 1.087 (15,27 por ciento) estuvieron ligadas con acceso abusivo a un sistema informático. Esto refiere a las situaciones donde se ingresó a un sistema con el ánimo de extraer información; 965 (13,5 por ciento) se vincularon con violación de datos personales; 279 (3,9 por ciento), con transferencia de activos (en estos casos, el cibercriminal afecta a la bolsa de valores y a las acciones); 198 (2,7 por ciento), con suplantación de sitios (el famoso 'phishing', una página web igual a la de una institución oficial para engañar a las personas), y 17 (0,2 por ciento), con la creación y uso de software malicioso.

Observamos en la siguiente imagen la estadística de denuncias instauradas durante el año 2015 según los delitos tipificados en la ley 1273 de 2009, donde se puede evidenciar que el delito más denunciado es el hurto por medios informáticos.

Figura 17 Estadística denuncias año 2015



Fuente DIJIN, Panda Security, Microsoft.

1.18. CAPACIDADES DE LOS FUNCIONARIOS ENCARGADOS DE INVESTIGAR HURTOS INFORMÁTICOS.

En la actualidad el Cuerpo Técnico de Investigación (CTI) de la Fiscalía General de la Nación cuenta con dos ingenieros de sistemas los cuales hacen parte del grupo investigaciones tecnológicas, pero no están dedicados a la investigación de delitos informáticos, también investigan delitos que afecten el patrimonio económico de la comunidad; la Policía Judicial de la Policía Nacional tiene un ingeniero de sistemas que es quien de manera exclusiva investiga las modalidades delictivas que se presenten relacionadas con delitos informáticos.

1.19. RESULTADOS DE OPERATIVIDAD DADOS A CONOCER POR LAS AUTORIDADES EN CUESTIÓN A ESTE DELITO.

Realizando búsquedas en las noticias de circulación local, nacional y regional en el departamento de Córdoba, se pudo obtener la siguiente información respecto a capturas de personas dedicadas a la ejecución de conductas delictivas asociadas al hurto por medios informáticos y semejantes, tipificado en la ley 1273 de 2009, articulo 269i del Código Penal Colombiano.

La imagen que más adelante encontraremos nos da a conocer 7 personas que fueron capturadas las cuales prestaron sus cuentas bancarias con el fin de recibir dinero que de manera virtual había sido hurtado a una empresa de la ciudad de Montería.

Figura 18 Noticia de interés

Desarticulamos banda delincuencial 'los cibernautas', al capturar siete de sus integrantes

Miércoles, 22 de Julio de 2015

Montería. Los operativos fueron realizados por parte de nuestros uniformados de la DIJIN.

Fuente www.policia.gov.co

Así mismo por medio de redes sociales y periódicos digitales se encontró la siguiente información respecto a las campañas de disuasión efectuadas por la Policía Metropolitana de Montería.

Con relación a la siguiente imagen se obtuvo información que mediante la ciberpatrulla, funcionarios de Policía bajo coordinación de personal responsable de investigar delitos informáticos de la SIJIN Montería, patrullaban las calles de la ciudad con el fin de obtener información relacionada con ciudadanos que mediante publicaciones por internet generara terrorismo, lo anterior teniendo en cuenta el paro armado que se llevó a cabo en abril del año 2016; así mismo recolectando información que permitiera identificar personas o estructuras dedicadas a la ejecución de delitos informáticos en el departamento de Córdoba.

Figura 19 Noticia de interés

Policía Metropolitana de Montería da conocer a la comunidad Patrulla Ciberseguridad

Lunes, Abril 11, 2016 - 16:15

Con tecnología de punta y con recurso humano especializado en delitos informáticos, la Policía Metropolitana de Montería dio a conocer a la comunidad la Patrulla Ciberseguridad con el fin de ubicar y judicializar personas que generen terrorismo, intimidación y zozobra en redes sociales como Facebook, WhatsApp, Instagram y Twitter.

La patrulla cuenta con un sistema de antecedentes a celulares para identificar aquellos que promocionan y auspician mensajes terroristas en redes como también un sistema de seguimiento a cuentas delincuenciales que incentivan a la comunidad a generar mecanismos de inseguridad en red.

Fuente: http://hsbnoticias.com/noticias/judicial/policia-metropolitana-de-monteria-da-conocer-la-comunidad-199845

Así mismo y con el fin de disuadir al delincuente informático teniendo en cuenta la zozobra generada anteriormente con la realización del paro armado en el departamento de Córdoba y municipios aledaños, la Policía Metropolitana de Montería siguió realizando patrullajes y actividades de control por medio de las cuales se recibiera información por parte de la comunidad relacionada con conductas delictivas asociadas a los delitos informáticos.

Figura 20 Noticia de interés

Fuente: http://larazon.co/2016/04/ciberpatrulla-hara-seguimiento-uso-redes-sociales-monteria/

Por medio de la siguiente imagen, la Policía Metropolitana busca generar confianza en la ciudadanía, permitiendo que de esta manera exista más cercanía y la comunidad crea en las actividades de la institución, utilizando para ello la ciberpatrulla, vehículo dotado de tecnología con la cual se está realizando

verificación de antecedentes a personas y rastreo de perfiles en redes sociales cuyo fin sea generar temor en la comunidad.

Figura 21 noticia de interés

Fuente: Twitter @PoliciaMonteria

1.20. ANTECEDENTES DE CASOS INVESTIGADOS EN LOS CUALES SE DÉ A CONOCER EL TIEMPO QUE DURÓ LA INVESTIGACIÓN Y RESULTADOS OBTENIDOS.

Toda investigación más precisamente proceso penal debe tener unas etapas las cuales son las que permiten que tanto la Fiscalía General de la Nación como Policía Judicial (CTI o Policía Nacional – SIJIN) realicen las coordinaciones necesarias y suficientes para la realización de un programa metodológico, art. 207 CPP, que es aquel en el cual se plasman las actividades que se realizaran con el fin de establecer el autor y/o participes de los hechos que se investigarán y de igual forma dispondrá del número de investigadores necesarios para la investigación como de los equipos tecnológicos que sean necesarios; lo cual conlleva a que dichas actuaciones o actividades a desarrollar por parte del equipo de Policía Judicial tomen un tiempo necesario puede ser en días o meses, inclusive años, dependiendo de la magnitud o complejidad del caso a investigar.

Para la investigación de un delito informático, en la mayoría de los casos es necesario acceder a bases de datos tanto públicas como privadas (art. 244 CPP), en este último caso de ser necesario acceder es indispensable contar con permiso por parte de un juez con funciones de control de garantías por medio del cual se den a conocer las pretensiones del acceso a dicha base de datos y que conlleven a violar el derecho a la intimidad de las personas al igual que al habeas data, tal como lo enuncia la carta magna en su artículo 15 y el Código de Procedimiento Penal en su artículo 14, basados en la sentencia C-336 de 2007, lo que conlleva a que no baste tener en cuenta la disposición que pueda tener el fiscal coordinador del caso, sino de la fecha de programación para la audiencia por medio de la cual se va a solicitar ante un juez con funciones de control de garantías, la autorización para acceder a una base de datos privada, permitiendo que de esta manera el tiempo de la investigación se aumente de una manera considerable y en muchas

ocasiones indeterminable, pues el tener la autorización para acceder a una base de datos no es garantía de obtener la información requerida en un tiempo determinado que puede ser de hasta 60 días calendario, ya que según el código de procedimiento penal, dentro de este tiempo se debe obtener la respuesta por parte de las entidades bancaria o que administren información confidencial que pueda afectar al indiciado o imputado.

Existen casos en los cuales en los primeros 30 días (tiempo inicial autorizado por el juez para acceder a una base de datos controlada) no se recibe respuesta por parte de la entidad a la cual se le solicitó la información, por lo cual se hace necesario realizar una nueva audiencia con el fin de solicitar una prórroga por un tiempo máximo igual al inicial, con el fin de esperar la respuesta de dicha entidad, pero es posible no obtener la respuesta, por lo cual y basados en la normatividad existente articulo 224 Código de Procedimiento Penal, se hace necesario iniciar nuevamente con el trámite para la obtención de acceso legal a una base de datos controlada, conllevando a que los tiempos de la investigación se extiendan.

Caso de ejemplo N° 1

Proceso penal bajo Número Único de Noticia Criminal 201300288 por el delito de hurto por medios informáticos y semejantes.

1. Hurto informático por medio de transacciones no autorizadas siendo víctima una empresa en la ciudad de Montería, hecho ocurrido el pasado 20 y 21 de junio de 2013.

Denuncia de los hechos

Yo, JCVD, mayor de edad, identificado como aparece al pie de la firma, en mi calidad de Gerente Operativo del Hotel S.A.S., por medio del presente escrito, con

todo respeto acudo ante su despacho con el objeto de formular denuncia escrita, bajo la gravedad del juramento, el cual se tipifica en los siguientes hechos.

HECHOS

PRIMERO. El día 20 de junio de 2013 a las 2:30 pm, El Sr. FN (Funcionario del Hotel), se encontraba en las instalaciones de la empresa consultando pagos a través del portal empresarial del Banco, cuando al tratar de entrar al portal observó que la página se bloqueó y luego lo sacó. No insistió en tratar de ingresar a la página y el computador fue desconectado de la red, pensando que era un problema de internet.

SEGUNDO. El día 21 de junio de 2013, a las 8:30 am, Se ingresó al portal empresarial para realizar consultas de pago y se verifico que habían sido realizadas 21 transferencias a otras cuentas bancarias desconocidas y no autorizadas continuando con el mismo problema de bloqueo.

TERCERO. Nos comunicamos inmediatamente con el Call Empresarial del banco donde nos informaron que efectivamente se realizaron las transferencias y se procedió a bloquear el usuario Portal Empresarial.

CUARTO. La pérdida total de la empresa asciende a la suma de $243.039.800 (Doscientos cuarenta y tres millones treinta y nueve mil ochocientos pesos M/cte.)

QUINTO. Por todo lo anterior, se hace necesario iniciar la respectiva investigación, ya que la empresa ha sufrido daño directo como consecuencia del injusto, tal y como lo señala el Artículo 132 del Código de Procedimiento Penal.

DERECHO

Fundo la presente denuncia en lo preceptuado por los artículos 66, 67 y siguientes

del código de procedimiento penal, al igual que las demás normas sustanciales y procesales concordantes.

ANEXOS

Me permito anexar a esta denuncia, copia de los siguientes documentos: Certificado de Existencia y Representación Legal del HOTEL S.A.S. RUT.

Listado de resumen de transacciones efectuadas y soporte electrónico remitido e-mail.

Análisis

Con relación a la ley 1273 de enero 05 de 2009, mediante la cual el gobierno sancionó la ley de la protección de la información y de los datos (más conocida como ley de delitos informáticos) y en la cual se tipificaron nuevas modalidades delictivas, siendo la de mayor pena la estipulada en al artículo 269i Hurto por medios Informáticos, no existe mucho conocimiento en la mayoría de los despachos fiscales respecto a la investigación de esta modalidad delictiva, que sin lugar a dudas afecta de una manera sorprendente el bolsillo de personas del común, como de empresas del sector privado y porque no del sector estatal.

En este caso especial y teniendo en cuenta el desconocimiento de la norma por parte de algunos funcionarios de diferentes despachos fiscales, el proceso estuvo rodando por diferentes despachos durante un periodo de 3 meses, basados en el concepto que por la cuantía de lo hurtado debería estar en fiscalía seccional y no en una local, ya que superaba para ese entonces el valor de los 150 SMMLV, sin tener en cuenta que la ley 1273 de 2009 enuncia en su artículo 3 que es competencia de los jueces penales municipales por lo cual debe también ser de conocimiento de fiscales locales, independiente de su cuantía por ser un delito que afecte el patrimonio económico; posterior a eso y luego de realizarse programa metodológico entre Policía Judicial y Fiscal al igual que las actuaciones

ordenadas, se solicitó a la señora Fiscal obtener la autorización con el fin de poder acceder a la base de datos de la entidad bancaria titular de las cuentas origen para de esta manera establecer a que entidad pertenecían las cuentas destino, al igual que la dirección IP utilizada para tal fin; cuando se hizo la solicitud al despacho fiscal, los despachos judiciales se encontraban en vacancia judicial (parte de diciembre y enero), conllevando a que de esta manera siga extendiéndose el tiempo de la investigación y llevando ya 7 meses de haber ocurrido los hechos denunciados.

La autorización se obtuvo para el mes de abril y las respuesta llegaron a mediados de mayo, algunas positivas otras negativas, ya que la normatividad (circular externa 042 de 2012 Superintendencia Financiera de Colombia) en el caso de material video gráfico y/o fotográfico de lugares comunes en las entidades bancarias exige que debe guardarse por un periodo mínimo de 8 meses y en caso de alguna queja, hasta que esta sea resuelta, sin embargo dicha situación no había sido solicitada al banco por lo cual al momento de solicitarse, la respuesta fue negativa.

Para el mes de julio ya se tenían identificadas, individualizadas las personas que habían recibido en dinero en sus cuentas, tal como lo había manifestado la entidad bancaria en sus respuestas, pero la fiscal coordinadora del caso generó nuevas actuaciones de Policía judicial, por medio de las cuales se obtuviera más información que permitiera el esclarecimiento de los hechos, las cuales se entregaron en septiembre de 2014.

Para octubre siguiente, se generaron nuevas órdenes a Policía Judicial las cuales se culminaron en el mismo mes, pero al momento de ser entregadas al fiscal coordinador del caso, no fue posible teniendo en cuenta el paro de actividades ordenado por el sindicato de empleados de la rama judicial, el cual duró más de un

mes y conllevó a que una vez se reiniciaran las actividades judiciales, la mayoría de despachos estuvieran nuevamente en vacancia judicial.

A inicios del 2015 y luego de varios tropiezos, el proceso investigativo fue trasladado a otro despacho fiscal esta vez una Fiscalía EDA, por sus siglas Estructura de Apoyo, la cual luego de analizar el caso y generar una serie de actividades, solicitó la expedición de 16 órdenes de captura durante el mes de junio de 2015, 11 de estas materializadas el mes siguiente a su expedición.

Actualmente de dicho proceso se han materializado 15 capturas, pero ninguna de las personas ha sido condenada a pesar de haber aceptado cargos en las diferentes audiencias, conllevando a que el tiempo de la investigación (51 meses) avance de una manera desmesurada y que la víctima no sea indemnizada, ya que la modalidad utilizada fue phishing, correo al cual uno de sus empleados accedió con el fin de “actualizar datos bancarios” y suministró los datos de acceso al ciberdelincuente, por lo que el banco luego de realizar sus respectivas investigaciones y análisis forenses, decidió no devolver el dinero al cliente, argumentando que las transacciones habían sido realizadas desde el mismo usuario autorizado para el cliente-victima, al igual que por no tener registrada una dirección IP única para acceder al portal virtual del banco.

Caso de ejemplo N° 2

Proceso penal bajo Número Único de Noticia Criminal 201500*** por el delito de hurto por medios informáticos y semejantes.

SDER, identificado con la cedula de ciudadanía N° ******* expedida en la ciudad de Montería, residente en la ciudad de Montería - Córdoba, muy respetuosamente me dirijo a usted, para presentar una denuncia penal, con base en los siguientes hechos:

Primero: Tengo una cuenta de ahorro en Bancolombia N° ******** desde alrededor 9 años.
Segundo: El día seis (6) de febrero de 2015 dejé un saldo que no refleja ninguna irregularidad en transacciones, que ascendía a la suma de $ 15.031.954.
Tercero: El día nueve (9) de febrero al sacar dinero del cajero, me di cuenta que no tenía el saldo esperado, ante lo cual procedí a llamar a la línea gratuita de Bancolombia donde me comunicaron al área de fraude y me confirmaron dos transacciones el día 7 de febrero por valor de $ 7.835.800 y $ 4.117.820 bajo el mismo concepto de PAGO TDA VIRTU PSE-ACH COLOM. Este mismo fraude le paso a una compañera el mismo día por un monto distinto.
Cuarto: El número de radicado de la queja bancaria es el ****** y que en 14 días hábiles me daban una respuesta.
Quinto: Como quiera que se me hurtó ese dinero, y se cometieron otros presuntos hechos punibles, pido a usted, adelantar todas las investigaciones pertinentes, con la práctica de pruebas viables, que conlleven a perseguir de los autores del ilícito, del cual soy víctima, y padeciendo graves perjuicios.
Estoy a su disposición para cualquier aclaración adicional.
Recibiré notificaciones en la indicada en el primer párrafo de la presente denuncia penal.

Análisis

En este caso y teniendo en cuenta la experiencia adquirida con ocasión al desarrollo del proceso penal descrito en el caso anterior, las diligencias fueron realizadas en un menor tiempo posible, a pesar de no contar con la respuesta dentro de los términos establecidos por parte de la entidad bancaria donde registraba la cuenta bancaria afectada, se pudo determinar la persona que recibió

los productos comprados utilizando la cuenta de ahorros de la víctima de los hechos.

Muy a pesar que la víctima denunció los hechos tan solo 48 horas después de la ocurrencia del mismo y que a su vez avisó ante mencionada entidad bancaria lo ocurrido, el banco no realizó las actividades correspondientes con el fin de impedir que la compra que ya se había efectuado y se había comprado por medio de una cuenta de ahorros que había sido accedida de manera no autorizada, el banco podía establecer a que empresa se había realizado la transacción y de esta manera impedir el despacho de los productos adquiridos, pues para nadie es un secreto que las empresas normalmente empiezan a despachar los productos adquiridos, 48 horas después de haberse efectuado la compra y más en este caso cuando se realizó un fin de semana.

La investigación se inició en febrero 09 de 2015 y para finales de mayo del mismo año, ya se tenía identificada e individualizada la persona que había recibido el producto comprado con el dinero hurtado de la cuenta afectada, al igual que se había establecido la empresa que vendió el producto, la empresa de mensajería que lo transportó, la modalidad de pago utilizada, la fecha, hora, minutos y segundos del momento en que se realizó cada una de las 4 transacciones no reconocidas por el cliente y la descripción de cada uno de los productos comprados utilizando la cuenta afectada, pero hasta la fecha de elaboración del presente documento, la Fiscalía no ha solicitado la orden de captura o ha generado nuevas órdenes a Policía Judicial por medio de las cuales los investigadores realicen nuevas actuaciones con el fin de recolectar más elementos materiales probatorios que sirvan para demostrar la autoría de la conducta punible investigada.

Con el material probatorio obtenido, se ha podido establecer que la entidad bancaria tardó aproximadamente quince días en solicitar a la entidad administradora de pagos electrónicos ACH – PSE, se estudiara la posibilidad de

reversar la compra efectuada desde la cuenta bancaria afectada, más sin embargo por parte de la entidad bancaria no se recibió respuesta a la petición originada dentro de la indagación adelantada.

1.21. CAPACIDADES FÍSICAS Y TECNOLÓGICAS CON QUE CUENTA LA POLICÍA NACIONAL PARA REALIZAR LAS ACTIVIDADES NECESARIAS Y QUE PERMITAN IDENTIFICAR LOS AUTORES DE HECHOS INVESTIGADOS.

Actualmente la Policía Judicial con sede principal del departamento de Córdoba en la ciudad de Montería, no cuenta con software licenciado para realizar imágenes forenses, ni con un laboratorio básico de informática forense por medio del cual se puedan realizar diferentes estudios o análisis a dispositivos tecnológicos utilizados para la ejecución de las diferentes modalidades delictivas dentro del delito de hurto por medios informáticos y semejantes, estudios con los cuales se pueda obtener material probatorio para demostrar la autoría o participación en una conducta punible que se investigue, actualmente solo cuenta con personal idóneo, capacitado y con experiencia en la investigación de delitos informáticos.

Mas sin embargo actualmente en la ciudad de Medellín se cuenta con un laboratorio regional que cubre los departamentos de Córdoba, Antioquia, Chocó y Urabá) de Policía Científica y Criminalística dentro del cual existe un laboratorio de informática forense, lugar en el cual aparte de las instalaciones, recursos físicos, tecnológicos, se cuenta también con personal capacitado (7 en total), que con su experiencia en el campo forense permite que el investigador obtenga más conocimientos sobre los análisis que allí se realizan y modalidad utilizada en cada caso investigado.

CONCLUSIONES

- En Colombia a pesar de que ya existe una ley (Ley 1273 de 2009) que castiga estos delitos, no existe el personal idóneo y capacitado que se dedique a investigar esta conducta delictiva, y a pesar que no existen cifras oficiales de policías dedicados a esta actividad, si existen cifras de uniformados que se deberían tener en cada municipio; según cifras oficiales por cada 100 mil habitantes en Bogotá hay 234 policías, y aunque la oficina para drogas y el delito de la Organización de las Naciones Unidas (ONU) recomienda tener 300 uniformados por cada 100 mil habitantes, en nuestro país no hemos podido alcanzar esta cifra, al igual que las herramientas tecnológicas suficientes con las cuales se puedan agilizar el esclarecimiento de los hechos investigados[4] [5].

- Fomentar ideas a las autoridades político administrativas y de Policía, por medio de las cuales se puedan realizar actividades de sensibilización con la comunidad a fin de darles a conocer las modalidades utilizadas por los delincuentes, y evitar que sean víctimas de las conductas delictivas, teniendo en cuenta que con los avances tecnológicos, la delincuencia también tiene nuevas metodologías para obtener de manera ilegal información, con la cual pueda realizar actividades ilegales por medios informáticos, afectando el bolsillo de los ciudadanos.

- Se ha logrado determinar e identificar las modalidades más comunes que utilizan los delincuentes informáticos en el departamento de córdoba como son las páginas web comerciales dedicadas a la venta de productos o a través de l cambiazo de tarjetas débito o crédito en los cajeros electrónicos de las diferentes entidades bancarias y clonación de tarjetas, esto se podría

[4] http://caracol.com.co/emisora/2016/10/04/bogota/1475582614_763546.html
[5] http://www.un.org/es/events/crimecongress2010/pdf/factsheet_ebook_es.pdf

reducir sensibilizando a la ciudadanía al no comprar en sitios no oficiales de las marcas y con campañas sociales de información.

- No existen las coordinaciones con las diferentes entidades bancarias, por medio de las cuales se puedan obtener respuestas oportunas, eficaz y eficiente, lo anterior teniendo en cuenta que las entidades se rigen según los términos establecidos en las búsquedas selectivas de bases de datos que se autoricen dentro de los procesos investigativos, conlleva a que los tiempos de respuesta para los investigadores al igual que de esclarecimiento de hechos, sean mayores, lo anterior según lo establecido en la normatividad vigente articulo 224 y 244 C.P.P. cuyos términos iniciales son de 15 y 30 días según la etapa en que se encuentre el proceso penal.

- Así mismo luego del análisis realizado a las denuncias realizadas durante los años 2015 y 2016 se pudo establecer que la modalidad más utilizada por los delincuentes informáticos es el cambiazo, ya que a través de esta pueden obtener de forma rápida el dinero y en efectivo.

- Basado en el número de denuncias (152 denuncias) radicadas durante los años 2015 y 2016 y comparado con el número de capturas (02 capturas) realizadas durante los años 2015 a 2016, los resultados obtenidos por las autoridades no compensan con el número de denuncias instauradas ante la Fiscalía General de la Nación, por lo cual es ideal que los entes del estado replanteen las acciones ejecutadas y permitan obtener mejores resultados.

- A pesar de que el proceso investigativo puede tardar más de 2 años, se puede analizar que durante los años 2017 y 2018 solo se evidencia 01 captura en el departamento de Córdoba por violación al artículo 269i de la ley 1273 de 2009, lo que conlleva a analizar que la actividad preventiva

realizada por las autoridades político administrativas y de Policía no ha sido efectiva.

- La normatividad existente en Colombia es muy flexible frente a este delito teniendo en cuenta que la pena establecida para este delito está entre 6 a 14 años, más aun cuando existen casos en los cuales las personas capturadas se acogen al derecho establecido en el artículo 269 C.P. que habla sobre la reparación (resarcir daños) lo que conlleva a que la pena pueda disminuirse de la mitad a las tres cuartas partes[6].

- La capacidad tecnológica de la Policía Nacional año tras año mejora a nivel central, por ejemplo en la ciudad de Bogotá la creación y puesta en funcionamiento (2017) del Centro de Comando, Control, Comunicaciones y Cómputo C4, a nivel local no se encontraron reportes en bases de datos, por lo que actualmente es necesario remitir las solicitudes al laboratorio regional ubicado en la ciudad de Medellín, lo cual conlleva a que pueda existir demora en las respuestas de solicitudes enviadas desde el departamento de Córdoba, ya que por ser regional debe atender casos de otros departamentos (Antioquia, Chocó y Urabá)[7].

[6] http://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf
[7] https://www.elespectador.com/noticias/bogota/ya-funciona-plenamente-el-c-4-el-corazon-de-la-seguridad-en-bogota-articulo-721944

DIVULGACIÓN

La presente investigación será divulgada a través del campus de la universidad Nacional Abierta y a Distancia, la cual servirá de referente ante futuras consultas que se lleguen a realizar sobre el delito de hurto por medios informáticos y semejantes, modalidades utilizadas por los delincuentes y variables que permiten la ejecución de la conducta punible.

REFERENCIAS BIBLIOGRÁFICAS

1) ALCALDIA DE BOGOTÁ. LEY 1273 DE 2009. Diario Oficial 47.223 de enero 5 de 2009 Bogotá. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

2) Bolaño, Andrés. Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica San Juan de Pasto, 2014, 100 p. Monografía (Especialización en Seguridad Informática). Universidad nacional Abierta y a Distancia, escuela de Ciencias Básicas Tecnología e Ingeniería.

3) CAMACHO LOSA, Luis. Delito Informático. Madrid. 1987. Gráficas Cóndor.

4) CARBAJAL, Cristian. Delitos informáticos {En línea}. Fecha. {26 de mayo de 2017}. Disponible en http://www.ilustrados.com/documentos/jp-Protocolo%20delitos%20informaticos.pdf

5) CERESOLE, A & OYARZABAL, Sergio. {En línea}. Fecha. {26 de mayo de 2017}. Disponible en: http://www.terragnijurista.com.ar/doctrina/Delitos_informaticos.pdf

6) CONDE, Hugo - GONZÁLES Cristóbal & HEREDIA Fecha. {26 de mayo de 2017}. Disponible en: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf

7) CORTÉS, Rodrigo - BALLÉN, Jhon & DUQUE Juan. La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. En: Revista de derecho comunicaciones y nuevas tecnologías. No 14 (Jul-Dic. 2015); p. 1-25.

8) Glosario de términos relacionados con los delitos informáticos. {En línea}. disponible en: http://www.educacion.gob.es/exterior/centros/ginerdelosrios/es/internet-seguro/DiccionarioDelitosTecnologicos.pdf

9) GONZÁLEZ HURTADO, Jorge. Delincuencia Informática: daños informáticos del artículo 264 del código penal y propuesta de reforma. Madrid, 2013, 408 p. Tesis doctoral (Derecho). Universidad Complutense de Madrid, facultad de derecho.

10) GUERRA VALDIVIA, Alicia. Delitos informáticos – caso de estudio. México, 2011, 144 p. Tesis de maestría (Tesis de grado (Maestro en ingeniería en seguridad y tecnologías de la información). Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica.

11) LEVENE, Ricardo. Delitos y Tecnología de la Información. Fecha. {26 de mayo de 2017}. Disponible en: http://www.delitosinformaticos.com/delitos/delitosinformaticos3.shtml

12) LÓPEZ GARCÍA, Elmer. Inclusión de los delitos informáticos, que se cometen en internet, dentro del Código Penal guatemalteco. Guatemala, 2011, 118 p. Tesis de grado (licenciado en ciencias jurídicas y sociales). Universidad de San Carlos de Guatemala. Facultad de ciencias jurídicas y sociales.

13) MANJARRÉS, I & JIMÉNEZ, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82. {En línea}. Fecha de consulta 25 de mayo de 2017. Disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

14) Martínez, S. Guía de apuntes básicos para el docente de la materia de técnicas de investigación en *Grupo Emergente de Investigación Oaxaca* [En línea] [Accesado el 27 de mayo de 2007] disponible en: http://geiuma-oax.net/invdoc/importanciaydef.htm

15) MONTAÑO ÁLVAREZ, Alejandro. La problemática jurídica en la regulación de los delitos informáticos. Ciudad Universitaria, 2013, 381 p. Tesis profesional (Licenciado en derecho). Universidad Nacional Autónoma de México, facultad de derecho.

16) OJEDA, Jorge – ARIAS, Miguel – RINCÓN, Fernando & DAZA, Libardo. Delitos informáticos y entorno jurídico vigente en Colombia. En: Cuadernos de Contabilidad. No 11 (28) (Ene – Jun 2010); p. 41 – 66.

17) ORTIZ MUÑOZ, Eberzon. Modalidades, participación y sanción en la comisión de delitos informáticos en Colombia a partir de la ley 1273 de 2009. Pereira, 2012, 71 p. Tesis de grado (Especialización en Derecho Penal y Criminología). Universidad Libre de Colombia, facultad de derecho.

18) PANDASECURITY. Phishing. Fecha. {26 de mayo de 2017}. Disponible en: http://www.pandasecurity.com/colombia/homeusers/security-info/cybercrime/phishing/

19) Proyecto fraudes informáticos. {En línea}. disponible en: http://fraudesinformaticos.es.tl/MARCO-TEORICO.htm

20) RECOVERYLABS. Definición de delitos informáticos. Fecha. {26 de mayo de 2017}. Disponible en: http://delitosinformaticos.info/delitos_informaticos/definicion.html

21) REPÚBLICA DE COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3854.

22) RODRÍGUEZ ÁLVAREZ, Juan. Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. {En línea}. Fecha. {26 de mayo de 2017}. Disponible en http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos%20en%20las%20Redes%20Sociales.pdf

23) RODRÍGUEZ FERNÁNDEZ, Alberto. Daños informáticos contra sistemas: el artículo 264 bis del código penal. {En línea}. Fecha de consulta 25 de mayo de 2017. Disponible en: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/ponencia%20Rodriguez%20Fernandez,%20Alberto.pdf?idFile=bd78e587-740d-4e30-abe4-ec7d2e0755dd

24) SUAREZ LEÓN, Sandra. Comisión de conductas punibles en la internet en Colombia. Bogotá, 2012, 53 p. Tesis de pregrado (Derecho). Universidad Militar Nueva Granada, facultad de derecho.

25) SUÁREZ-SÁNCHEZ, Alberto. La estafa informática, 45-46. Bogotá. 2009. Grupo Ibáñez.

26) TÉLLEZ VALDEZ, Julio. Derecho informático. 3ª ed. México. 2007. McGraw Hill.

27) VERNEY, Silvina. Delitos Informáticos. Fecha. {26 de mayo de 2017}. Disponible en: http://www.terragnijurista.com.ar/doctrina/informaticos.htm

28) VIEGA, María. Un nuevo desafío jurídico: los delitos informáticos. Fecha. {26 de mayo de 2017}. Disponible en: http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf

29) WIKIPEDIA. Concepción de seguridad de la información. Fecha. {26 de mayo de 2017}. Disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_información#Confidencialidad

30) WIKIPEDIA. Keylogger. Fecha. {26 de mayo de 2017}. Disponible en: https://es.wikipedia.org/wiki/Keylogger

31) WIKIPEDIA. Programa espía. Fecha. {26 de mayo de 2017}. Disponible en: https://es.wikipedia.org/wiki/Programa_espía

32) BALANTA, Heidy. Legislación que protege la información en Colombia. Derecho Informático. {En línea}. Fecha de consulta 03 de septiembre de 2017. Disponible en: http://derechoinformatico.co/legislacion-que-protege-la-informacion-en-colombia/.

33) PARRA ROJAS, Astrid & GRANADOS RAMÍREZ, Ricardo. 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. Cúcuta, 2016, 77 p. Tesis de pregrado (abogado). Universidad Libre de Colombia, facultad de derecho, ciencias políticas y sociales.

34) OJEDA-PÉREZ, Jorge Eliécer; RINCÓN-RODRÍGUEZ, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11* (28), 41-66.

35) CASTILLO, José Luis; BLANCO-PARRA, Brigido; PEREZ-FLOREZ, Reinaldo. (2016). La protección de la información y los datos como delito informático en Colombia: sanciones penales. Cúcuta, 2016. Tesis de maestría (derecho). Universidad Libre de Colombia, facultad de derecho, ciencias políticas y sociales.

36) ASOBANCARIA, qué es el cambiazo y como evitar caer en él. {19 de marzo de 2019}. Disponible en: https://www.asobancaria.com/sabermassermas/que-es-cambiazo-como-evitar-caer/

37) Corte Suprema de Justicia, Sala de Casación, proceso 42724, providencia SP1245-2015, disponible en http://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

38) UNODC Oficina de las Naciones Unidas Contra la Droga y el Delito, Brasil, abril de 2010, 12° Congreso de las Naciones Unidas Sobre Prevención del Delito y Justicia Penal.

39) (12 de Mayo de 2017). Recuperado el 12 de 05 de 2017, de https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

40) Alegsa, L. (05 de 12 de 2010). alegsa. Obtenido de http://www.alegsa.com.ar/Dic/delito_informatico.php

41) Avast. (s/f). Recuperado el 01 de 05 de 2017, de https://www.avast.com/es-es/c-malware

42) Avast. (s/f). Recuperado el 22 de 04 de 2017, de https://www.avast.com/es-es/c-malware

43) Balanta, H. (15 de Junio de 2014). Derecho Informático. Obtenido de http://derechoinformatico.co/legislacion-que-protege-la-informacion-en-colombia/

44) Cuadernos de contabilidad vol. 11 n° 28. (enero a diciembre de 2010). Delitos informáticos y entorno jurídico vigente en Colombia. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

45) BENEDETTI, A. (11 de Julio de 1992). DERECHO A LA INFORMACION Y VIDAD PRIVADA. EL TIEMPO.

46) Definición de fichero. (s/f). Recuperado el 12 de 05 de 2017, de http://www.definicionabc.com/acerca-de desconocido. (s.f.). Obtenido de http://penta.ufrgs.br/gereseg/unlp/t1abomba.htm

47) Dic, P. (01 de Agosto de 2009). la tecnologiavirtual. Obtenido de http://latecnologiavirtual.blogspot.com.co/2009/08/datos.html

48) EPN, E. P. (2017). http://epn.gov.co/. Obtenido de http://epn.gov.co/: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/13_riesgo_amenaza_y_vulnerabilidad.html

49) Española, G. d. (2016). For Larousse Diccionario Enciclopedico. Larousse .

50) habeas dat. (s.f.). Obtenido de http://www.habeasdat.com/faq.html

51) Informática hoy. (s.f.). Obtenido de http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php

52) Informático, d. d. (2015). Delitos informaticos.info. Obtenido de http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html

53) Isabella Gandini, A. I. (S/f). delta asesores. Recuperado el 10 de 05 de 2017, de http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

54) Kaspersky. (06 de 2017). https://latam.kaspersky.com/. Obtenido de https://latam.kaspersky.com/: https://latam.kaspersky.com/resource-center/threats/adware

55) Manjarres, I. &. (2012). caracterizacion de los delitos informaticos en colombia. Obtenido de http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

56) Merino., J. P. (2008). Recuperado el 05 de 05 de 2017, de definicion.de: http://definicion.de/hardware/

57) MINTIC. (04 de 01 de 2009). Recuperado el 31 de 03 de 2017, de http://www.mintic.gov.co/portal/604/w3-article-3705.html

58) Policía Nacional de Colombia, 15 de marzo de 2019. Recuperado el 16 de marzo de 2019 de https://www.policia.gov.co/grupo-informaci%C3%B3n-criminalidad/resultados-operativos

59) Policía Nacional de Colombia, 15 de marzo de 2019. Recuperado el 16 de marzo de 2019 de https://www.policia.gov.co/grupo-informaci%C3%B3n-criminalidad/estadistica-delictiva

60) MINTIC. (15 de 04 de 2016). Recuperado el 31 de 03 de 2017, de http://www.mintic.gov.co/portal/604/w3-article-15033.html

61) Molina, J. C. (18 de 09 de 2009). ugr. Obtenido de https://www.ugr.es/~derechosdeautor/colaboradores.html

62) País. (04 de 07 de 2016). 75% de la poblacion en Colombia ha utilizado internet durante el último mes. Obtenido de http://www.dinero.com/pais/articulo/el-75-de-la-poblacion-en-colombia-ha-utilizado-internet-en-el-ultimo-mes/222137

63) Pérez, J. (2008). Definición de. Recuperado el 12 de 05 de 2017, de http://definicion.de/informatica/

64) proteccion on line. (s/f). Recuperado el 12 de 05 de 2017, de http://www.proteccionline.com/que-es-el-smishing/

65) Prto, J. P. (2016). definicion.de . Recuperado el 12 de 05 de 2017, de http://definicion.de/base-de-datos/

66) Rouse, M. (s/f). TechTarget. Recuperado el 28 de 04 de 2017, de http://searchdatacenter.techtarget.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion

67) seguridad pc. (s/f). Recuperado el 02 de 05 de 2017, de http://www.seguridadpc.net/spam.htm

68) SIA. (09 de 03 de 2017). SIA. Recuperado el 31 de 03 de 2017, de SERVICIO DE INFORMACION ATLAS: http://sia-atlas.com.co/index.php/informe-preventivo/los-delitos-informaticos-mas-comunes-en-colombia

69) Tecnosfera, Redaccion. (27 de 01 de 2016). El Tiempo. Recuperado el 31 de 03 de 2017, de http://www.eltiempo.com/archivo/documento/CMS-16493604

70) Valdez, J. T. (2009). Derecho informatico . Mexico : Mc Graw Hill.

71) Wikipedia. (17 de Agosto de 2011). Obtenido de https://es.wikipedia.org/wiki/C%C3%B3digo_fuente

72) wikipedia. (03 de marzo de 2014). Recuperado el 01 de mayo de 2017, de https://es.wikipedia.org/wiki/Sistema_inform%C3%A1tico

73) Wikipedia. (24 de 11 de 2014). Recuperado el 12 de 05 de 2017, de https://es.wikipedia.org/wiki/Defacement

74) Wikipedia. (31 de Octubre de 2015). Recuperado el 24 de Abril de 2017, de https://es.wikipedia.org/wiki/Software

75) Wikipedia. (16 de 01 de 2016). Recuperado el 12 de 05 de 2017, de https://es.wikipedia.org/wiki/Sabotaje

76) wikipedia. (03 de 05 de 2017). wikipedia. Recuperado el 03 de 05 de 2017, de https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

77) wikipedia. (s/f). Recuperado el 01 de 05 de 2017, de https://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica)

78) wikipedia. (S/F). Recuperado el 12 de 05 de 2017, de https://es.wikipedia.org/wiki/Internet

79) Wikipedia. (s/f). Recuperado el 28 de 04 de 2017, de https://es.wikipedia.org/wiki/Intimidad

80) Wikipedia. (s/f). Recuperado el 12 de 05 de 2017, de https://es.wikipedia.org/wiki/Red_social

81) Wikipedia. (s/f). Recuperado el 02 de 05 de 2017, de https://es.wikipedia.org/wiki/Programa_esp%C3%ADa

82) Wikipedia. (s/f). Recuperado el 12 de 05 de 2017, de https://es.wikipedia.org/wiki/Vishing

83) Redacción. (07 de noviembre de 2017). El Espectador. Recuperado el 18 de 03 de 2019, de https://www.elespectador.com/noticias/bogota/ya-funciona-plenamente-el-c-4-el-corazon-de-la-seguridad-en-bogota-articulo-721944

Anexo I Resumen Analítico en Educación - RAE

1. Información General	
Tipo de documento	Monografía para obtener el título de Especialista en Seguridad Informática.
Acceso al documento	Universidad Nacional Abierta y a Distancia (UNAD) Facultad de Ciencias Básicas, Tecnología e Ingeniería. Programa de Especialización en Seguridad Informática.
Título del documento	Análisis del aumento en el hurto informático en el departamento de Córdoba durante los años 2015 y 2016.
Autor(es)	Devia Orozco, William Guillermo - Martínez Muñoz, Mauricio Miguel
Director	Peña Hidalgo, Hernando José
Publicación	Digitado en computador
Unidad Patrocinante	Universidad Nacional Abierta y a Distancia (UNAD) Facultad de Ciencias Básicas, Tecnología e Ingeniería Programa de Especialización en Seguridad Informática
Palabras Claves	Amenaza, riesgos, vulnerabilidad, Antivirus, Ataques, seguridad, Autenticación, Cambiazo, Clonación, Disponibilidad.

2. Descripción

En el informe de trabajo de grado los autores plantean cómo en el departamento de Córdoba y según la estadística de denuncias instauradas, el principal delito denunciado dentro de los consagrados en la ley 1273 de 2009, es el hurto por medios informáticos y semejantes ya sea por medio de páginas comerciales dedicadas a la venta de productos o a través del cambiazo de tarjetas débito o crédito en los cajeros electrónicos de las diferentes entidades bancarias, modalidad en la cual el delincuente, normalmente dos personas, simulan brindar una ayuda al tarjeta habiente que se encuentra en el cajero y mientras uno le cambia la tarjeta, el otro observa la clave de uso para posteriormente realizar retiros, compras, transacciones, que en su mayoría de casos superan los dos millones de pesos, esto cuando momentos después el cliente se da cuenta, debido a las notificaciones enviadas vía mensajes de texto o correo electrónico por parte de la entidad bancaria con relación a las transacciones efectuadas desde sus cuentas bancarias o tarjetas de crédito, a raíz de lo anteriormente descrito, y mientras el gobierno nacional no implemente la capacitación de personal idóneo para la investigación de denuncias por delitos informáticos, realice un plan de choque para disminuir dicha actividad ilegal, los delitos informáticos en todas sus modalidades principalmente el hurto por medios informáticos, no parará, por lo cual se hace necesario implementar desde los hogares y empresas medidas preventivas que permitan minimizar riesgos impidiendo así ser víctimas de este flagelo.

3. Fuentes
Los autores presentan 9 referencias relacionadas con los planteamientos realizados.
• Rodríguez, J (2011) Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. • Bolaño, Andrés. Análisis comparativo sobre delitos informáticos en

Colombia con relación a seis países de Latinoamérica San Juan de Pasto, 2014, 100 p. Monografía (Especialización en Seguridad Informática). Universidad nacional Abierta y a Distancia, escuela de Ciencias Básicas Tecnología e Ingeniería.

- PARRA ROJAS, Astrid & GRANADOS RAMÍREZ, Ricardo. 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. Cúcuta, 2016, 77 p. Tesis de pregrado (abogado). Universidad Libre de Colombia, facultad de derecho, ciencias políticas y sociales.

- González, J (2013) Delincuencia Informática: daños informáticos del artículo 264 del código penal y propuesta de reforma. Madrid, 2013, 408 p. Tesis doctoral (Derecho). Universidad Complutense de Madrid, facultad de derecho

- Montaño, A (2013). La problemática jurídica en la regulación de los delitos informáticos. Ciudad Universitaria, 2013, 381 p. Tesis profesional (Licenciado en derecho). Universidad Nacional Autónoma de México, facultad de derecho.

- Guerra, A (2011) Delitos informáticos – caso de estudio. México, 2011, 144 p. Tesis de maestría (Tesis de grado (Maestro en ingeniería en seguridad y tecnologías de la información). Instituto Politécnico Nacional. Escuela Superior de Ingeniería Mecánica y Eléctrica.

- Suarez, S (2012) Comisión de conductas punibles en la internet en Colombia. Bogotá, 2012, 53 p. Tesis de pregrado (Derecho). Universidad Militar Nueva Granada, facultad de derecho

- Balanta, H (2014). Legislación que protege la información en Colombia.

Derecho Informático.

- Ojeda, J – Arias, M – Rincón, F & Daza, L (2010). Delitos informáticos y entorno jurídico vigente en Colombia.

4. Contenidos

El presente informe de trabajo de grado, contiene una propuesta que busca promover la práctica y enseñanza del dibujo de una forma distinta a la tradicional, presenta un ambiente virtual de aprendizaje (AVA) como herramienta pedagógica que puede favorecer a niños y jóvenes en la creación de nuevas formas narrativas, dando una mirada a un panorama donde los niños y jóvenes podrán experimentar con el aprendizaje del dibujo, donde se les abrirán las posibilidades de contar historias, enseñar a sus pares la técnica del dibujo de una forma más sencilla y finalmente publicar sus creaciones; pretende incentivar la capacidad creadora de los niños y jóvenes, además de reivindicar la importancia del dibujo en su proceso de aprendizaje y que experimenten cómo plasmar sus ideas, imaginarios, fantasías y realidades por medio del gráfico, que comuniquen sus sentimientos y emociones sin temor a ser censurados. Para esto se han tenido en cuenta diferentes trabajos de grado sobre narrativas gráficas, libros de enseñanza y aprendizaje del dibujo de una forma virtual.

El informe se divide en:

1. Antecedentes: los cuales brindan una guía, sobre la pertinencia y aplicabilidad para el diseño de la propuesta
2. Planteamiento del problema: Allí se evidenciarán las dificultades que existen por el hurto en medios informáticos
3. Justificación: Muestra la importancia de fomentar ideas a las autoridades político administrativas y de Policía, por medio de las cuales se puedan

realizar actividades de sensibilización con la comunidad a fin de darles a conocer las modalidades utilizadas por los delincuentes

4. Alcance y delimitación: Marcan el horizonte por el cual debe ir encaminado el trabajo y las pretensiones del mismo.
5. Objetivos: Con base en el planteamiento problema, allí están planteadas las posibles soluciones y que se quiere lograr
6. Metodología del trabajo: Se encuentran las fases de desarrollo del trabajo, desde la contextualización hasta la aplicación y análisis del mismo.
7. Marco teórico: Se encuentra un recorrido de como los clientes/usuarios permiten que se materialicen los riesgos de ser víctima de un hurto informático
8. Propuesta: allí se encuentran los aspectos generales de la misma, así como la población, la temática, las características y las actividades.
9. Conclusiones: están consignados los logros, aciertos y desaciertos obtenidos con la propuesta.

Bibliografía: autores citados, libros, trabajos y páginas utilizadas como guía para el trabajo en general.

5. Metodología

La metodología a realizar en esta monografía es de tipo descriptiva, documental y jurídica, ya que el objetivo principal de este tipo de investigación busca llegar a conocer actitudes o situaciones que se han presentado, en nuestro caso el hurto informático en el departamento de Córdoba durante los años 2015 y 2016.

Descriptiva porque con ella se va a dar a conocer las modalidades utilizadas por los delincuentes para concurrir en el delito de hurto informático en el departamento de Córdoba durante los años 2015 y 2016.

Documental ya que es basada en la estadística existente en bases de datos de empresas del estado, en las que se analizaran la modalidad realizada en cada caso denunciado.

Jurídica ya que pretende demostrar el aumento de denuncias por el delito de hurto informático en el departamento de Córdoba, tipificado en el artículo 269i de la Ley 1273 de 2009 la cual aumentó tipos penales en la ley 599 de 2000.

6. Conclusiones

En Colombia a pesar de que ya existe una ley (Ley 1273 de 2009) que castiga estos delitos, no existe el personal idóneo y capacitado que se dedique a investigar esta conducta delictiva, y a pesar que no existen cifras oficiales de policías dedicados a esta actividad, si existen cifras de uniformados que se deberían tener en cada municipio; según cifras oficiales por cada 100 mil habitantes en Bogotá hay 234 policías, y aunque la oficina para drogas y el delito de la Organización de las Naciones Unidas (ONU) recomienda tener 300 uniformados por cada 100 mil habitantes, en nuestro país no hemos podido alcanzar esta cifra, al igual que las herramientas tecnológicas suficientes con las cuales se puedan agilizar el esclarecimiento de los hechos investigados[8] [9].

Fomentar ideas a las autoridades político administrativas y de Policía, por medio de las cuales se puedan realizar actividades de sensibilización con la comunidad a fin de darles a conocer las modalidades utilizadas por los delincuentes, y evitar que sean víctimas de las conductas delictivas, teniendo en cuenta que con los avances tecnológicos, la delincuencia también tiene nuevas metodologías para obtener de manera ilegal información, con la cual

[8] http://caracol.com.co/emisora/2016/10/04/bogota/1475582614_763546.html
[9] http://www.un.org/es/events/crimecongress2010/pdf/factsheet_ebook_es.pdf

pueda realizar actividades ilegales por medios informáticos, afectando el bolsillo de los ciudadanos.

Se ha logrado determinar e identificar las modalidades más comunes que utilizan los delincuentes informáticos en el departamento de córdoba como son las páginas web comerciales dedicadas a la venta de productos o a través de l cambiazo de tarjetas débito o crédito en los cajeros electrónicos de las diferentes entidades bancarias y clonación de tarjetas, esto se podría reducir sensibilizando a la ciudadanía al no comprar en sitios no oficiales de las marcas y con campañas sociales de información.

No existen las coordinaciones con las diferentes entidades bancarias, por medio de las cuales se puedan obtener respuestas oportunas, eficaz y eficiente, lo anterior teniendo en cuenta que las entidades se rigen según los términos establecidos en las búsquedas selectivas de bases de datos que se autoricen dentro de los procesos investigativos, conlleva a que los tiempos de respuesta para los investigadores al igual que de esclarecimiento de hechos, sean mayores, lo anterior según lo establecido en la normatividad vigente articulo 224 y 244 C.P.P. cuyos términos iniciales son de 15 y 30 días según la etapa en que se encuentre el proceso penal.

Así mismo luego del análisis realizado a las denuncias realizadas durante los años 2015 y 2016 se pudo establecer que la modalidad más utilizada por los delincuentes informáticos es el cambiazo, ya que a través de esta pueden obtener de forma rápida el dinero y en efectivo.

Basado en el número de denuncias radicadas durante los años 2015 y 2016 y comparado con el número de capturas realizadas durante los años 2015 a 2018, los resultados obtenidos por las autoridades no compensan con el número de denuncias instauradas ante la Fiscalía General de la Nación, por

lo cual es ideal que los entes del estado replanteen las acciones ejecutadas y permitan obtener mejores resultados.

La normatividad existente en Colombia es muy flexible frente a este delito teniendo en cuenta que la pena establecida para este delito está entre 6 a 14 años, más aun cuando existen casos en los cuales las personas capturadas se acogen al derecho establecido en el artículo 269 C.P. que habla sobre la reparación (resarcir daños) lo que conlleva a que la pena pueda disminuirse de la mitad a las tres cuartas partes.

La capacidad tecnológica de la Policía Nacional sigue igual pero aun ubicada en la ciudad de Medellín a través del laboratorio regional, lo cual conlleva a que pueda existir demora en las respuestas de solicitudes enviadas desde el departamento de Córdoba, ya que por ser laboratorio regional debe atender casos de otros departamentos.

Elaborado por:	Devia Orozco, William Guillermo- Martínez Muñoz, Mauricio Miguel		
Revisado por:			
Fecha de elaboración del Resumen:	01	03	2019