Fecha de recepción: 12 de julio de 2015 / Fecha de aprobación: 2 de octubre de 2015

Revista de Derecho Comunicaciones y Nuevas Tecnologías

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

Rodrigo Cortés Borrero

Jhon Alexander Ballén Rojas

Juan José Duque Montes

Artículo de investigación científica y tecnológica

DOI: http://dx.doi.org/10.15425/redecom.14.2015.05

Universidad de los Andes

Facultad de Derecho

Rev. derecho comun. nuevas tecnol.

No. 14, julio - diciembre de 2015. ISSN 1909-7786

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

Resumen

El mundo jurídico y la sociedad actual se enfrentan a una nueva clase de delitos: los delitos informáticos. Dichas conductas se empezaron a discutir desde la década de los ochenta, sin embargo, en Colombia no es sino hasta el año 2009 con la Ley 1273 que se logra tener una herramienta para castigarlos y proteger el nuevo bien jurídico de *la información y los datos*. Esta ley plantea nuevos retos para la administración de justicia en la persecución penal de estas conductas. Este artículo presenta la investigación cualitativa adelantada para describir la efectividad judicial de la persecución penal de los delitos informáticos en el Distrito Judicial de Villavicencio (Meta), trabajo que implicó la realización de entrevistas a los funcionarios públicos (fiscales) y el ejercicio del derecho de petición para el acceso a la información pública. El trabajo confirma la tesis de la criminología crítica, que considera insuficiente la consagración de un tipo penal para que exista una efectiva materialización de la persecución penal que es, de acuerdo con esta teoría, selectiva. Los delitos informáticos, y esta es la conclusión parcial de este trabajo, no están siendo conocidos por el sistema penal colombiano debido a la ausencia de denuncias o de mecanismos adecuados de investigación oficiosa en la etapa de indagación penal. Ambos fenómenos, que constituirían hipótesis de trabajo, podrían ser nuevos campos de investigación sociojurídica en el derecho penal.

Palabras clave: criminología crítica, delitos informáticos, derecho penal especial, información y datos, Ley 1273 de 2009.

The legal prosecution of cyber crime in the judicial district of Villavicencio

Abstract

The legal world and society today face a new kind of crime: cyber crime. Although this has been a topic of discussion since the 1980s, it was not until 2009 when Colombia enacted the Law of 1273 which serves a tool to punish those who carry out cyber crimes and to provide new legal protections to information and data. This law presents new challenges for the administration of justice in the criminal prosecution of cyber crime. This article uses advanced qualitative research to describe the legal effectiveness of the prosecution of cyber crime in the Judicial District of Villavicencio (Meta). Such work involved interviewing public officials (prosecutors) and the use of the right of request for access to public information. The study confirms the thesis of critical criminology, which considers the perpetration of a criminal offense insufficient to ensure effective realization of criminal prosecution which is, according to this theory, selective. The partial conclusion of this work is that the Colombian penal system is failing to recognize cyber crime due to the absence of complaints or the appropriate investigative mechanisms at the criminal investigative stage. Both of these phenomena are working hypotheses, which could be new fields of socio-legal research in criminal law.

Keywords: critical criminology, cyber crime, specific criminal law, information and data, Law 1273 of 2009.

A persecução judicial contra os delitos informáticos no distrito judicial de Villavicencio

Resumo

O mundo jurídico e a sociedade atual se enfrentam a um novo tipo de delitos: os delitos informáticos. Ditas condutas começaram a ser discutidas desde a década de oitenta, porém, na Colômbia não é senão até o ano 2009 com a Lei 1273 que se consegue ter uma ferramenta para castigá-los e proteger o novo bem jurídico d*a informação e dos dados*. Esta lei propõe novos desafios para a administração de justiça na persecução penal destas condutas. Este artigo apresenta a investigação qualitativa realizada para descrever a efetividade judicial da persecução penal dos delitos informáticos no Distrito Judicial de Villavicencio (Meta), trabalho que implicou a realização de entrevistas aos funcionários públicos (fiscais) e o exercício do direito de petição para o acesso à informação pública. O trabalho confirma a tese da criminologia crítica, que considera insuficiente a consagração de um tipo penal para que exista uma efetiva materialização da persecução penal que é, de acordo com esta teoria, seletiva. Os delitos informáticos, e esta é a conclusão parcial deste trabalho, não estão sendo conhecidos pelo sistema penal colombiano devido à ausência de denúncias ou de mecanismos adequados de investigação oficiosa na etapa de indagação penal. Ambos os fenômenos, que constituiriam hipótese de trabalho, poderiam ser novos campos de investigação sócio jurídica no direito penal.

Palavras-chave: criminologia crítica, delitos informáticos, direito penal especial, informação e dados, Lei 1273 de 2009.

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

Rodrigo Cortés Borrero**

Jhon Alexander Ballén Rojas***

Juan José Duque Montes****

Sumario

Introducción – I. PROYECTO DE INVESTIGACIÓN – II. MARCO TEÓRICO – *A. Los delitos informáticos – B. La criminología crítica – C. Tipología de los delitos informáticos – D. El perfil del ciberdelincuente – E. Política pública de ciberseguridad en Colombia* – III. METODOLOGÍA – IV. RESULTADOS – *A. Las denuncias penales – B. Las condenas penales en Villavicencio – C. La Fiscalía, el CTI y su capacidad para enfrentar la cibercriminalidad desde la perspectiva oficial. – D. La perspectiva interna – 1. Composición de la Unidad Especializada de Delitos Informáticos – 2. Fiscales asignados para esta Unidad – 3. Funciones desplegadas por esta Unidad Especializada – 4. Capacitaciones – 5. Recursos de esta Unidad para perseguir los delitos – 6. Recursos tecnológicos – 7. Presupuesto – 8. Cooperación con otros sectores – 9. Cantidad de investigaciones desplegadas por la Unidad* – V. DISCUSIÓN – VI. CONCLUSIONES – Referencias.

* Cómo citar este artículo: Cortés Borrero, R., Ballén Rojas, J. A., Duque Montes, J. J. (Diciembre, 2015). La persecución judicial contra los delitos informáticos en el Distrito Judicial de Villavicencio. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* 14. Universidad de los Andes (Colombia).

** Abogado Summa Cum Laude; especialista en Derecho Administrativo; conciliador en Derecho; magíster (-c-) en Derecho Contractual Público y Privado de la Universidad Santo Tomás, sede Villavicencio; docente investigador y director del Semillero de Derecho Informático y de las Tecnologías en la Sociedad de la Información (DITSI) de la misma Universidad.

*** Abogado Summa Cum Laude, Universidad Santo Tomás. Docente investigador y conciliador en Derecho de la misma Universidad. Especialista en Derecho Constitucional y máster en Democracia y Buen Gobierno, Universidad de Salamanca (España).

**** Abogado, especialista en Derecho Administrativo de la Universidad Nacional de Colombia. Docente investigador y conciliador en Derecho, Universidad Santo Tomás. Actual secretario del Juzgado Segundo Civil Municipal de Descongestión de Villavicencio.

Introducción

Internacionalmente se había visto la necesidad de implementar en las distintas legislaciones la tipificación de las conductas que estaban poniendo en aprietos a la sociedad en el aspecto informático. En las décadas de los sesenta y setenta no se logra una uniformidad de conceptos ni colaboración, tampoco se le da relevancia al aspecto penal que surgía de las tecnologías informáticas. No es sino hasta 1983 que se logra consolidar el primer paso en el derecho penal para con estas nuevas conductas punibles.

En 1983, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) inició un estudio sobre las posibilidades de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas computacionales (Segu-Info, 2009).

En Colombia, el primer antecedente es el Decreto 1360 de 1989 que reglamenta la inscripción del soporte lógico (*software*) en el Registro Nacional de Derecho de Autor, y sirvió como fundamento normativo para resolver reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha comenzó a tener asidero jurídico la protección de la producción intelectual de los creadores de aplicativos y soluciones informáticas, a pesar de que desde 1995 el país contaba:

> Con una alianza estratégica entre sector público y sector privado, denominada CONVENIO ANTIPIRATERÍA PARA COLOMBIA, para enfrentar la lucha contra la piratería de obras y prestaciones intelectuales, es decir, de las obras protegidas por el derecho de autor y las prestaciones protegidas por los derechos conexos. (Torres, 2005, pág. 1).

En el marco internacional, a mediados de 1992:

> La Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos. (Segu-Info, 2009, pág. 1).

> Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** [negrillas en el original] como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. (Segu-Info, 2009, pág. 1).

La anterior definición "fue elaborada por un Grupo de Expertos, invitados por la OCDE a París en mayo de 1993" (Segu-Info, 2009, nota 3).

Así mismo las recomendaciones del XV Congreso Internacional de Derecho Penal (1994), uno de cuyos temas fue "Los delitos informáticos y otros delitos relativos a la tecnología de la información", reconocieron la emergencia de nuevos bienes jurídicos ante las transformaciones de la tecnología.

Transcurrieron varios años en la década de los noventa en nuestro país, para que hubiera la vo-

luntad política que impulsara una respuesta a las nuevas conductas delictivas. Con la llegada del nuevo milenio se replantea el Código Penal colombiano mediante la Ley 599 de 2000, que en su capítulo séptimo, del libro segundo, título III, regula los delitos contra la libertad individual y otras garantías, y la violación a la intimidad, reserva e interceptación de comunicaciones. Los tipos penales creados fueron los siguientes: violación ilícita de comunicaciones (artículo 192); ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas (artículo 193); divulgación y empleo de documentos reservados (artículo 194); acceso abusivo a un sistema informático (artículo 195); violación ilícita de comunicaciones o correspondencia de carácter oficial (artículo 196) y utilización ilícita de equipos transmisores o receptores (artículo 197).

Respecto a las anteriores inclusiones al Código Penal, Salazar (2009, pág. 97) señala:

> Tímidamente, el legislador colombiano de 2000 introdujo al Código Penal un tipo que denominó acceso no autorizado a un sistema informático, el cual confería al infractor una multa como sanción. La norma estuvo vigente durante nueve años, sin que hubiese sido estrenada en la práctica judicial, denotando su rampante ineficacia, al no haber contemplado una sanción más drástica para el transgresor.

Con este replanteamiento del Código Penal se inicia una serie de modificaciones en normas nacionales, acordes con la importancia de los medios tecnológicos como instrumentos para la ejecución de delitos y pasaron a ser sancionables las conductas de almacenamiento e intercambio de la pornografía infantil (Ojeda, Rincón, Arias y Daza, 2010).

El 23 de noviembre del 2001, en Budapest, el Consejo de Europa logró constituir el primer escrito internacional con fuerza vinculante para los países europeos sobre los delitos informáticos: el *Convenio sobre la ciberdelincuencia*.

Con los anteriores precedentes, tanto en el plano internacional como en el nacional se logra constatar que se requería de una norma que tratara de unos delitos en crecimiento y gran impacto que no tenían desarrollo ni tratamiento en Colombia por parte del Código Penal del 2000. Es por ello que se impulsa y se logra materializar la Ley 1273 de 2009 que consagra los delitos informáticos.

Como lo explica Salazar (2009, pág. 98):

> No es hasta 2009 que el legislador colombiano finalmente hace una adición al catálogo delictual, a través de la expedición de la Ley 1273, conocida como Ley de Delitos Informáticos. Al crear un nuevo bien jurídico tutelado, denominado la información y los datos, la norma consagra una decena de tipos que condenan el actuar de la criminalidad informática. Interesantemente, la expedición de la norma se dio gracias al impulso académico del juez Alexánder Díaz García y del profesor Harvey Rincón Ríos, quienes, fundamentados en el convenio de Budapest de 2001, redactaron el proyecto de ley que se convirtió en la mencionada Ley de Delitos Informáticos.[1]

1 En el mismo sentido, ver Ojeda et al., 2010.

Con ello, Colombia se ubicó en el mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron a nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de sus países miembros, mediante el Convenio sobre la cibercriminalidad, vigente desde julio de 2004. Con los desarrollos jurídicos hasta ahora logrados para "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las organizaciones pueden amparar gran parte de sus sistemas integrados de información: datos, procesos, políticas, talento humano, accesos, partidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo, de manera que además de contribuir a asegurar las características de calidad de la información se incorpora la administración y el control, en el concepto de protección integral.

Por ende, la Ley 1273 de 2009 es un gran avance en la manera como se pretende contrarrestar los delitos informáticos en Colombia, lo que hace necesario estar preparados íntegramente en los sectores público y privado para enfrentar los desafíos que emergerán en la cotidianidad, con una adecuada capacitación a los operadores jurídicos y políticas que prevengan y sancionen los delitos tipificados.

Debido a estas realidades a que se enfrenta la sociedad colombiana y el aparato estatal de persecución al delito en sus campos de policía judicial, fiscalía y jueces se realizó la investigación para conocer cómo en nuestra región se le ha dado aplicación a esta norma, e identificar las herramientas que poseen los funcionarios investigadores, conocer su compresión de las normas penales y, sobre todo, saber cómo en la realidad la confrontan.

I. PROYECTO DE INVESTIGACIÓN

El proyecto se inició por una situación evidente: las condenas por delitos informáticos son bajas en Colombia. Únicamente se registran 206 del universo de 170.195 impuestas por los jueces penales de conocimiento (Instituto Nacional Penitenciario y Carcelario [INPEC], 2013). Las anteriores razones llevaron a formular la pregunta: ¿Cómo ha sido la persecución criminal de los delitos informáticos, desde su investigación hasta su judicialización en el Distrito Judicial de Villavicencio en el periodo 2011-2012?

El objetivo general del proyecto fue responder dicha pregunta de investigación y los siguientes cuatro objetivos específicos:

- Determinar cuántas investigaciones criminales por delitos informáticos se tramitaron en la Fiscalía Seccional de Villavicencio.

- Determinar cuántos procesos penales fueron tramitados desde sus etapas de judicialización.

- Diagnosticar cuáles son los recursos físicos, tecnológicos y de talento humano con los que cuenta la policía judicial para contrarrestar los delitos informáticos.

- Indagar cómo afrontan los procesos por delitos informáticos el Fiscal, la policía judicial y el juez.

II. MARCO TEÓRICO

A. Los delitos informáticos

El delito informático, concebido desde el punto de vista doctrinal, tiene todo un concepto progresivo que desde los albores de la tecnología informática y los ordenadores ha venido transformándose.

En el derecho penal, específicamente en lo referente a los delitos informáticos se han constituido diversos puntos de vista teóricos sobre su definición. La doctrina ha hecho un gran trabajo al tratar de dilucidar un concepto uniforme, internacional e íntegro; los variados conceptos que han surgido en distintas épocas y desde distintas áreas, como el derecho, la ingeniería, la ciencia, entre otras, son los siguientes:

La definición genérica es la dada por OCDE en 1983: "Cualquier conducta ilegal o no autorizada que involucre el procesamiento de datos y/o la transmisión de datos."

Para Irving J. Sloan (1984, pág. 2) un delito informático (*computercrime*) "consiste en el uso de una computadora como instrumento de un delito económico."

Lima de la Luz (1984, pág. 100) lo define como una conducta:

> En sentido amplio (...) que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel como método, medio o fin.

Para Luis Camacho Losa (1987) es: "Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material, técnico, e informático, o que están en relación significativa con esta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos" (págs. 45-46).

Rivera Llano (1995, pág. XIII) lo define como "aquellas conductas ilícitas, realizadas a través de las computadoras, empleadas como método, medio o fin, con peculiaridades."

Choclán Montalvo (1997, págs. 22-28) considera que "la especificidad del delito informático le viene dada por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial."

Así mismo, son delitos mediante sistemas informáticos todos aquellos comportamientos determinados por el legislador, los cuales no tienen un objeto material determinado pero, en los que el modus operandi es compuesto por tecnologías de la informática, de manera que en la comisión del delito han de intervenir, como medio, las tecnologías utilizadas para el procesamiento de la información.

En Colombia, entre quienes han tratado el tema, podemos referir a Henry William Torres-Torres (2002), ya que amplía el concepto a lo internacional:

> Toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software a que sin estar reconocida [sic] por nuestro legislador es aceptada por tratadistas internacionales como Infracción Informática. (Pág. 40).

Davara Rodríguez (2006, págs. 358-359) define este delito así: "La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software."

Téllez-Valdés (2007), 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)."

Suárez-Sánchez, por su parte, señala:

> En conclusión, el delito informático está vinculado no solo 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* como bien jurídico tutelado, diferente de los intereses jurídicos tradicionales. (2009, págs. 45-46).

Castro Ospina (2002) los define como: "Aquellas conductas típicas, antijurídicas y culpables que lesionan la seguridad informática de los sistemas tecnológicos y dirigidas contra bienes intangibles como datos, programas, imágenes y voces almacenados electrónicamente."

El delito informático también se conoce con el término anglosajón *computercrime,* y se sabe que quienes cometen estos delitos son expertos conocedores de la tecnología, con fundamento científico e investigativo de los sistemas y también del comportamiento humano y organizacional. Otra característica importante es que el atractivo del delito no siempre es el aspecto económico, sino que puede obedecer a intereses de diverso orden, como los personales, psicológicos, sociales, laborales, políticos o de simple curiosidad tecnológica. Paradójicamente, sus ejecuciones están cubiertas o protegidas por la misma seguridad que ofrece la tecnología informática.

Para concluir, la definición más acertada que se derive de toda la teoría expuesta debe reconocer los elementos que da el legislador en Colombia y llevarlos a lo más abstracto. En este entendido proponemos la siguiente definición: toda conducta punible, es decir típica, antijurídica y culpable señalada por el legislador; haciendo uso indebido de la información y de cualquier medio informático empleado para su manejo, o de la tecnología electrónica o computariza-

da, como método, medio o fin que menoscabe, mengüe o ponga en riesgo el bien jurídico de la información y de los datos; además que con ocasión de ellos en circunstancias específicas se pueda afectar otros bienes jurídicos como la vida, la libertad, la familia, el patrimonio, la seguridad pública y la seguridad del Estado.

B. La criminología crítica

Como pilar de nuestra investigación escogimos la criminología crítica, corriente que procedemos a definir, y a conceptualizar una serie de preceptos.

Para definir su origen, Baratta y Faría (2004) nos señalan que la criminología desplazó su interés de la etiología del comportamiento al proceso de etiquetamiento criminal (págs. 91-92).

Así mismo, Ávila (2005, pág. 7) plantea:

> La criminología crítica es la corriente que da al traste con toda la criminología tradicional, que se caracterizaba por un enfoque netamente positivista, dependiente de las categorías dadas por el derecho penal, para obtener su objeto de estudio. Abandona las concepciones legalistas, biológicas y funcionalistas (protectoras del orden establecido), que consideran al delincuente como un individuo distinto al resto de la sociedad y se concentra en el estudio del delincuente no convencional (delitos de cuello blanco o criminalidad de los poderosos) y de la violencia legal-institucional. La criminología crítica se rebela, no solamente contra la criminología existente y el derecho penal ("derecho desigual por excelencia"), sino contra todo el orden establecido.

La consagración de leyes penales por sí mismas, en este caso la consagración legal de los delitos informáticos, no permite entender el sistema penal en su conjunto.

En la criminología crítica se ha entendido que no todos los delitos son necesariamente penalizados. Las causas de impunidad o la cifra negra de los delitos según Pavarini (citado por Bergalli, 1983a) son:

> En primer lugar las *causas Legislativas* que se refieren tanto a la estructura general del derecho punitivo («valoración histórica política de las normas incriminadoras como pertenecientes a la matriz clasista del ordenamiento penal burgués») como a la configuración de los tipos penales («valoración técnico-jurídica») y a la naturaleza eminentemente *«ideológica* del derecho penal burgués. (Pág. 236).
>
> (...)
>
> En segundo lugar, *las causas relacionadas con la aplicación de la ley penal,* que comprenden tanto las dificultades de criminalización primaria (la norma incriminadora existe pero no es aplicada) como las de criminalización secundaria (la norma incriminadora es aplicada pero el condenado no adquiere la consideración social de criminal) no entra en la clásica. (Pág. 237).

C. Tipología de los delitos informáticos

Las modalidades de delitos informáticos en Colombia y a nivel internacional más comunes son los que se presentan en la tabla 1.

Tabla 1. Modalidades de delitos informáticos

A nivel nacional	Tendencias internacionales
Acceso no autorizado.	Fraudes cometidos mediante manipulación de computadores.
Destrucción de datos.	
Infracción de los derechos de autor.	Falsificaciones informáticas.
Infracción del copyright de bases de datos.	
Interceptación de correos electrónicos.	Daños a datos computarizados.
Estafas electrónicas.	
Trasferencia de fondos.	

Fuente: elaboración propia con base en Rincón Cárdenas (2015, pág. 430).

Como lo expone Alexander Díaz García (2014), las conductas en lenguaje informático de delitos informáticos que se presentan en Colombia actualmente son los que se resumen en la tabla 2.

Tabla 2. Conductas y lenguaje de los delitos informáticos

Delitos	Lenguaje
Estafa	Cracking
Carta Nigeriana	Grooming
Falsedad personal	DDOS
Vishing	APT
Sexting	Phising
Defacement	Smishing
Bonet	Sextorcion
Injuria	Skimming
Ciberbulling	Turinet
Calumnia	Morphing

Fuente: elaboración propia con base en Díaz García (2014, pág. 73).

D. El perfil del ciberdelincuente

Los delincuentes informáticos han sido sujetos que aparecieron paralelamente al desarrollo de las tecnologías de computadoras, de comunicación e informática.

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 acrecentaron los usos de *malware o software malicioso* en la Internet. De igual manera, han utilizado el correo electrónico y los *chat rooms* o salas de conversación virtual de Internet para buscar sujetos vulnerables.

Además de los delincuentes informáticos propiamente, existen otros tipos de delincuentes que han encontrado espacios propicios en los distintos medios de comunicación electrónica, para desarrollar sus crímenes. Estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, traficantes de drogas, traficantes de personas, creadores de pornografía, homicidas 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.

La tabla 3 muestra unos patrones que explican el perfil del ciberdelincuente, la clase de delito y el sujeto que normalmente realiza determinadas conductas delictivas.

Tabla 3. Perfil del ciberdelincuente, según clase de delito

Clase de delito	Sujetos
Delitos patrimoniales bancos y entidades financieras.	Empleados, en especial cajeros o personal del área de sistemas, exempleados, terceros en connivencia.
Delitos de acceso ilegítimo o delito de los menores.	Hackers, preakers, usuarios descontentos.
Daño o sabotaje informático.	Empleados de la empresa o espías profesionales o industriales.
Violaciones a la privacidad, tratamiento ilícito de datos personales.	Investigadores privados, empresas de marketing, agencias de informes crediticios y de solvencia patrimonial.
Violaciones a la propiedad intelectual del software y bancos de datos, con informes o compilaciones de datos.	Piratas informáticos, o también usuarios (copia amigable) y empresas que realizan competencia "parasitaria".

Fuente: Palazzi (2000, pág. 68).

Se considera que el delincuente informático no necesariamente tiene profundos conocimientos de computación, sino que es inducido a delinquir por la oportunidad que se le presenta frente al uso diario del ordenador y la impunidad que este le brinda, o por los conocimientos que este tiene frente al resto del personal.

E. Política pública de ciberseguridad en Colombia

En el presente año (2015), con posterioridad al Conpes 3701 de 2011 (Rincón Cárdenas, 2015) el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunica-

ciones (MinTIC) comenzó a brindar capacitación al sector privado sobre ciberseguridad y seguridad de la información. Adicionalmente a lo anterior se crearon tres nuevas dependencias para la protección ciudadana:

- Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) encargado de coordinar a nivel nacional todo lo relacionado con ciberseguridad.

- Comando Conjunto Cibernético de las Fuerzas Militares, responsable de salvaguardar los intereses nacionales en el ciberespacio.

- Centro Cibernético Policial, encargado de la prevención, investigación y apoyo judicial de delitos informáticos, para lo cual contará con un Comando de Atención Inmediata Virtual (CAI Virtual).

III. METODOLOGÍA

La presente investigación se desarrolló por medio del método cualitativo, ya que se interesó por la comprensión de los fenómenos legales y el conocimiento de estos por los funcionarios de la policía judicial, el Cuerpo Técnico de Investigación (CTI) de la Fiscalía y la Fiscalía General de la Nación, para lo cual se utilizaron instrumentos investigativos cualitativos como entrevistas, recolección de documentos escritos y derechos de petición (Taylor y Bodgan, 1987).

Se trabajó bajo un enfoque etnográfico porque se buscó conocer el fenómeno social de los delitos informáticos en el Distrito Judicial de Villavicencio desde la perspectiva de los sujetos sociales: las personas que han sido designadas institucionalmente y tienen la obligación legal de conocer, investigar y judicializar a quienes se encuentren inmersos en las diferentes modalidades reguladas por nuestro Código Penal.

La investigación fue sociojurídica debido a que su objetivo es ir de lo conocido a lo desconocido con ayuda del método científico. Se ha señalado que existe una normativa de carácter nacional e internacional como marco para limitar y regular el desarrollo científico, tecnológico y de las comunicaciones; este desarrollo ha traído consigo la afectación de diferentes bienes jurídicos. El Estado cuenta con unos recursos humanos, físicos y tecnológicos destinados a investigar y judicializar a quienes cometen delitos informáticos. Partiendo de esto, quisimos conocer cómo se desarrolla la persecución criminal desde su investigación hasta su judicialización, los recursos con los que cuenta la policía judicial, las investigaciones que están actualmente abiertas y la forma en que son afrontados estos delitos por el fiscal, la policía judicial y el juez en el Distrito Judicial de Villavicencio.

Para Sánchez Zorrilla (2010), la investigación jurídica se puede dividir en tres formas, una de estas la que se presenta en el aspecto social, por lo cual es llamada sociojurídica. Soriano (1997) afirma que “la sociología jurídica se ocupa de la influencia de los factores sociales en el derecho y de la incidencia que este tiene, a su vez, en la sociedad; la mutua interdependencia de lo social y lo jurídico” (pág. 17). Nuestra investigación se enmarca en este tipo, pues hemos podido

observar que la continua y constante evolución tecnológica llevó al derecho a establecer unos límites a este, por medio de las políticas y normatividades desarrolladas dentro de cada país y de manera global, cumpliendo así el Estado con su función de garante de los derechos y libertades de sus ciudadanos y en especial de las víctimas de los delitos informáticos.

La información se obtuvo mediante derechos de petición y entrevistas a distintas entidades judiciales, tales como el CTI, la Fiscalía General de la Nación y los cuatro juzgados municipales que tienen conocimiento de los delitos informáticos en el Distrito Judicial de Villavicencio, que nos permitieron recolectar la información que se muestra en la tabla 4.

Tabla 4. Estado de los procesos que adelantan los juzgados municipales del Distrito Judicial de Villavicencio, según delitos informáticos

Juzgado	Delito	Estado del proceso
Juzgado Tercero Penal Municipal	Hurto por medios informáticos –agravado.	Se condenó al imputado a 83 meses de prisión como pena principal, igual término como pena accesoria, inhabilidad en el ejercicio de derechos y funciones públicas.
Juzgado Tercero Penal Municipal	Hurto usando medios informáticos o electrónicos.	Se condenó a la pena de 35 meses y 7 días de prisión, se le concede el subrogado de la suspensión de la ejecución de la pena.
Juzgado Tercero Penal Municipal	Hurto por medios informáticos y semejantes.	Se condenó a la pena de 17 meses de prisión, se le concede el subrogado penal de la suspensión de la pena.
Juzgado Cuarto Penal Municipal	Hurto por medios informáticos y semejantes.	Se condena a los imputados a la pena principal de 12 meses de prisión y se concede el subrogado penal caución juratoria.
Juzgado Cuarto Penal Municipal	Violación de datos personales (art. 269f), acceso abusivo a sistemas informáticos (art. 269a).	El acusado hace uso del allanamiento, se verifica el allanamiento, se le condena a 18 meses de prisión, se le concede el subrogado penal en cuanto a la caución juratoria.
Juzgado Cuarto Penal Municipal	Hurto por medios informáticos y semejantes (art. 269i).	Se condena al imputado a la pena de 48 meses de prisión y se niega el subrogado penal, se concede la prisión domiciliaria.
Juzgado Cuarto Penal Municipal	Hurto por medios informáticos (art. 269i).	Se condena a la pena de 24 meses de prisión, se niega el subrogado penal de la suspensión condicional de la ejecución de la pena, se concede prisión domiciliaria, además deberá suscribir caución juratoria.
Juzgado Cuarto Penal Municipal	Hurto por medios informáticos y semejantes en grado de tentativa (art. 269i).	Hurto por medios informáticos y semejantes en grado de tentativa art. 269i.
Juzgado Cuarto Penal Municipal	Hurto por medios informáticos y semejantes (art. 269i).	Se devuelve al Centro Judicial de Servicios.
Juzgado Séptimo Penal Municipal	Hurto calificado por medios informáticos y semejantes.	Se dictó sentencia condenatoria, se impuso una pena de 15 meses de prisión y se concedió el subrogado penal de la suspensión condicional de la pena garantizada mediante caución prendaria.
Juzgado Séptimo Penal Municipal	Hurto calificado por medios informáticos y semejantes.	Se decretó la preclusión de la investigación, se ordenó revocar las medidas cautelares impuestas y la libertad inmediata.

Elaboración propia con base en la información suministrada por los juzgados penales municipales de conocimiento.

Se presentó un derecho de petición a la Fiscalía General de la Nación – Seccional Villavicencio, que fue respondido el 16 de abril de 2013, en el que se solicitó indicar el número de denuncias penales, imputaciones, acusaciones, audiencias preparatorias, condenas obtenidas por la Fiscalía Seccional Villavicencio; así mismo, sobre las absoluciones, preclusiones y archivo de diligencias sobre los delitos informáticos que trata el título VII Bis Código Penal colombiano, artículos 269a hasta 269j.

Así mismo se presentó derecho de petición al Cuerpo Técnico de Investigaciones de la Fiscalía General de la Nación en el que se preguntó lo relacionado con los siguientes tópicos:

- ¿Existe una unidad especializada en Villavicencio para combatir los delitos informáticos?

- ¿Con qué personal cuenta la ciudad de Villavicencio para afrontar las investigaciones y qué preparación tiene?

- ¿Qué tipo de preparación técnica, tecnológica, profesional o posgradual requiere un investigador en este tipo de delitos?

- ¿Cuáles son los delitos más frecuentes que afronta su entidad como apoyo a los fiscales, en cuanto a delitos informáticos?

- ¿Se requiere software o hardware especializados para combatir los delitos informáticos?

Finalmente, se entrevistó a la directora de la Unidad de Delitos Informáticos, el 5 de junio de 2013.

IV. RESULTADOS

A. Las denuncias penales

El objetivo fue determinar cuántas investigaciones criminales por delitos informáticos se tramitaron en la Fiscalía Seccional de Villavicencio.

Los datos que reporta la Fiscalía General de la Nación, Seccional Villavicencio, nos indican que solo se presentaron:

- Veintitrés (23) denuncias penales por acceso abusivo a un sistema informático y una (1) condena por este delito en 2011.

- Veinte (20) denuncias penales por violación de datos personales, una (1) condena y once (11) archivos de las diligencias en 2011.

- Veinte (20) denuncias por hurto por medios informáticos semejantes, una condena y ocho (8) archivos de las diligencias en 2011.

- Veintidós (22) denuncias por hurto por medios informáticos o semejantes, una (1) condena y ocho (8) archivos de las diligencias en 2011.

- Doce (12) denuncias por acceso abusivo a un sistema informático y dos (2) imputaciones en 2012.

- Una (1) denuncia por daño informático en 2012.

- Cinco (5) denuncias por violación de datos personales y un (1) archivo de las diligencias en 2012.

- Diez (10) denuncias por hurto por medios informáticos o semejantes; cuatro (4) formulaciones de imputación, una (1) formulación de acusación, dos (2) condenas y cuatro (4) archivos de las diligencias en 2012.

- Una (1) denuncia por transferencia no consentida de activos en 2012.

B. Las condenas penales en Villavicencio

El objetivo fue determinar cuántos procesos penales fueron tramitados desde la etapa de judicialización. De acuerdo con la información recolectada en los juzgados penales de conocimiento de la ciudad de Villavicencio, se encontró que en materia de delitos informáticos la situación fue la siguiente:

- El periodo 2011 tiene seis (6) procesos con condena.

- El periodo 2012 tiene tres (3) procesos con condena.

- El periodo 2012 tiene una (1) preclusión.

- El hurto por medios informáticos y semejantes del artículo 269i tiene cinco (5) condenas en el periodo 2011.

- El hurto por medios informáticos y semejantes del artículo 269i tiene tres (3) condenas en el periodo 2012.

- Violación de datos personales del artículo 269f y acceso abusivo a un sistema informático del artículo 269a tiene una (1) condena en el periodo 2011.

- De las nueve (9) condenas impuestas:

  - una (1) está bajo la modalidad de tentativa

  - dos (2) tienen suspensión condicional de la pena

  - cuatro (4) tienen caución juratoria

  - una (1) persona está en establecimiento carcelario

  - dos (2) personas tienen prisión domiciliaria

En la respuesta al derecho de petición de tres (3) de abril de 2013, la Fiscalía General de la Nación, Seccional Villavicencio, manifestó:

> c. En la actualidad el delito más frecuente es el hurto por medios informáticos y semejantes. Con relación a las investigaciones que se llevan en la Unidad sobre personas que son víctimas de retiros de dinero de sus cuentas bancarias, tanto de ahorro/corriente o compras o pagos por Internet, se encuentran las siguientes modalidades:
>
> • Clonación de tarjetas débito y/o crédito: corresponde al copiado no autorizado de la banda magnética de las tarjetas y captura de clave por medios externos, con el fin de efectuar retiros o compras por Internet.
>
> • Fraude por Internet modalidad *Phishing* (pesca): en este caso las víctimas reciben un correo electrónico a nombre de una entidad financiera para que accedan a hacer click en un enlace que lo llevará a una supuesta página segura para que actualice sus datos. La página a donde lleva el enlace es una fal-

sificación de la página original del banco. El usuario es engañado y digita sus datos confidenciales, con lo cual proceden a extraerle el dinero de su cuenta.

• Cambiazo de tarjetas débito y crédito: esta modalidad consiste en que el delincuente le ofrece ayuda al usuario a la hora de realizar una transacción, y sin que este se dé cuenta le cambia la tarjeta débito o crédito por otra a través de un juego de "manos".

C. La Fiscalía, el CTI y su capacidad para enfrentar la cibercriminalidad desde la perspectiva oficial

En la respuesta al derecho de petición de 3 de abril de 2013, la Fiscalía General de la Nación, Seccional Villavicencio, informó:

> a. La Fiscalía cuenta con Unidades Especializadas en delitos informáticos; esta Seccional del CTI cuenta con un grupo de Investigadores profesionales que apoya esta labor.
>
> b. El conocimiento e investigación de los delitos informáticos, requiere de personal profesional en ingeniería de sistemas, tecnólogos en sistemas, así como la preparación específica en el uso de herramientas forenses, manejo de evidencia digital y cursos especializados para este tipo de investigación impartidos por la entidad.
>
> (...)
>
> d. para el análisis de evidencia digital (discos duros, memorias USB, MicroSD, teléfonos móviles de diferentes marcas y modelos, entre otros elementos, se requiere equipos (hardware) y software forense especializado.
>
> e. En la actualidad este grupo cuenta con investigadores; los cuales han sido capacitados por el Gobierno de los Estados Unidos, entidades privadas, así como por la Entidad en el manejo de herramientas forenses, recolección de evidencia digital, técnicas avanzadas. Es de anotar que la preparación y los cursos particulares de cada funcionario es información personal, por lo cual están protegidos por la figura del habeas data.

D. La perspectiva interna

A partir de la entrevista realizada a la directora de la Unidad de Delitos Informáticos perteneciente a la Fiscalía, en Villavicencio, se obtuvo la siguiente información:

1. Composición de la Unidad Especializada de Delitos Informáticos

La Unidad está compuesta por dos funcionarios. Una ingeniera de sistemas especialista y un tecnólogo. La asignación de los investigadores se da según los perfiles y aptitudes personales, así como de la disposición de cursos en ese momento por parte de la Fiscalía.

2. Fiscales asignados para esta Unidad

No hay fiscales asignados para la Unidad en Villavicencio de manera específica, sin embargo, actualmente existen dos fiscales de la EDA (estructura de apoyo) locales, competentes para llevar las investigaciones sobre delitos informáticos.

3. Funciones desplegadas por esta Unidad Especializada

Es una unidad de carácter híbrido, debido a que tiene múltiples funciones.

- Hace parte del laboratorio forense, para el manejo de evidencia digital y electrónica forense, así mismo del tratamiento a todo medio de almacenamiento de información existente en el mercado (discos duros, USB, MicroSD, tarjetas de micro chip, entre otros), pudiendo realizar estudios técnicos y peritazgos.

- Es la encargada de realizar todas las investigaciones sobres delitos informáticos.

- Es una Unidad de apoyo para la persecución de cualquier delito en el cual se vea involucrado un medio tecnológico, electrónico o digital. Así mismo, es un soporte vital para los funcionarios adscritos cuando deben realizar imputaciones, por la alta carga de tecnicismos y para que exista comprensión de lo que se intenta demostrar al juez y al propio indiciado.

4. Capacitaciones

Anualmente los investigadores reciben dos capacitaciones especializadas en cuanto a delitos informáticos, y capacitación continua sobre evidencia forense informática.

Las capacitaciones son brindadas por convenios que se suscriben con la Embajada Americana y el International Criminal Investigative Training Assistance Program (ICITAP).

5. Recursos de esta Unidad para perseguir los delitos

En cuanto al talento humano, a pesar de que a nivel nacional hay alrededor de cien investigadores designados para las distintas unidades informáticas, no son suficientes. Ejemplo de esto es la designación de solo dos funcionarios en Villavicencio.

6. Recursos tecnológicos

Existen recursos tales como el dispositivo UFED para el análisis de lo respectivo a telefonía celular; un laboratorio especializado con Convenio SIJÍN para el manejo de la evidencia y de cualquier dispositivo de almacenamiento de datos y de información, que permite, por ejemplo, reconstruir imágenes, es decir, información de discos duros que se encuentran estropeados o eliminados. En dicho laboratorio se hace el análisis de toda evidencia electrónica o digital y el rastreo de las huellas digitales.

7. Presupuesto

No existe un presupuesto designado específicamente para la Unidad; los recursos hacen parte de un presupuesto general que maneja el CTI y la Fiscalía en cada seccional.

8. Cooperación con otros sectores

No existe cooperación de manera oficial entre el sector privado, la Fiscalía y el CTI, porque en las funciones de policía judicial las entidades finan-

cieras, en el caso de los delitos informáticos cometidos en este contexto, nos brindan la información solicitada por autorización judicial. Cada entidad financiera, de manera independiente y con sujeción al direccionamiento de la matriz correspondiente, envía la información, pero no existe una entidad centralizada que unifique los datos e información de las entidades financieras, como se ha querido implementar por parte de la Asobancaria.

9. Cantidad de investigaciones desplegadas por la Unidad

Teniendo en cuenta que esta Unidad no solo maneja los delitos informáticos, sino delitos que tengan que ver con informática, registra un volumen aproximado de 70 informes al año. Semestralmente, en años anteriores, manejó 42 informes.

V. DISCUSIÓN

En las encuestas de victimización que desarrolló el DANE (2003) en Bogotá, Cali y Medellín no se incluyeron los delitos informáticos dentro del listado de conductas. Las mismas conductas tampoco tuvieron relevancia alguna en las encuestas de percepción y victimización realizadas en Bogotá por la Cámara de Comercio de Bogotá (2012). La OEA (2013) afirma que Colombia fue "el país [que] registró menos incidentes cibernéticos en 2012 que en 2011" (pág. 7) dentro de un contexto de ataques en aumento (pág. 14) y de poca fiabilidad de la información (pág. 1).

Según el artículo "Delitos informáticos sumaron $771.000 millones en Colombia", publicado en Portafolio.com el 19 de octubre de 2012, con base en el Informe sobre Colombia de Norton, una de las empresas más representativas del mercado en proveer servicios de seguridad para prevenir que existan delitos informáticos tanto en sector público como en el privado:

> Mientras disminuye el costo por víctima, los incidentes en las redes sociales y los teléfonos celulares aumentan.

El informe de Norton calcula que en Colombia hay unas 9,7 millones de personas víctimas de delitos informáticos en los últimos doce meses y que tuvieron pérdidas financieras directas por un monto de 79.180 millones de pesos.

Por cada segundo, 18 adultos son víctimas de un delito informático lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial. Lo anterior, con pérdidas totales de 197 dólares por víctima en el mundo.

En los últimos doce meses, aproximadamente 556 millones de adultos en todo el mundo fueron víctimas de los delitos informáticos, más que la población completa de la Unión Europea. Esta cifra representa el 46 por ciento de los adultos que se conectan a la red y que han sido víctimas de delitos informáticos en los últimos doce meses, a la par con los resultados del año 2011 (45 por ciento).

Colombia ha empezado a plantear una visión rectora consolidada en el documento Conpes

3701 (Departamento Nacional de Planeación [DNP], 2011) que contiene los lineamientos nacionales de política en materia de ciberseguridad, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. En él recomendó:

> 16. Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones, al Ministerio de Defensa Nacional y al Departamento Administrativo de Seguridad o a quien haga sus veces, *diseñar e implementar planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos, para policía judicial.*
>
> 17. Sugerir a la Fiscalía General de la Nación en coordinación con el Consejo Superior de la Judicatura *diseñar e implementar planes de capacitación sobre temas de investigación y judicialización de delitos informáticos, para policía judicial, jueces y fiscales.*
>
> (...)
>
> 19. Solicitar al Ministerio del Interior y de Justicia realizar en coordinación con el Ministerio de Defensa Nacional y el Ministerio de Tecnologías de Información y Comunicaciones un documento en el que se *analice la normatividad actual y se propongan las modificaciones necesarias en materia de seguridad de la información y protección de datos, para prevenir el ciberdelito, identificando las dificultades de interpretación y aplicación* (DNP, 2011). [Cursivas añadidas].

En la *Agenda Estratégica de Innovación: Ciberseguridad,* del Ministerio de Comunicaciones y Vive Digital (2012, pág. 7) se lee:

> C. Incorporación de los delitos cibernéticos como elemento fundamental de las políticas, normas, actos administrativos y otras figuras jurídicas, con el fin de fortalecer al Estado en su capacidad para identificar, reconocer y juzgar de manera adecuada estos elementos en los procesos jurídicos, constitucionales, penales, etc., definiendo también los alcances, los niveles de gravedad, las penalidades y los procedimientos necesarios ante la ocurrencia de los mismos.

A partir de lo anterior se puede afirmar que existe una disparidad entre el número de víctimas de la delincuencia informática y los datos o registros que manejan las autoridades nacionales, las agencias privadas como Norton y las entidades públicas, como se mostró en los resultados a nivel local (Villavicencio) recolectados en esta investigación. En el marco teórico se afirmó que para la criminología crítica no basta con la creación de tipos penales como los de delitos informáticos, sino que haya un efectivo proceso de criminalización primaria, la cual no se presenta porque de la multiplicidad de delitos (criminalidad oculta) solo fueron seleccionados por el sistema penal en el Distrito Judicial de Villavicencio 114 denuncias, de las cuales solo un ínfimo número (9) registraron condena efectiva, es decir, sentencias penales.

A pesar de la tipificación en materia de delitos informáticos, se observó en los libros radicadores que aun con este número pequeño de condenas, se concedieron en muchos casos subrogados penales y, por esta razón, la sentencia penal no significó necesariamente el cumplimiento efectivo de la pena en un establecimiento de re-

clusión. La tesis de la criminología crítica de la existencia de una cifra negra de la criminalidad se confirma, de esta manera, nuevamente.

¿Cuáles son los factores que no permiten que toda la cibercriminalidad oculta llegue al conocimiento del sistema penal?

No existe cultura de la denuncia, y como se afirmó en el marco teórico, el perfil criminal de los ciberdelincuentes los hace invisibles a la persecución penal: son sujetos con conocimientos especializados.

Cuando las denuncias se evidencian en una disminuida proporción y muy pocas llegan al sistema penal del Estado colombiano, en nuestro caso al Distrito Judicial de Villavicencio, no se cuenta con el recurso humano y técnico suficiente y necesario para iniciar la persecución penal. Aun existiendo este recurso humano sería necesario su cualificación constante, permanente y actualizada ante los cambios frecuentes y súbitos de la tecnología. Un funcionario investigador de policía judicial al tener que estar capacitado permanentemente incrementa los costos de transacción para el sistema judicial. Esto significa que la Ley 1273 de 2009 fue creada sin una perspectiva de financiación de largo plazo que tuviera en cuenta la magnitud de conductas criminales con las que se enfrentaría. La fijación, recolección y embalaje de la evidencia digital requiere de funcionarios capacitados y especializados en informática, que distan mucho de la policía judicial que usualmente realiza estas labores en el terreno.

VI. 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 proce-

dimiento 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 profesio-

nes 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.

Referencias

1. Asociación Internacional de Derecho Penal. XV Congreso Internacional de Derecho Penal. (Septiembre de 1994). *Recomendaciones sobre delitos informáticos y otros delitos informáticos cometidos contra la tecnología informática.* Río de Janeiro.

2. Ávila, K. (Abril de 2005). Aproximación a las propuestas de prevención y control del delito desde la criminología crítica. *Capítulo Criminológico, 33(2).*

3. Baratta, A. y Faría, J. C. (2004). *Criminología y sistema penal.* Montevideo, Uruguay: B de F; Buenos Aires, Argentina: Euros.

4. Bergalli R., Ramírez, J. B., Miralles, T. y de Sola, Á. (1983a). *El pensamiento criminológico, un análisis crítico* (Vol. I). Bogotá: Temis.

5. Bergalli R., Ramírez, J. B., Miralles, T. y de Sola, Á. (1983b). *El pensamiento criminológico, Estado y control* (Vol. II). Bogotá: Temis.

6. Camacho Losa, L. (1987). *El delito informático. Un análisis en profundidad del mayor riesgo con que se enfrenta la sociedad moderna informatizada.* Madrid: Gráficas Cóndor.

7. Cámara de Comercio de Bogotá. (Septiembre de 2012). *Encuesta de percepción y victimización.* Recuperado el 21 de junio de 2013 de ccb: http://www.ccb.org.co/documentos/11085_encuestapecepcionIsemestre2012.pdf

8. Castro Ospina, S. J. (Julio 15 de 2002). *Delitos informáticos. La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano*. Recuperado en febrero de 2012 de delitosinformaticos.com: http://delitosinformaticos.com/delitos/colombia.shtml

9. Consejo de Europa. (Noviembre 23 de 2001). *Convenio sobre la Ciberdelincuencia*. Recuperado en febrero de 2012, de coe: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF

10. Choclán Montalvo, J. A. (1997). Estafa por computación y criminalidad económica vinculada a la informática. *Actualidad Penal,* (47).

11. Davara Rodríguez, M. Á. (2006). *Código de Internet.* Madrid: Thomson Aranzadi.

12. Decreto 1360 de 1989 [Presidencia de la República de Colombia]. Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. Junio 23 de 1989. Recuperado en febrero de 2012 de convenioantipirateria: http://www.convenioantipirateria.org.co/index.php?option=com_content&view=article&id=98:decreto-1360%20de1989&catid=45:decretosreglamentarios&Itemid=109

13. *Delitos informáticos sumaron $771.000 millones en Colombia*. (Octubre 19 de 2012). Recuperado el 9 de junio de 2013 de portafolio: http://www.portafolio.co/portafolio-plus/delitos-informaticos-sumaron-771000-millones-colombia

14. Departamento Administrativo Nacional de Estadística. (2003). *Ficha metodológica encuesta de victimización*. Recuperado el 21 de junio de 2013 de dane: http://www.dane.gov.co/files/investigaciones/fichas/enc_victim.pdf

15. Departamento Nacional de Planeación (Julio 14 de 2011). Conpes 3701. *Lineamientos de política para ciberseguridad y ciberdefensa*. Bogotá: Conpes.

16. Díaz García, A. (2014). *Apuntes de derecho informático.* Ibagué: NTP. Habeas Data Consultores Editorial.

17. Instituto Nacional Penitenciario y Carcelario [Inpec]. (Abril 4 de 2013). Instituto Nacional Penitenciario y Carcelario. Recuperado el 25 de mayo de 2013 de inpec: http://www.inpec.gov.co/portal/page/portal/INPEC

18. Ley 599 del 2000. Por la cual se expide el Código Penal. Julio 24 de 2000. DO n.° 44097.

Obtenido de secretariasenado: http://www.secretariasenado.gov.co/senado/basedoc/ley/2000/ley_0599_2000.html

19. Ley 679 del 2001. Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Agosto 3 de 2001. DO n.° 44509. Recuperado en febrero de 2012 de secretariasenado: http://www.secretariasenado.gov.co/senado/basedoc/ley/2001/ley_0679_2001.html

20. 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. Enero 5 de 2009. DO n.° 47223. Recuperado en febrero de 2012 de secretariasenado: http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.htmlç

21. Ley 1336 de 2009. Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Julio 21 de 2009. DO n.° 47417. Recuperado en febrero de 2012 de secretariasenado: http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1336_2009.html

22. Lima de la Luz, M. (1984). *Delitos electrónicos.* México: Porrúa.

23. Ministerio de Tecnologías de la Información y las Comunicaciones. Plan Vive Digital. (Agosto de 2012). *Agenda estratégica de innovación: ciberseguridad*. Recuperado el 9 de junio de 2013 de vivedigital: http://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

24. Norton. (2012). *Norton Cybercrime Report*. Recuperado el 21 de junio de now-static: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

25. Ojeda Pérez, J. E., Rincón Rodríguez, F., Arias Flórez, M. E. y Daza Martínez, L. A. (Junio de 2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Revista Cuadernos de Contabilidad*, *11*(28), 41-66. Recuperado en febrero de 2012 de: dialnet.unirioja.es/servlet/fichero_articulo?codigo=3643404

26. Organización de los Estados Americanos [ONU]. (Mayo de 2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los Gobiernos*. Recuperado el 9 de junio de 2013 de oas: http://www.oas.org/es/ssm/cyber/documents/OASTrendMicroLAC_SPA.pdf

27. Palazzi, P. A. (2000). *Delitos informáticos.* Buenos Aires: Ad Hoc.

28. Rincón Cárdenas, E. (2015). *Derecho del comercio electrónico y de Internet.* Bogota: Legis Editores.

29. Rivera Llano, A. (1995). *Dimensiones de la informática en el derecho: perspectivas y problemas: delito informático, rol de la jurisprudencia frente al enfoque informático, hábeas data, legislación extranjera.* Bogotá D. C.: Ediciones Jurídica Radar.

30. Salazar, J. F. (2009). Situación normativa de la Sociedad de la Información en Colombia. *Criterio Jurídico, 9*(1). Obtenido de criterio-juridico: http://criteriojuridico.puj.edu.co./archivos/CJ2009S1.pdf

31. Sánchez Zorrilla, M. (2010). Apuntes para una metodología jurídica: la idea de marco teórico. *Revista Telemática de Filosofía del Derecho*, (13), 297-310. Recuperado el 9 de junio de 2013 de rtfd: http://www.rtfd.es/numero13/13-13.pdf

32. Segu-Info. Seguridad de la Información. (2009). *Legislación y delitos informáticos – La información y el delito.* Recuperado en febrero de 2012 de segu-info: http://www.segu-info.com.ar/legislacion/

33. Sloan, I. J. (1984). *The Computer and the Law*. New York: Oceana Publications.

34. Soriano, R. (1997). *Sociología del derecho*. Barcelona: Ariel.

35. Suárez Sánchez, A. (2009). *La estafa informática*. Bogotá: Grupo Editorial Ibáñez.

36. Téllez Valdés, J. (2007). *Derecho informático* (Tercera ed.). México, D. F.: McGraw Hill.

37. Taylor S. J. y Bodgan, R. (1987). *Introducción a los métodos cualitativos de investigación: la búsqueda de significados*. Barcelona: Paidós.

38. Torres, M. (2 de julio, 2005). La piratería es un asunto de todos. Convenio antipiratería para Colombia. *Pensar el libro*. Obtenido de http://www.cerlalc.org/Revista_Pirateria/pdf/n_art07.pdf

39. Torres Torres, H. W. (2002). *Derecho informático: delitos informáticos, software, contratos informáticos, informática jurídica, habeas data.* Medellín: Ediciones Jurídicas Gustavo Ibáñez.