APROXIMACIÓN A LA INFORMÁTICA FORENSE Y EL DERECHO INFORMÁTICO:

Ámbito Colombiano

ISBN: 978-958-8399-67-6

Autora:
Ana María Mesa Elneser

Coautores:
Jorge Eduardo Vásquez Santamaría
Juan Guillermo Lalinde Pulido
Juan David Pineda Cárdenas

Fundación Universitaria Luis Amigó
Fondo Editorial FUNLAM

APROXIMACIÓN A LA INFORMÁTICA FORENSE Y EL DERECHO INFORMÁTICO:
Ámbito Colombiano

Ana María Mesa Elneser
Fundación Universitaria Luis Amigó
Facultad de Derecho y Ciencias Políticas
Investigadora - Coordinadora principal
Grupo de Investigaciones Jurídicas y Sociales

Jorge Eduardo Vásquez Santamaría
Corporación Universitaria de Colombia IDEAS
Facultad de Derecho
Co-investigador
Grupo de Investigaciones en Responsabilidad Jurídica, Social y Empresarial

Juan Guillermo Lalinde Pulido
Universidad EAFIT
Escuela de Ingeniería
Co-investigador
Grupo de Investigación en Redes de Distribución

Juan David Pineda Cárdenas
Universidad EAFIT
Escuela de Ingeniería
Co-investigador
Grupo de Investigación en Redes de Distribución

Medellín, 2013

340.0285861 M578

Mesa Elneser, Ana María

Aproximación a la informática forense y el derecho informático : ámbito colombiano / Ana María Mesa Elneser ; coautores Jorge Eduardo Vásquez Santamaría, Juan Guillermo Lalinde Pulido, Juan David Pineda Cárdenas . -- Medellín : FUNLAM, 2013
214 p. + anexos

SEGURIDAD EN COMPUTADORES - COLOMBIA; PROTECCION DE DATOS - COLOMBIA ; DELITO INFORMATICO - COLOMBIA; INFORMATICA JURIDICA - COLOMBIA; DERECHO INFORMATICO - COLOMBIA; INFORMATICA FORENSE – COLOMBIA ; Vásquez Santamaría, Jorge Eduardo; Lalinde Pulido, Juan Guillermo; Pineda Cárdenas, Juan David ; Mesa Elneser; Ana María

APROXIMACIÓN A LA INFORMÁTICA FORENSE Y EL DERECHO INFORMÁTICO:
Ámbito Colombiano

© Fundación Universitaria Luis Amigó
Transversal 51A 67 B 90. Medellín, Antioquia, Colombia
Tel: (574) 448 76 66 (Ext. 9711. Departamento de Fondo Editorial)
www.funlam.edu.co - fondoeditorial@funlam.edu.co

ISBN: 978-958-8399-67-6

Fecha de edición: 23 de diciembre de 2013

Autora: Ana María Mesa Elneser

Coautores: Jorge Eduardo Vásquez Santamaría
Juan Guillermo Lalinde Pulido
Juan David Pineda Cárdenas

Corrección de estilo: Silvia Milena Vallejo Garzón

Diagramación y diseño: Arbey David Zuluaga Yarce

Edición: Carolina Orrego Moscoso (Departamento Fondo Editorial Funlam)

Hecho en Colombia / Made in Colombia

Texto resultado de investigación. Financiación realizada por la Fundación Universitaria Luis Amigó.

Los autores son moral y legalmente responsables de la información expresada en este libro, así como del respeto a los derechos de autor. Por lo tanto, éstos no comprometen en ningún sentido a la Fundación Universitaria Luis Amigó.

Prohibida la reproducción total o parcial, por cualquier medio o con cualquier propósito, sin autorización escrita de la Fundación Universitaria Luis Amigó.

APORTARON A LA INVESTIGACIÓN

Fundación Universitaria Luis Amigó:

Verónica Bedoya. Estudiante practicante
Dany Gómez. Estudiante practicante

Corporación Universitaria de Colombia IDEAS:

Rodrigo Orlando Osorio Montoya. Coinvestigador – Coordinador del Proyecto
Jenny Correa. Estudiante practicante
Paula Andrea Echeverri. Estudiante practicante

Universidad EAFIT:

Juan Felipe Arango. Estudiante practicante
Jaime Alejandro Pérez Heredia. Estudiante practicante

AGRADECIMIENTOS

El proyecto de “Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009” no hubiera sido posible, debido a su especialidad temática, sin el apoyo y trabajo que se dio entre los investigadores y las unidades involucradas de la Facultad de Derecho y Ciencias Políticas de la Fundación Universitaria Luis Amigó, Escuela de Ingeniería, con el Departamento de Investigaciones Co-financiadas de la Universidad EAFIT y la Facultad de Derecho de la Corporación Universitaria de Colombia, IDEAS, sede Itagüí, al igual que el personal administrativo y los directivos encargados de la investigación de cada una de las instituciones.

Extendemos nuestro agradecimiento a las estudiantes practicantes quienes realizaron un esfuerzo académico e investigativo para apoyar a todos los investigadores en el desarrollo del proyecto: Funlam, IDEAS y EAFIT.

Igualmente, se agradece a instituciones y personas que fueron objeto de aplicación de instrumentos como entrevistas y encuestas, tales como: Colegio de Abogados (COLEGAS); Colegio de Jueces y Fiscales sede Antioquia, Colegio de Defensores Públicos (COLDEFENSORES) de Medellín; Universidad de Medellín, en la coordinación de la maestría y doctorado en Derecho Procesal Contemporáneo; al doctor Alexander Díaz, Juez Penal de Rovira, Tolima, quien fuera el creador y promotor del proyecto de Ley de Delitos Informáticos que dio origen a la Ley 1273 de 2009, la cual fue objeto de estudio en la presente investigación y que ha enmarcado un verdadero camino de diálogo y discusión al ámbito Colombiano en materia de Derecho Informático, escuela de pensamiento que ha formado entre las rivalidades doctrinales dedicadas a la negación sobre el nuevo surgimiento temático de esta nueva rama del Derecho denominada y reconocida a nivel mundial como Derecho Informático. Gracias a los expertos forenses como el Sr. Manuel Santander y a los demás, a quienes les debemos la total confidencialidad por la información.

Se extienden los agradecimientos a abogados, jueces y fiscales encuestados; personas mediadoras en calidad de jueces, fiscales, abogados y defensores públicos que apoyaron con su gestión para la aplicación de los instrumentos tipo entrevistas y encuestas, las cuales fueron resueltas; a la doctora Gloria Luz Restrepo Mejía, Jueza Tercera Penal del Circuito de Medellín, reconocida por su juicio académico e investigativo impartido al momento de valorar y fallar, funcionaria que permitió la realización de una entrevista a profundidad debido a su experiencia en la judicialización de casos en delitos informáticos.

Es pertinente concluir que este texto no habría sido escrito sin el apoyo y la ayuda dada por cada persona física y jurídica involucrada de forma directa e indirecta con su tiempo y valoraciones en el trabajo de campo.

TABLA DE CONTENIDO

PRÓLOGO

Desde cuando realizamos la titánica tarea de homologarnos ante el mundo (Conferencia de Budapest), al sacar adelante el proyecto de Ley de Delitos Informáticos en el Congreso de Colombia, hasta el día de hoy, hemos logrado despertar en muchos académicos, arduos, serios y excelentes trabajos de investigación, y la Dra. Ana María Mesa Elneser y sus compañeros, no han sido la excepción, han brillado por un espíritu emprendedor, selecto y visionario, en sus investigaciones.

Nunca los autores esperan que se refieran a ellos en términos inadecuados en el Prólogo, y sería de poco estilo literario que el prologuista denigrara de los investigadores titulares del trabajo por analizar. No obstante, si el prólogo no se convierte en un solo panegírico o en una declaración pública de amistad y es lo que debe ser (análisis objetivo de la obra que se presenta) entonces se cumple con la ética y esas palabras preliminares pueden ser guía útil para quien toma por primera vez el libro en su manos. Ese es el propósito de los párrafos que siguen, sin dudar claro está, lo agradecido que me encuentro con la Dra. Ana María y su equipo, al aceptar justamente ese reto.

Decíamos que es todo un reto intelectual, ser el elegido para el honroso encargo de presentar una obra producto del ingenio y talento de un colectivo. Para mí referirme a la obra Aproximación a la relación entre la informática forense y el derecho informático en el ámbito colombiano, más que un reto constituye un placentero ejercicio intelectual, por la sistemática, interesante y cuidadosa metodología que la Dra. Ana María Mesa Elneser y su equipo de trabajo: Jorge Eduardo Vásquez Santamaría, Juan Guillermo Lalinde y Juan David Pineda, le imprimieron a la obra.

He tenido la fortuna de conocer personalmente a la Dra. Ana María Mesa Elneser, desde ya hace varios años, y particularmente nuestras comunicaciones han sido vía electrónica y siempre el tema es informático, en donde me formula, la mayoría de las veces, complejas y llamativas preguntas, algunas de ellas fueron tan interesantes que hoy son motivo de algunos artículos míos, publicados en la Internet. Desde entonces disfruto de una respetuosa, afable e interactiva amistad, hasta el día de hoy, cuando me encarga la delicada misión que les hable de su obra asociada. Sé de su alto nivel de compromiso, seriedad y entrega con el Derecho y las Nuevas Tecnologías y en especial con los DELITOS INFORMÁTICOS, dejando en claro y siguiendo mis humildes conceptos como brillante discípula, la diferencia entre éstos y los DELITOS ELECTRÓNICOS, que harto problema le ha dado a la jurisprudencia y a la doctrina establecerla, porque es usual que la judicatura, academia y los medios de comunicación no la establezcan, ignorando los motivos, siendo potísimas las razones, pues una conducta vulnera el BIEN JURÍDICO TUTELADO DE LA INFORMACIÓN Y EL DATO y el mal llamado “delito electrónico” como acertadamente la Dra. Ana María, nos lo explica, es más concretamente un medio para consumar la conducta, lo que para algunos autores ha sido considerado su fundamento para describir qué son delitos informáticos.

Antes de comentar el trabajo de la Dra. Ana María Mesa E. debo reconocer que su lectura me ha resultado muy amena y en muchos apartados de las unidades, simplemente apasionante, es como si el lector hubiera acompañado a los protagonistas de la obra en los foros de discusión, en donde intervinieron para extraer y fundamentar sus teorías. Nos ilustra nítidamente y de las pocas científicas en el país que lo hace, la diferencia que existe entre estas dos tesis (DELITO INFORMÁTICO con el DELITO ELECTRÓNICO) y el error en que se incurre, si persistimos en mantener el concepto, porque olvidan que el delito informático es el que viola al BIEN JURÍDICO TUTELADO DE LA INFORMACIÓN Y EL DATO, el que fuera creado, con bastante resistencia legislativa y académica con la Ley 1273 de 2009, implicando que para consumar la conducta se viola es la información y el dato, y no ningún otro bien jurídico, a no ser que se realice mediante concurso de tipos.

Resaltamos como los autores con un lenguaje técnico, pero adecuado para el incipiente estudioso de los delitos informáticos, sin restarle lo útil que le resultará al avezado Forense, podrán establecer claramente que con la consumación del mal llamado “delito electrónico” no se viola la información ni los datos, lo que se vulnera es el bien al que hace parte o está adscrito capitularmente en el Código Penal el tipo (no hay ni puede haber en Colombia por ejemplo: estafa informática o hurto informático, pero sí estafa o hurto consumados a través de medios electrónicos), pues se vulnera el BIEN JURÍDICO TUTELADO DEL PATRIMONIO ECONÓMICO u otro, implicando que el delito informático no necesariamente tenga que consumarse a través de medios electrónicos, porque perfectamente se puede apoderar, difundir, ofrecer, vender, interceptar, etc., una información contenida en un fichero en soporte papel, los muy común llamados legajadores o carpetas; esto es un DELITO INFORMÁTICO.

El libro que hoy sugerimos para su consulta está constituido por seis unidades temáticas, el espacio de conclusiones y el de anexos, a saber:

MEMORIA METODOLÓGICA

Capítulo 1. Escenario problemático y metodológico de la investigación.

REFERENTES TEÓRICOS

Capítulo 2. Aproximación a aspectos internacionales relevantes en delitos informáticos y la informática forense.

Capítulo 3. Una mirada jurídica a los delitos informáticos en Colombia y su evolución legal en el marco del Derecho Comparado.

Capítulo 4. Mirada holística a la informática forense en Colombia.

HALLAZGOS

Capítulo 5. Análisis de la información y de los datos de la investigación en delitos informáticos.

Capítulo 6. Consideraciones frente al derecho procesal penal con miras a la evolución legal frente a la informática forense.

Para finalizar, orgulloso y satisfecho, tengo el honor de presentar a la comunidad académica del País y del continente, una obra que a partir de hoy se convierte en referente obligatorio de la doctrina sobre DELITOS INFORMÁTICOS. No puedo dejar escapar esta excelente oportunidad para reconocer en la Dra. Ana María Mesa E. una colega pionera de la causa como especialista en Nuevas Tecnologías del Derecho, en nuestro País, la que articula a su gran capacidad de trabajo en equipo plasmada en esta obra, que no dudamos calificarla encomiable, cuyo resultado palpable es la alta productividad de material y documentación de referencia en este importante aporte que nos une en la especialidad.

ALEXANDER DÍAZ GARCÍA
Juez Segundo de Control de Garantías Constitucionales
Especialista en: Ciencias Penales y Criminológicas de la Universidad Externado de Colombia.
Ciencias Constitucionales y Administrativas de la Universidad Católica de Colombia.
Nuevas Tecnologías del Derecho y Protección de Datos, de la Escuela de Gobierno y Políticas Públicas de Madrid, adscrita al Ministerio de Administraciones Públicas de España.

Mayo, 2013

INTRODUCCIÓN

La presente obra literaria ha sido escrita con la finalidad de realizar un aporte al conocimiento generando una correlación de dos ciencias, el Derecho y la Forense, ambas se ocupan de un mismo objeto de estudio, pero desde diferentes miradas o tópicos o saberes, siendo el núcleo central el incidente informático en correlación con la evidencia digital como medio de prueba.

El objeto de estudio antes delimitado encuentra en la unidad 1, el sustento metodológico que permitió abordar la temática de forma objetiva y lógica, respondiendo a las exigencias de toda ciencia, máxime cuando va a ser abordada por medio de proyectos investigativos; se complementa su desarrollo en la unidad 2 con un estudio a las fuentes que han documentado su interrelación a nivel internacional, tomando como ejes temáticos los delitos informáticos y la informática forense.

En la unidad 3 se especializa el conocimiento de la investigación solo en el ámbito de los delitos informáticos desde el contexto internacional y nacional; para luego pasar a la unidad 4 donde se realizar el mismo estudio profundo y específico dado a los delitos, pero ya a la informática forense tanto en el contexto o ámbito nacional como el internacional, éste último con mayor relevancia en la información contenida en el texto, puesto que esta disciplina científica fue descubierta y desarrollada en cabeza de la gran potencia mundial (EEUU), sin que Colombia esté en la capacidad de responder al nivel de desarrollo tecnológico y relevancia mundial necesaria para ser un referente forense digital, a pesar, como se en algunos apartes del texto, de que si nos encontramos en el deshonroso quinto lugar de países donde más se cometen delitos informáticos.

Posteriormente, se construye la unidad 5, donde se analizan las diferentes posturas que en el ámbito colombiano tienen los actores relevantes y en correlación con los delitos informáticos y su modo de investigarse, información obtenida de la aplicación de encuestas cerradas anónimas por vía electrónica a jueces, fiscales, abogados y defensores públicos, y además de entrevistas a profundidad con expertos abogados, jueces y forenses certificados. En la unidad 6, se responde a un estructura propositiva de pertinencia en reforma al Código Procesal Penal Colombiano Ley 906 de 2004, donde uno de los avances en materia investigativa más relevantes que debe corresponder en Colombia es la ampliación de los medios cognitivos sobre hechos delictuales y permitir la inclusión de la evidencia digital como uno más, que pueda corresponder a las necesidades reales del objeto de investigación, el cual no es más que un incidente informático.

En el apartado 7, el equipo de investigadores liderado por la Funlam a través de la investigadora principal Ana María Mesa Elneser, plantean conclusiones y recomendaciones dirigidas al Estado Colombiano a través del Gobierno actual y a toda la comunidad científica del Derecho y la Informática, para que, a partir del texto general y de esos breves apuntes, pueda generarse un impulso en la dinámica académica e investigativa que debe responder la disciplina forense digital, máxime que las nuevas formas de comportamiento social en el ámbito digital siguen en aumento diariamente. Finalmente, se estructura espacio de anexos donde se insertaron los instrumentos aplicados de entrevistas y encuestas.

MEMORIA METODOLÓGICA

CAPÍTULO 1.

ESCENARIO PROBLEMÁTICO Y METODOLÓGICO DE LA INVESTIGACIÓN

Ana María Mesa Elneser

Jorge Eduardo Vásquez Santamaría

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso (Cano, 2006)

La necesidad de alcanzar una especialización científica en temas de innovación social, ha sido para el Derecho un desafío constante, trayendo con ello múltiples efectos en la distribución y concepción de la norma en sí misma, basada en ramas y áreas específicas normativas, procurando detallar y delimitar cada uno de los componentes que deben ser abordados por aquellas.

En el escenario jurídico una de esas áreas delimitadas, en procura de alcanzar una eficaz especialidad basada en el Derecho Probatorio, es el Derecho Informático, el cual, de manera global, establece vínculos específicos con cada una de las ramas que complementan la ciencia jurídica. Puntualmente, en el escenario probatorio penal se identifican las conductas delictuales ocurridas e investigadas en torno a la informática.

Esa situación plantea un dinamismo permanente de la norma, debido a la existencia de circunstancias que generan imposibilidad de probar aquellas conductas, entre las cuales se reconocen los costos operativos desde el campo forense digital, la insuficiencia de personal y de calidad de auxiliares de la justicia capacitados en el campo de la computación forense informática, insuficiencia de laboratorios y herramientas forenses informáticas en el campo público y privado, incipiente conocimiento y capacitación de abogados litigantes, fiscales, jueces, funcionarios públicos en el manejo y elección de los medios de prueba pertinentes para probar conductas desplegadas en un entorno electrónico e informático, generando en muchos casos la renuencia de denunciar, por parte de la víctima, sobre el hecho acaecido, toda vez que no es posible probar la conducta, o ante la denuncia realizada, no existe posibilidad de probar los hechos ocurridos por ausencia de material probatorio pertinente (Delitos informáticos.com, julio 2010).

Las figuras delictuales denominadas recientemente delitos informáticos, con la expedición de la Ley 1273 de 2009, han generado un cambio paradigmático en el tratamiento e investigación de las conductas delictuales, que hasta el momento de expedición de la ley se venían presentando sin que el investigador, el fiscal e incluso el juez pudiesen procesar ciertas conductas aparentemente violadoras de bienes jurídicos, por ausencia de tipificación (Delitos informáticos.com, julio 2010).

Expedida la Ley 1273 de 2009, el campo de la investigación y la obtención de la prueba tuvo una nueva interacción en el conocimiento, una nueva forma de desarrollo, es allí donde vemos el surgimiento de la informática forense como ciencia del conocimiento que permite establecer métodos, procedimientos y estándares de políticas en el procesamiento de una evidencia digital o elemento material probatorio, para dar soporte a una investigación en el grupo de los delitos informáticos contemplados en la ley.

Es así como el proyecto de investigación propone la siguiente pregunta: ¿Se hace necesaria en Colombia la evaluación, identificación y determinación de las técnicas forenses en la investigación de delitos informáticos consagrados en la Ley 1273 de 2009?; interrogante que se articula al objetivo general centrado en establecer la evidencia digital requerida para dar soporte probatorio en la inves-

tigación de la comisión de los delitos informáticos expedidos con la Ley 1273 de 2009, desplegando dicha actividad desde los medios técnicos, tecnológicos y científicos que garanticen la validez y eficacia de la imputación o acusación conforme con el ordenamiento jurídico colombiano.

Para ello se proponen una serie de objetivos específicos que permiten orientar el adecuado desarrollo y ejecución del proyecto de investigación, a los cuales el equipo de investigación de la Facultad de Derecho de la Corporación Universitaria de Colombia - IDEAS se articula al objetivo específico número uno, tendiente en presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria. El Departamento de Investigaciones Co-financiadas Institucionales, delegado en el área de Investigaciones de la línea de Ingeniería Informática Educativa de la Universidad EAFIT, será el encargado de orientar y desarrollar los objetivos específicos tres, cuatro y cinco. Para la Facultad de Derecho y Ciencias Políticas coordinando el desarrollo, orientación y lineamiento del objetivo específico dos, y coordinando el desarrollo de todos los objetivos específicos a cargo de las demás instituciones en procura del desarrollo del objetivo general. Los resultados obtenidos frente a los objetivos específicos se articularán a los contenidos programados en las ocho unidades sobre delitos informáticos y la informática forense, contenidos en la tabla general de contenido.

Para dar desarrollo a los objetivos específicos se adopta un estudio exploratorio- descriptivo, pues se enfrenta ante un problema de investigación de poco estudio e indagación en el contexto nacional colombiano, no abordado en las universidades convocadas para el proyecto o en el medio. Este método se emplea cuando se examina un nuevo interés o cuando el objeto de estudio es relativamente nuevo (Babbie, 2000, p. 72), a él se articula la metodología de la investigación documental, donde los instrumentos para el manejo de la información documental son: rastreo documental, fichado bibliográfico y la matriz de sistematización de información. Sin embargo, fue pertinente incluir la aplicación de instrumentos de consulta como encuestas y entrevistas, toda vez que el fundamento legal, jurisprudencial y doctrinal existente fue escaso para dar cumplimiento al desarrollo y estudio de los diferentes objetivos específicos.

Dicha etapa del trabajo se centra en la identificación, descripción y definición de los delitos informáticos en el ordenamiento jurídico colombiano, sus antecedentes históricos desde evidencias fácticas internacionales y motivaciones jurídicas en Colombia que dieron lugar a la Ley 1273 de 2009 que hoy regula las conductas objeto de investigación; así como en la descripción y definición de los mencionados delitos a nivel nacional e internacional, todo con la finalidad de promover la presentación de los citados delitos existentes en la Ley 1273 de 2009.

También se desarrolla un estudio de las ciencias forenses aplicables en Colombia y la articulación del estudio del derecho informático en concordancia con la informática forense digital, con la finalidad de establecer una correlación transversal de la información que permita el desarrollo temático planteado desde el problema de investigación.

En esta actividad participa como coordinador principal del proyecto, en representación la Facultad de Derecho de la Corporación Universitaria de Colombia, IDEAS, el abogado Jorge Eduardo Vásquez Santamaría, acompañado del coinvestigador y abogado penalista Rodrigo Orlando Osorio Montoya, quien participó en la etapa inicial de recolección y análisis de datos. Además, un equipo de estudiantes del programa de Derecho, quienes intervienen en calidad de practicantes, siendo los directamente involucrados Paula Andrea Echeverry Bolívar, Jheny Patricia Correa Quintero y Miguel Alejandro Palacio Hernández.

Por la Universidad EAFIT participa como coordinador del proyecto del departamento de investigaciones co-financiadas el doctor Juan Guillermo Lalinde Pulido, y en calidad de co-investigador el ingeniero Juan David Pineda Cárdenas y como estudiantes del semillero Juan Felipe Arango para el periodo 2011-1 y Jaime Alejandro Pérez Heredia para el periodo 2011-2.

Por la Fundación Universitaria Luis Amigó, Funlam, participando como coordinadora general del proyecto de investigación interinstitucional y proponente del proyecto adscrito a la Facultad de Derecho y Ciencias Políticas, se encuentra la abogada e investigadora Ana María Mesa Elneser, y como estudiantes auxiliares, adscritos al semillero de Investigación en Derecho e Informática SIDI están Dany Gómez y Verónica Bedoya para la totalidad de ejecución del proyecto en el año 2011 y los tres primeros meses del año 2012.

Las tres etapas de investigación, pre análisis, análisis y final tuvieron como características y derroteros metodológicos el trabajo de encuentros periódicos entre docentes y estudiantes, por medio de los cuales en ejercicios de investigación formativa se promovió la preparación en rastreo bibliográfico y elaboración de fichas doctrinarias, legales y jurisprudenciales; un segundo momento con la elaboración y aplicación de instrumentos de consulta y finalmente el análisis de datos, documentación de resultados y elaboración de informes finales con los productos esperados, entre los cuales se encuentran la formulación de cursos académicos para programas de derecho e ingeniería informática, cinco artículos en formato publicable y la participación en diferentes medios de divulgación como son eventos académicos, programas de radio y televisión.

Estos soportes alimentaron las actividades de investigación adelantadas por los dos docentes involucrados, para obtener como resultado un rastreo conformado por 73 fichas bibliográficas, legales, jurisprudenciales, comentadas, softwares y videos. Igualmente se cuenta con ocho entrevistas a profundidad y 80 encuestas realizadas a abogados, defensores públicos, fiscales y jueces.

En cuanto a los instrumentos aplicados en modalidad de entrevista se direccionó la recolección de la información para dos especialidades del conocimiento, como son: expertos forenses informáticos en el campo de la ciencia informática, específicamente en cuanto a la disciplina forense digital, y expertos en el campo científico del derecho; fueron entrevistados abogados y jueces con categoría de control de garantías y juez de conocimiento.

En la aplicación de las entrevistas se encontraron algunas dificultades por la disponibilidad de tiempo y la pertinencia en el conocimiento específico del tratamiento de los delitos informáticos, de hecho, gran parte de la información fue dada bajo estricta confidencialidad, y se permitió su uso sin revelar la identidad del entrevistado, es por eso que en la Unidad 6 se harán consideraciones sobre las diferentes posturas y miradas de los actores colombianos en el tratamiento de delitos informáticos, aclarando que solo se hará pública la identidad de los entrevistados que así lo permitieron, entre los cuales podemos mencionar al doctor Alexander Díaz, Juez Penal de Rovira Tolima; la doctora Gloria Luz Restrepo Mejía, Jueza Tercera Penal del Circuito de Medellín; el doctor Hernán Darío Elejalde, Abogado e Ingeniero de Sistemas del Área Metropolitana; y el Ingeniero Manuel Santander, funcionario de Empresas Públicas de Medellín.

REFERENTES TEÓRICOS

CAPÍTULO 2.

APROXIMACIÓN A ASPECTOS INTERNACIONALES RELEVANTES EN DELITOS INFORMÁTICOS Y LA INFORMÁTICA FORENSE

Ana María Mesa Elneser

Jorge Eduardo Vásquez Santamaría

Juan David Pineda Cárdenas

Juan Guillermo Lalinde Pulido

Estimando que una lucha bien organizada contra la cibercriminalidad requiere una cooperación internacional en materia penal acrecentada, rápida y eficaz (Convenio Ciberdelincuencia de Budapest).

Una característica de los delitos informáticos es la facilidad de comisión con impacto trasnacional, afectando ordenamientos jurídicos de varios Estados, todos diferentes por más similitudes que puedan colegir, generando inconvenientes al momento de la investigación criminal y la judicialización del sujeto individualizado. Es por ello que para la presente investigación tiene relevancia el contexto internacional que involucra a los delitos informáticos y la informática forense, ya que, finalmente, pondrá el contexto de la política criminal internacional en materia de la cibercriminalidad.

Convención Cibercrimen Budapest[1]

En el escenario internacional debemos retomar la postura unificada que defiende la ausencia de una definición formal y universal de delito informático; sin embargo, ello no ha sido razón para que en diversos contextos se hayan presentado iniciativas y formulado conceptos respondiendo a realidades nacionales concretas:

> No es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión 'delitos informáticos' esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún (Tellez, 1996, p. 103).

Dentro de los antecedentes identificados que presentan disposiciones en torno a los denominados delitos informáticos se tiene, en 1983, el estudio adelantado por la Organización de Cooperación y Desarrollo Económico (OCDE) 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.

Para 1992, durante la celebración del Coloquio de la Asociación Internacional de Derecho Penal de Wurzburgo, Alemania, fueron acogidas distintas recomendaciones respecto a los delitos informáticos, entre las que se destaca aquella tendiente a pluralizar la definición de delito informático ya mencionada en la doctrina colombiana, pues no siendo suficiente el Derecho Penal, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos.

La OCDE (1993) 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 como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos".

En materia de normas internacionales se identifica como el único acuerdo en el tema de disposiciones penales informáticas el texto de ciberdelincuencia suscrito por los Estados de la Unión Europea el 23 de noviembre de 2001. Este acuerdo fue adoptado por el Comité de Ministros del Consejo de Europa en la sesión N.o 109 del 8 de noviembre de 2001, firmado en Budapest, Hungría y con en-

[1] Subtema desarrollado por el equipo de investigación de las IES: FUNLAM e IDEAS.

trada en vigor el 1 de julio de 2004. Dicho acuerdo es el único que se encarga de la seguridad de la información y trata los delitos contra la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

La cibercriminalidad le deja a los Estados la necesidad de cooperación e integración en la estructura legal del tipo penal y los sistemas de investigación; la Resolución N.º 1, adoptada por los ministros europeos de justicia, en su 21ª Conferencia (Praga, junio 1997), que recomienda al Comité de Ministros mantener las actividades organizadas por el Comité Europeo para los Problemas Criminales (CDPC) relativas a la cibercriminalidad a fin de acercar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de infracciones informáticas, así como la Resolución N.º 3, adoptada en la 23ª Conferencia de Ministros Europeos de Justicia (Londres, junio 2000), que anima a las partes negociadoras a persistir en sus esfuerzos para encontrar soluciones adecuadas que permitan al mayor número posible de Estados ser parte del Convenio, y reconoce la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga en cuenta las específicas exigencias de la lucha contra la cibercriminalidad (Convenio Ciberdelincuencia de Budaspest, 2001).

El convenio (2001) establece para el campo de los delitos un contexto conceptual y alcance de conductas a ser reguladas, basadas en las descripciones de conductas a ser consideradas delitos en el campo informático y al igual que parámetros en el campo de la investigación y judicialización de las conductas, incluyendo de forma novedosa el “Capítulo I – Terminología” pretendiendo la unificación de conceptos y alcance de los tipos penales, así la conducta lesiva de bienes jurídicos tutelados con la legislación de delitos informáticos de cada país no pierde legitimidad en la judicialización por falta de unificación en la interpretación de bienes jurídicos tutelados; se incluye una “Sección 1 – Derecho penal material” en la cual se establecen los bienes jurídicos, objetivo de protección, con las conductas penales que se reglamentan posteriormente, dado principalmente en el campo de la información y el dato informático, así: “Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos”, integrando en este título las diferentes conductas penales que permiten, en conjunto, materializar la diversidad de hechos calificados como conductas criminales del ámbito del cibercrimen; entre estas están: “Artículo 2 – Acceso ilícito”, “Artículo 3 – Interceptación ilícita”, “Artículo 4 – Atentados contra la integridad de los datos”, “Artículo 5 – Atentados contra la integridad del sistema”, “Artículo 6 – Abuso de equipos e instrumentos técnicos”; posteriormente se incluye otro título que estructura su alcance regulatorio en otros aspectos de conductas de carácter más engañoso, así: “Título 2 – Infracciones informáticas”, con tipos penales de “Artículo 7 – Falsedad informática”, “Artículo 8 – Estafa informática”.

Se incluye un título tercero donde el alcance de la conducta contenida busca la protección desde la regulación de los contenidos, direccionando la protección a un bien jurídico que requiere toda la protección internacional y nacional, que es la pornografía infantil por medio del tipo penal denominado “Título 3 – Infracciones relativas al contenido”, “Artículo 9 – Infracciones relativas a la pornografía infantil”.

En el plano internacional, en el contexto actual, uno de los problemas que ha enmarcado la red para los ordenamientos jurídicos, también en el plano nacional, es la vulneración a la propiedad intelectual tanto en los derechos de autor como en la propiedad industrial, por conductas realizadas en la red, es por ello que la convención no deja por fuera conductas en este plano estableciendo el "Título 4 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines", con la conducta penal descrita en el "Artículo 10 – Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines".

Se reglamenta la existencia de aspectos necesarios para la judicialización del sujeto activo y las conductas desplegadas en la red, sin que su ausencia permita la impunidad por falta de objetividad en la judicialización, integrando un "Título 5 – Otras formas de responsabilidad y sanción" y que se ha materializado en tres artículos: "Artículo 11 – Tentativa y complicidad", "Artículo 12 – Responsabilidad de las personas jurídicas", "Artículo 13 – Sanciones y medidas".

En el convenio se establecen políticas en el campo del derecho procesal que van desde las sanciones y los tipos de sanciones a imponerse en la perspectiva de conservar las garantías del sindicado y procesado; en el campo de la conservación de los datos de tráfico almacenados en los servidores de propiedad de ISP (Proveedores de Servicios de Internet), estableciendo para los estados la facultad de regular el tiempo y la forma de conservación al igual que los parámetros de divulgación de los mismos; igualmente, en el Título 3 de la sección segunda, se incluye un título importante en la obtención de una evidencia digital y es la denominada como mandato de comunicación, pues en el Artículo 18 se establece para los estados la facultad de regular esta facultad de los ISP propietarios de los servidores donde se encuentran los datos de tráfico, ante un incidente informático, siendo necesaria la apertura de los logs[2] siempre preservando el derecho a la intimidad y la información; en el Título 4 se registran las políticas encaminadas a que cada estado reglamente de forma legal la autorización otorgada por la autoridad competente con el fin de acceder a sistemas informáticos y dispositivos de almacenamiento de información, con el fin de obtener evidencia digital del incidente informático investigado.

Se reguló igualmente la facultad de los estados para la ejecución de políticas que permitan la interceptación de tráfico de datos, sea directamente por el ISP o por la autoridad competente investigadora de un incidente, sin que ello implique violación de derecho al investigado.

La convención inicialmente implicaba la participación de los estados miembros del Organismo Internacional de la Unión Europea y fue pertinente determinar los lineamientos de la competencia, ya que cada Estado posee su derecho interno; por esta razón el tema de competencia en la judicialización de delitos no podía quedar por fuera, delimitando a los estados para determinar las variables que indican la competencia para investigación del delito entre las cuales está que el delito sea cometido en el territorio del estado, pasando por la ejecutoria del delito, ya sea en aguas del mar o en

[2] Un *log* es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.

el espectro electromagnético a bordo de una aeronave, finalmente, en los hechos donde no exista competencia específica.

Siendo un tratado desarrollado, discutido y ratificado entre varios estados, los lineamientos de cooperación internacional establecen principios direccionados a la facultad de "investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal" (Consejo Europeo, 2001). permitiéndose la interceptación de comunicaciones, captura de datos de tráfico, su almacenamiento, la conservación de la confidencialidad, su comunicación y acceso con o sin autorización del propietario del dato, mediando autorización judicial al acceso, sea éste en el campo nacional o transfronterizo, pues el delito informático es volátil, expansivo, de ejecutoria en muchos casos con servidores del ámbito internacional, como ocurre con delitos informáticos a través de los correos electrónicos de proveedores como son hotmail, gmail, terra, entre otros.

Finalmente, como estructura novedosa se crea una red denominada 24/7 que tiene como finalidad "asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal" (Consejo Europeo, 2001).

Colombia no se encuentra como miembro de la convención pero a través de la expedición de la Ley 1273 de 2009 o ley de delitos informáticos, ha homologado los lineamientos legales de la convención, con la finalidad de unificar criterios de tipicidad en cuanto a la cibercriminalidad, e igualmente respondiendo a la red *24/7* de cooperación internacional contra el delito, especialmente la pornografía infantil, que de ello ha dado cuenta colombia estableciendo políticas publicas direccionadas a la protección de los derechos de los niños, niñas y adolecentes, se reitera entonces que Colombia ha homologado el tratado con la finalidad de impulsar la lucha contra la ciberdelincuencia.

Organismo internacional, entidades privadas y gobierno, líderes en la informática forense[3]

Entre muchos estados, organismos internacionales e instituciones privadas dedicadas a la promoción y administración de la informática forense o computación forense, con el fin de garantizar la validez y eficacia de la investigación forense digital y para esclarecer el alcance que posee, a nivel internacional, esta disciplina, se toman como referencia las instituciones y los gobiernos más notorios a nivel mundial, aseveración fundamentada en la incidencia y relevancia que poseen en la creación de política internacional, en la cooperación entre estados y el desarrollo constante de la disciplina forense digital materializada en la creación y promoción de protocolos y herramientas forenses digitales.

La INTERPOL es la segunda organización internacional más grande del mundo después de la ONU (creada como la policía internacional); en la actualidad tiene ciento noventa países miembros y promueve la colaboración en la lucha contra el delito. En esta organización la dinámica del delito y

[3] Subtema desarrollado por el equipo de investigadores de las IES: FUNLAM y EAFIT.

la novedosa forma de su comisión le exige poseer la infraestructura técnica y operativa para apoyar a los estados cuando estos no cuenten con los medios de investigación pertinentes o, al tenerlos, no resulten suficientes; recordemos un claro ejemplo de ello en Colombia, en el caso del ataque al campamento de Raúl Reyes perpetrado en el año 2008[4].

El apoyo otorgado por la policía internacional se enmarca en: instrumentos y servicios para realizar su función policial con validez y eficacia; igualmente imparte formación específica, apoyo especializado en materia de investigaciones, y proporciona información y conductos de comunicación protegidos, los 365 días del año y las 24 horas del día. Igualmente su existencia a través de una oficina satelital en cada país miembro facilita la cooperación interestatal, es por ello que su sede principal se encuentra en Lyon, Francia, sin embargo, cuenta con dos grandes subsedes principales en Nueva York y en Bruselas, con el objetivo principal de expandir la cooperación internacional de los estados.

Se entiende la actividad de la INTERPOL, en la cooperación a los estados, enmarcada bajo el estándar: "Neutralidad entendida como los límites de su intervención y cooperación está excluido por 'toda actividad o intervención en cuestiones o asuntos de carácter político, militar, religioso o racial'" (INTERPOL, 1946).

El Gobierno de Estados Unidos

Para delimitar el contexto internacional en cuanto a los Delitos Informáticos y de la disciplina científica Forense Digital se hace relevante identificar la intervención del Gobierno de Estados Unidos, en razón que es el país de origen de la Web, el Comercio Electrónico y la identificación de la comisión del primer Delito Informático, siendo la estructura orgánica y administrativa, como primera potencia mundial, dada por agencias federales y conformación de comisiones encargadas de manejar diferentes responsabilidades, tales como la gestión del programa espacial de Estados Unidos, la protección de sus bosques y la recolección de inteligencia e institutos de investigación forense que sirvan de cooperación tanto al departamento de investigación adscrito al departamento de justicia como a los organismos de investigación judicial; al igual que la representación judicial a través de los fiscales y defensores públicos y del ente encargado de la judicialización donde se tienen como participantes a los jueces y los jurados. Todos estos organismos poseen cooperación directa a nivel policial con la Interpol adscrita al Departamento de Justicia.

Es así como el gobierno de los Estados Unidos participa en el desarrollo y en la cooperación internacional contra la ciberdelincuencia, pues a su vez, la Internet es originaria de su país y es allí donde se da el mayor índice de cibercriminalidad en el mundo; también es considerado uno de los países con mayor cooperación internacional en contra a esta forma de criminalidad suscribiendo tratados internacionales con diferentes países de forma bilateral. Recientemente se suscribió un tratado con Italia, además de los impulsados con el Reino Unido y España, entre otros (Ciberdelincuencia.org).

[4] La INTERPOL intervino dando el concepto sobre la validez de los archivos hallados en el equipo portátil del guerrillero, esta cooperación permitió al gobierno colombiano iniciar procesos judiciales, administrativos y disciplinarios contra funcionarios y personajes civiles involucrados con las FARC, sin desconocer lo acaecido posteriormente entre el Consejo de Estado y la Corte Constitucional. Finalmente, las pruebas fueron endilgadas como nulas y excluidas de los procesos, sin que ello pueda fundamentarse en el tratamiento de las evidencias digitales.

SANS es una institución de investigación y educación en seguridad informática y campos afines. La educación que se imparte en esta institución permite difundir la educación a los auditores y administradores de red, que entre sí se cooperan mutuamente, con una única finalidad que es la lucha contra los desafíos que la delincuencia plantea, tal y como sucede con los delitos informáticos; ahora, la mayor cooperación y aprendizaje se encuentra encaminada a la seguridad de la información.

Se considera el instituto más confiable, y se encuentra entre los mayores referentes como fuente de seguridad en la información, incluso brindando certificación a los expertos sobre seguridad informática nivel mundial, la cual funciona como una forma de cooperación a los Estados y a todo ciudadano, a saber que investigador es profesional en la disciplina científica de investigación forense digital y realmente puede aportar su experticia en la solución de casos que involucren evidencias digitales.

Igualmente, el interés del instituto es la difusión y cooperación en las técnicas y protocolos forenses aplicables en caso de delitos informáticos y los demás que involucren la aplicación de herramientas informáticas, con la finalidad de ayudar a los investigadores certificados, poniendo a disposición de forma gratuita documentos de investigación científica en el campo de la seguridad de la información y en los aspectos que involucran la informática forense y el derecho informático, temáticas que nutren el contexto total del campo de la investigación forense digital para la obtención de evidencia digital, con la aplicación de protocolo y herramientas forenses, no solo las consideradas por certificadas por un instituto reconocido como es SANS, sino también que permiten la obtención de la evidencia digital con características de autenticidad, integridad, originalidad, confiabilidad y no repudio.

Uno de los aspectos más importantes y relevantes de SANS, como instituto, es el de los programas académicos que ofrece para la certificación de profesores o instructores que se dedican al campo de seguridad de la información y la ciberdelincuencia, siendo tan exigente el proceso en cuanto al nivel de competencia profesional en el área de conocimiento específico que se cuenta con un indicador de noventa personas matriculadas para el año 2011 con graduación certificada de solo cinco, que pudieron cumplir con el proceso académico; esta capacitación de formación para certificación internacional para instructores está direccionada en el aprendizaje de medidas prácticas necesarias para defender los sistemas y redes contra las amenazas más peligrosas, como son los ciberataques.[5] (Sans, 2012).

NIST[6] es un instituto que hace parte de la Agencia Federal de Estados Unidos; tuvo origen en el año 1901 en el Departamento de Comercio de los Estados Unidos con el fin de promover la competencia en innovación e industria, con proyección de metrología, normas y tecnología direccionada al mejoramiento de la calidad de vida.

Se encuentra dedicado a todos los campos científicos y disciplinares existentes, y los que están por desarrollarse; estableciendo políticas claras en materia de laboratorios, protocolos, herramientas, investigadores, entre otros aspectos.

[5] Programas de entrenamiento SANS. sitio web: *SANS*, disponible en: http://www.sans.org/top-cyber-security-risks/ y http://www.sans.org/,consulta: 13 octubre 2011

[6] Acerca de NIST, sitio web: *Instituto Nacional de Estándares y Tecnología*, disponible en: http://www.nist.gov/index.html, consulta: 13 octubre 2011

Uno de sus objetivos es la colaboración que permanentemente le brinda a la industria, promueve investigaciones para el gobierno americano que se materializan en el avance sobre la infraestructura tecnológica al servicio de la nación. Otro de sus alcances es la formación y la capacitación de instituciones e investigadores del campo privado y público, con especial énfasis para el reconocimiento de excelencia de desempeño y logro de la calidad.

Las competencias de acción del instituto son: ciencia de medición, rigurosa trazabilidad, y desarrollo y uso de estándares con énfasis en el desarrollo de la innovación al servicio de la ciencia y la industria.

La Tecnología de la Información (TI) hace parte de las ciencias y disciplinas de las que se ocupa el NIST, entre otras labores ha documentado el estado del arte de la ciberseguridad y biométricos; igualmente desarrolla Estándares y Tecnología que acelera el desarrollo y despliegue de sistemas que son confiables, utilizables, interoperables y seguros, en el ámbito de la computación forense, promoviendo siempre avances de la ciencia de la medición a través de innovaciones en matemáticas, estadística y ciencias de la computación. Otra de las facetas a cargo del instituto es realizar investigaciones para desarrollar la infraestructura de medidas y normas que responden a lo que hoy se conoce como nuevas tecnologías de la información, la comunicación y aplicaciones (soporte lógico o software).

Uno de los aspectos más importantes y relevantes de SANS, como instituto, es el de los programas académicos que ofrece para la certificación de profesores o instructores que se dedican al campo de seguridad de la información y la ciberdelincuencia, siendo tan exigente el proceso que de noventa personas matriculadas para el año 2011 solo cinco pudieron cumplir con su proceso académico y obtuvieron la certificación; esta capacitación para instructores está direccionada para el aprendizaje en medidas prácticas necesarias para defender los sistemas y redes contra las amenazas más peligrosas, como son los ciberataques. (Sans, 2012).

NIST es un instituto que hace parte de la Agencia Federal de Estados Unidos; tuvo origen en el año 1901 en el Departamento de Comercio de los Estados Unidos con el fin de promover la competencia en innovación e industria, con proyección de metrología, normas y tecnología direccionada al mejoramiento de la calidad de vida.

Se encuentra dedicado a todos los campos científicos y disciplinares existentes, y los que están por desarrollarse; estableciendo políticas claras en materia de laboratorios, protocolos, herramientas, investigadores, entre otros aspectos.

Uno de sus objetivos es la colaboración que permanentemente le brinda a la industria, promueve investigaciones para el gobierno americano que se materializan en el avance sobre la infraestructura tecnológica al servicio de la nación. Otro de sus alcances es la formación y la capacitación de instituciones e investigadores del campo privado y público, con especial énfasis para el reconocimiento de excelencia de desempeño y logro de la calidad.

Las competencias de acción del instituto son: ciencia de medición, rigurosa trazabilidad, y desarrollo y uso de estándares con énfasis en el desarrollo de la innovación al servicio de la ciencia y la industria.

La Tecnología de la Información (TI) hace parte de las ciencias y disciplinas de las que se ocupa el NIST, entre otras labores ha documentado el estado del arte de la ciberseguridad y biométricos; igualmente desarrolla Estándares y Tecnología que acelera el desarrollo y despliegue de sistemas que son confiables, utilizables, interoperables y seguros, en el ámbito de la computación forense, promoviendo siempre avances de la ciencia de la medición a través de innovaciones en matemáticas, estadística y ciencias de la computación. Otra de las facetas a cargo del instituto es realizar investigaciones para desarrollar la infraestructura de medidas y normas que responden a lo que hoy se conoce como nuevas tecnologías de la información, la comunicación y aplicaciones (soporte lógico o software).

Para el campo de la informática o computación forense promueve programas académicos de contenido novedoso y contemporáneo, satisfaciendo los retos diarios que la ciberdelincuencia plantea, entre los cuales podemos encontrar: Educación Nacional de Seguridad Cibernética de la Iniciativa (Niza), Biblioteca Nacional de referencia de Software es un proyecto apoyado por el Departamento de Justicia Estadounidense adscrita al Instituto Nacional de Justicia Federal, el Estado y Policía Local, además del National Institute of Standards y Tecnología-NIST, y las organizaciones de la industria para revisar los archivos de las computadoras, se puede definir esta cooperación como la forma eficiente y eficaz de usar tecnología informática “haciendo coincidir perfil de los archivos en el RDS, Esto ayudará a aliviar gran parte del esfuerzo necesario para determinar qué archivos son importantes como pruebas en los equipos o sistemas de archivos han sido incautados en el marco de las investigaciones penales” (NIST - National Institute of standards and technology), por ello se constituye como biblioteca dedicada al almacenaje de los tipos de software, Equipos forenses y referencia datos (CFReDS), permitiendo el desarrollo de equipos forenses de referencia Data Sets (CFReDS) para pruebas digitales.

Estos conjuntos de datos de referencia (CFReDS) proporcionan un conjunto de datos para el investigador documentando casos de pruebas digitales simulados para examen entre los cuales se pueden encontrar casos que dan cuenta de cadenas de búsqueda de destino en establecen lugares conocidos de CFReDS, los investigadores podrían comparar los resultados de búsquedas para las cadenas de destino con la colocación de las cadenas conocidas (entiéndase el término cadena referente a cadenas de custodia que son dadas en cada ordenamiento jurídico penal a nivel nacional e internacional para el tratamiento de delitos).

Los investigadores pueden igualmente acceder a esta información para la validación de las herramientas software que se utilizan en las investigaciones, los equipos y la formación de investigadores como parte de acreditación de un laboratorio forense, aspectos relevantes para dar credibilidad a un informe forense digital en el curso de una investigación penal.

El planteamiento internacional en materia de laboratorios, protocolos y herramientas forenses, al igual que investigadores en el campo de la disciplina forense digital, es válido para el entorno internacional, al igual que es aplicable en todos los Estados; es por ello que Colombia no se aleja, y tanto en

el campo público como en el privado, la validez de la evidencia digital tiene mayor fortaleza cuando esta generada bajo estándares internacionales como los certificados por SANS, NIST e INTERPOL entre otros, toda vez que han sido creados para la investigación científica en el campo.

Colombia ha dedicado sus esfuerzos a fortalecer el estado en ciberseguridad y ciberdefensa, como política pública de estado, a fin de garantizar la seguridad de la información, generando una interrelación de las entidades gubernamentales involucradas en el desarrollo de las bases normativas del campo y mecanismos direccionados a garantizar la seguridad de la información a nivel nacional. Aunque su labor deberá siempre tener en cuenta las normas técnicas y los estándares nacionales e internacionales (Departamento Nacional de Planeación, 2011).

REFERENTES TEÓRICOS

CAPÍTULO 3.

UNA MIRADA JURÍDICA A LOS DELITOS INFORMÁTICOS EN COLOMBIA Y SU EVOLUCIÓN LEGAL EN EL MARCO DEL DERECHO COMPARADO

Ana María Mesa Elneser

Jorge Eduardo Vásquez Santamaría

Análisis desde la Ley 1273 de 2009

Antecedentes

a) Antecedentes conductuales relevantes en el ámbito internacional

La realidad delictual en materia informática comenzó a evidenciar situaciones de gran afectación a los bienes jurídicos de la información, los datos, e incluso a la intimidad, lo que despertó la necesidad de la regulación para el control y represión de dichas conductas. Como antecedentes destacados en el contexto global se referencian los ataques contra los equipos y redes de los Proveedores de Servicios de Internet (ISP), los ataques políticos contra determinados websites, la introducción en equipos de la red informática para sustraer información confidencial, la revelación de información sensible de los clientes de una empresa o institución y los Ataques Distribuidos (DDOS) mediante equipos "zombis" controlados de forma remota. Una reflexión expuesta en 1996, por August Bequai, en el Consejo de Europa en Bruselas dice:

> Si prosigue el desorden político mundial, las redes de cómputo globales y los sistemas de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos. (…) Las guerras del mañana serán ganadas o perdidas en nuestros centros de cómputo, más que en los campos de batalla. ¡La destrucción del sistema central de una nación desarrollada podría conducir a la edad del oscurantismo! (…) En 1984, de Orwell, los ciudadanos de Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta. En el mundo moderno, todos nos encontramos bajo el ojo inquisidor de nuestros gigantes sistemas computacionales. En occidente, la diferencia entre el Hermano Grande y nuestra realidad es la delicada fibra política llamada democracia; de colapsarse ésta, el edificio electrónico para una implantación dictatorial ya existe. (…) La revolución de la electrónica y la computación ha dado a un pequeño grupo de tecnócratas un monopolio sobre el flujo de información mundial. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos. Somos ahora testigos del surgimiento de una elite informática (A. Bequai, Comisión de las comunidades Europeas, 1996).

En lo relacionado con los ataques contra los equipos y redes de los proveedores de servicios de Internet, los registrados en los últimos años han tenido como consecuencia la revelación de los datos y las claves de acceso de sus clientes, la manipulación o eliminación de ficheros y páginas web y el acceso a los buzones de correo electrónico de los clientes. Por ejemplo, en agosto de 1999 un fallo de seguridad en el servicio de correo electrónico hotmail perteneciente a Microsoft dejaba al descubierto durante varias horas los mensajes de correo de cuarenta millones de usuarios, ya que el sistema permitía acceder a las cuentas sin necesidad de introducir ninguna contraseña (Firtman, 2005, p. 312).

En el tema de ataques políticos contra websites, se registran por ejemplo los ataques sufridos por el servidor web de la OTAN en 1999, a raíz de la intervención realizada por la Alianza entre Serbia y Kosovo; se destacan los ataques de árabes contra páginas de Israel (y viceversa) y más

recientemente los ataques contra determinados websites para lanzar mensajes reivindicativos en contra de la Guerra de Irak (Firtman, 2005, p. 312).

En febrero de 2006 más de mil páginas web danesas fueron víctimas de una oleada de ataques procedentes de países islámicos debido a la crisis provocada por la publicación de unas caricaturas de Mahoma en un diario de ese país. En muchos casos estos ataques consiguieron modificar las páginas web, sustituyendo el contenido original con proclamas a favor del Islam o mensajes amenazantes contra los daneses (Firtman, 2005, p. 312).

La introducción en equipos de la red informática para sustraer información confidencial tiene casos registrados, como el incidente sufrido por Microsoft en el año 2000: durante tres meses unos piratas informáticos habían conseguido burlar los sistemas de seguridad de esta empresa para tener acceso a ordenadores de su red interna que contenían el código fuente de sus productos más importantes (Windows, Office, herramientas de Internet, etc.). El incidente parece estar originado por un empleado de Microsoft que recibió un correo electrónico aparentemente inofensivo que contenía un troyano en un fichero adjunto, denominado “QAZ. Trojan”, diseñado para abrir puertas traseras en los equipos infectados. Instalado este troyano se procedía al envío de la dirección del ordenador infectado a otro situado en algún lugar de Asia, reduciendo así el nivel de seguridad de este ordenador infectado para facilitar la instalación de herramientas más sofisticadas de asalto. Una vez instaladas estas herramientas (*snifers* y rastreadores de contraseñas), el troyano localizó nombres de usuario y sus correspondientes contraseñas, enviándolas a una dirección de correo electrónico de San Petersburgo, en Rusia.

Gracias a estas contraseñas los piratas informáticos consiguieron acceder a los ordenadores de la red interna de Microsoft haciéndose pasar por empleados. La compañía sólo tuvo conocimiento de la actividad de los intrusos cuando detectó el envío de un correo electrónico con contraseñas secretas desde un ordenador interno de la empresa. A finales de febrero de 2006, la propia Microsoft reconocía que debido a un error interno había publicado en una de sus páginas web información supuestamente confidencial sobre el lanzamiento de su nuevo sistema operativo, Windows Vista (Firtman, 2005, p. 312).

Pero vale la pena aclarar que la revelación de información sensible de los clientes de una empresa o institución es una conducta que ha sido vivida por una gran cantidad de compañías con consecuencias severas. En marzo del año 2000, un fallo de seguridad en el portal financiero de Terra tuvo como consecuencia que todos los datos de sus usuarios: nombre, apellidos, *login*, *password* y sus movimientos en la cuenta quedaran al descubierto por unas horas. Este incidente supuso además la imposición de una sanción de 120.000 euros contra Terra por parte de la Agencia Española de Protección de Datos, al considerar que esta empresa no había adoptado las medidas de seguridad adecuadas para proteger los datos personales de sus clientes, incumpliendo de este modo la Ley Orgánica de Protección de Datos (LOPD) (Firtman, 2005, p. 312).

Otro antecedente importante se presentó en noviembre de 2001 con el website de la revista *Playboy,* el cual sufrió un ataque por parte de unos crackers que se hicieron con los datos personales de los usuarios registrados: nombre, domicilio e incluso los datos de sus tarjetas de crédito para acceder a las secciones de pago del website. Larry Lux, presidente de la compañía, reconocía la situación a través de una carta que remitió a sus clientes y usuarios, recomendándoles que contactasen con su entidad financiera para comprobar los posibles cargos en sus tarjetas de créditos. *Playboy* tuvo conocimiento de este ataque no gracias a sus cortafuegos u otras medidas de seguridad internas, sino porque el presunto atacante se dirigió a los clientes y usuarios del website para informarles de que había conseguido acceder a sus datos personales, incluidos los de sus tarjetas de crédito (Firtman, 2005, p. 312).

El Gobierno del Reino Unido, en junio de 2002, se vio obligado a suspender temporalmente el Servicio de Declaración de Impuestos on-line, tras detectarse un grave fallo informático que permitía a los usuarios acceder a los datos confidenciales de otros declarantes. En este caso fueron los propios usuarios quienes detectaron el fallo del Servicio de Impuestos, y los que informaron que mientras complementaban sus datos *online* podían acceder a los datos relativos de otros ciudadanos simplemente cambiando el código de identificación que figura en la dirección URL de la página web que estaban visualizando.

En junio de 2003, un grupo de hackers españoles, conocidos con el nombre de “Mentes inquietas”, publicaba en su página web diversas pruebas de cómo habían podido acceder a datos de distintos usuarios del banco Uno-e (entre ellos sus cuentas y saldos disponibles), aprovechando deficiencias en la seguridad de su website. Simplemente modificando en la dirección URL de la página web el parámetro con el identificador de un usuario, había sido posible acceder a los datos de otro usuario sin que fuera necesaria una nueva autenticación por parte del servidor de la entidad financiera.

La empresa LexisNexis se dedica a la venta de información de ciudadanos estadounidenses a otras empresas, investigadores privados e instituciones financieras. Esta compañía sufrió un ataque informático en enero de 2005, cuando unos crackers tuvieron acceso a la información de más de 300.000 ciudadanos almacenada en la base de datos de esta empresa. Los ciberdelincuentes podrían utilizar esta información para solicitar tarjetas de crédito bajo nombres falsos o para apropiarse de la identidad de estas personas para otros fines ilegales. Supuestamente el acceso ilegal a su base de datos se produjo cuando la empresa permitió que los ciberdelincuentes asumieran identidades de clientes legítimos para conectarse a su red informática.

Igualmente, la empresa ChoicePoint, compañía competidora de LexisNexis, admitió en febrero de 2005 que había entregado a estafadores, que se hicieron pasar por clientes, los datos de 145.000 ciudadanos. También, en 2005, Bank of America reconocía haber perdido unos ficheros que contenían información sobre más de un millón de trabajadores del gobierno federal, entre ellos

varios senadores estadounidenses. En ese mismo año unos crackers consiguieron entrar en una base de datos del Boston College, donde se almacenaba información de 100.000 antiguos alumnos. Un incidente similar tuvo lugar en enero de 2005 en la Universidad George Mason, en Virginia, cuando los ciberdelincuentes tuvieron acceso a los datos de más de 30.000 estudiantes y empleados de esta universidad.

En agosto de 2005 se descubrió el caso de un cracker que había logrado introducirse en algún momento, entre los meses de mayo o junio de 2005 en una base de datos de la Fuerza Aérea de Estados Unidos que contenía información personal de unos 33.000 militares. El ciberdelincuente se hizo con números de la Seguridad Social (el equivalente al número de cédula en Colombia), fechas de nacimiento y otra información con la que potencialmente podría hacerse pasar por estos oficiales.

El portal de Internet del Servicio de Hacienda del Reino Unido fue víctima de la actuación de varias bandas organizadas que consiguieron suplantar la identidad de al menos 13.000 empleados de la empresa ferroviaria Network Rail y modificar su situación; un fraude de enormes proporciones que ha tenido un coste de veintidós millones de euros para el Servicio Fiscal de este país. Los estafadores suplantaron la identidad de los trabajadores de la empresa ferroviaria, utilizando el nombre, la fecha de nacimiento y su número de identificación para a continuación realizar un cambio en su situación fiscal en lo referente al número de hijos, el estado civil o la situación laboral, reembolsándose los beneficios que se derivaban de esta situación (una cantidad cercana a los 150 euros mensuales por empleado).

Relacionado con casos de empleados descuidados que revelan información confidencial se identifica lo sucedido en enero de 2005 donde un miembro del ejército holandés había compartido por error documentos confidenciales sobre determinadas personas a través de la red P2P de Kazaa, utilizando para ello su propio ordenador personal. También Mitsubishi Electric de Japón reconocía, en junio de 2005, que se había difundido a través de Internet información confidencial sobre plantas nucleares de diferentes lugares de ese país, proveniente de un ordenador personal de un inspector de centrales de la compañía que había sido infectado por un virus informático.

Finalmente, algunos de los ataques distribuidos (DDOS) mediante equipos “zombis” controlados de forma remota, se ejemplifican con el caso dirigido contra los trece servidores raíz (*root servers*) del servicio DNS, cuyo papel resulta fundamental para el mantenimiento del directorio maestro de los recursos de la propia Internet.

En ese momento los internautas no experimentaron lentitud ni desconexiones en su navegación gracias a las medidas de protección existentes en la arquitectura de Internet, pero un ataque más prolongado y extenso podría haber dañado seriamente las comunicaciones electrónicas en todo el mundo.

En 2004 se produjo un ataque masivo durante varios días contra los servidores del LRC Hispano, provocando un deterioro de la calidad del servicio e impidiendo que algunos usuarios pudieran comunicarse con normalidad. Los responsables tuvieron que restringir el tráfico procedente de algunas zonas geográficas concretas para poder limitar los efectos de este ataque, poniéndolo además en conocimiento de la Unidad de Delitos Informáticos de España.

b) Antecedentes legislativos en Colombia

Colombia no ha sido ajena a la gravosa realidad de la criminalidad informática. Los amplios antecedentes citados a nivel global encuentran en el caso de nuestro país un caso preocupante que clama por la consolidación de medidas jurídicas eficaces que se correspondan con los medios forenses suficientes y óptimos para probar y soportar la comisión de las conductas.

Resumir la problemática en el caso de Colombia es posible con un ejemplo reciente por medio del cual las cifras dan cuenta de la imperiosa urgencia de especializar el sector oficial en la materia y de dotar al Estado colombiano de todas las herramientas necesarias que especialicen esta área del Derecho. El pasado 30 de octubre de 2011, Colombia celebró una jornada electoral para elección de gobernadores, alcaldes, diputados y concejales, la cual se caracterizó por las siguientes noticias:

> Pese a los intentos de ataques cibernéticos realizados ayer a la página web de la Registraduría Nacional, el blindaje adoptado por la Entidad para proteger su información y sus datos demostró ser exitoso.
>
> Entre las 4:00 pm y las 7:00 pm de ayer domingo 30 de octubre, el sitio web recibió 35.618.582 visitas, pero adicionalmente se registraron más de 400 millones de accesos bloqueados, correspondientes a tráfico malicioso y más de 2.000 direcciones IP fueron bloqueadas.
>
> En cuanto al componente de Seguridad Informática se implementó una novedosa tecnología de mitigación de ataques distribuidos a gran escala, como los que se evidenciaron contra la infraestructura de la Entidad desde el sábado 29 de octubre y que su magnitud se explica por sí sola con las siguientes cifras:
>
> • Más de 400 millones de accesos bloqueados, correspondientes a tráfico malicioso.
> • Más de 2.000 direcciones IP bloqueadas.
> • Ataques provenientes desde Colombia y de ocho países más alrededor del mundo.
>
> Los ataques que se bloquearon fueron realizados por colectivos internacionales de Hackers quienes actuaron de forma concertada y conjunta, tales como Anonymous Colombia, Anonymous Chile, Colombian Hackers y Lulzsec; este último famoso por recientes ataques exitosos a redes y páginas Web internacionales como Mastercard, Visa, Sony, Honda, Policía Española, Parlamento Australiano, FBI y al consultor federal de seguridad HB Gary en los Estados Unidos, entre otros.

> Es importante resaltar que la totalidad de las evidencias recogidas de los ataques bloqueados, están contenidos en más de 28 Gigabytes de información que están a disposición tanto de la Entidad, como de las autoridades competentes.
>
> Entre las medidas de seguridad adoptadas por la Registraduría Nacional del Estado Civil para proteger su información y los datos de este domingo se encontraba la de alojar su página web en servidores ubicados en Estados Unidos como medida de seguridad. Este servicio de alojamiento continuará durante los próximos días.
>
> Otras de las medidas adoptadas fueron la de entregar la información de manera descentralizada y por ello en cada departamento se habilitó una de prensa con canales de comunicaciones especiales, lo que permitió que de manera local se conociera el proceso, antes de proceder a la consolidación nacional de información (Sincelejo Herald, octubre de 2011).

Otros medios de comunicación registraron la misma noticia en términos como:

> El registrador Carlos Ariel Sánchez en diálogo con la F.M. reveló que fueron detectados más de 400 millones de accesos que no correspondían a consultas válidas, y que al parecer pretendían hackear la página de la entidad. Indicó que dichos accesos fueron bloqueados impidiendo ser blanco de saboteos (La F.M., octubre de 2011).
>
> La seguridad de la página de la Registraduría bloqueó más de dos mil direcciones IP. Sin embargo, la semana pasada la página web de la entidad fue migrada como medida de seguridad para blindar los datos y la información de los comicios (Radio Nacional de Colombia, octubre de 2011).
>
> Según el registrador, la página web recibió 25 millones de accesos válidos y más de 400 millones de intentos de hackers, los cuales fueron enfrentados a través de 'contratos con servidores poderosos fuera del país y la ejecución de medidas antihackers como los temporizadores de consultas'. Sánchez explicó que los temporizadores impiden consultas abiertas, es decir que si la consulta demanda varios minutos, se cierra de forma automática y es necesario el reingreso a la página (Semana.com, octubre de 2011).

Acontecimientos como los descritos dejan ver la necesidad de la intervención del Derecho en el campo informático para la protección de múltiples bienes jurídicos concurrentes en la comisión de acciones delictivas como las mencionadas, siendo el más relevante de ellos el derecho a la información.

Fue por ello que Colombia buscó en años anteriores la incorporación de un conjunto de tipos penales destinados a la protección del mencionado bien, apareciendo en el contexto jurídico nacional la denominada ley de delitos informáticos.

Promulgada el 5 de enero de 2009 permitió la incorporación al Código Penal Colombiano de un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos". Esta nueva legislación en Colombia presenta antecedentes que evidencian un contexto político complejo para su aprobación, así como la lectura de una realidad delictiva creciente en materia internacional.

Específicamente, el proyecto legislativo sobre inclusión del tema fue una iniciativa que comenzó aproximadamente desde finales de los años noventa y principios del 2000 con la intención de concientizar a la judicatura y a jurisconsultos con el delito informático, cuenta Alexander Díaz García, autor del proyecto. En un principio, los congresistas registraron el texto, y por técnica legislativa se acordó que su trámite comenzaría en la Cámara de Representantes, siendo su ponente el doctor Carlos Arturo Piedrahíta Cárdenas, perteneciente a la Comisión Primera de esa corporación, quien lo lideró.

El trámite legislativo del mencionado proyecto de ley contó con varias dificultades, entre ellas la oposición de varios parlamentarios que afirmaban lo innecesario de la legislación en la materia debido a la preexistencia de la Convención de Budapest, Hungría, del año 2001, sobre cibercriminalidad, figura internacional que podría ingresar al ordenamiento jurídico colombiano dejando de lado la iniciativa legislativa de contar con tipos penales y disposiciones diversas (Díaz García, enero de 2010). Adicionalmente, reporta Díaz García (enero de 2010) las dificultades en la Mesa de Trabajo del Ministerio de Relaciones Exteriores, en donde se puso en consideración de los miembros de la misma el proyecto de ley, a la postre el único que se había presentado, donde se manifestó su posible acogida en el legislativo, debido a que ese poder se inclinaba por una norma procesal y no sustantiva como era el caso de la Ley 1273, afirmación que realizaba el delegado del Señor Fiscal General de entonces.

En el proceso legislativo el Senador Parmenio Cuéllar Bastidas, ex ministro de Justicia de Colombia, registró ponencia negativa para hundir el trámite logrado hasta este momento en la Cámara, acontecimiento que se superó en la Comisión Conciliadora para finalmente lograr el 5 de enero de 2009 la sanción presidencial de la actual Ley 1273.

Como toda legislación, la ley de delitos informáticos en Colombia procura un alcance general, abstracto e impersonal dirigido a garantizar un bien común representado en la protección de la información y de los datos. Sin incurrir en redundancias, la ley debe mantener su fiel propósito de ser reguladora de la conducta humana en su dinámica social, y ante desorganizaciones que quebranten el orden institucional,[1] o la carencia de disposiciones que atiendan las demandas y urgencias de una colectividad por medio del ordenamiento jurídico promulgado por las autoridades estatales competentes, el Derecho debe elaborar e incorporar en su sistema objetivo, aquellas normas jurídicas que se dirijan a las nuevas dinámicas sociales complejas.

En este caso, los tipos penales informáticos son la base de la informática forense, y como tal, ejemplifican un nuevo fenómeno conductual de alcance internacional desarrollado en la era moderna, de avances intensamente significativos que ponen en riesgo y situación de vulnerabilidad a los diversos mecanismos de seguridad y gestión.

[1] Si retoma la sustentación del concepto de Derecho desde la Teoría Institucionalista de Santi Romano, Mauricio Houriou o Carl Schmitt.

c) Convención sobre Cibercrimen de Budapest

Este acápite fue debidamente desarrollado en la unidad temática 2 de la Convención de Cibercrimen, convirtiéndose en los lineamientos de política pública internacional de carácter obligante para los Estados miembros fundadores y adheridos, al igual que se convierte para los Estados que aun no lo han ratificado como un espectro legal internacional para el tratamiento del ciberdelito y la ciberdelincuencia.

Un ejemplo de ello es el lineamiento que existe en la convención sobre el acceso a archivos o ficheros donde se contiene información, requerida siempre, como fundamento para vincular al sujeto activo de la conducta con el delito cometido, pues la sola prueba pericial no involucra al sujeto, salvo que esté complementada y soportada en los logs de tráficos de datos que posee el ISP en sus servidores de almacenamiento de la información, temática que en Colombia se encuentra restringida de forma significativa en correlación con la intimidad de la persona natural, consagrada en el Artículo 15 de la Constitución Política, y el límite que el acceso a la información posee igualmente desde el contexto internacional como lo indica el Artículo 20 de la Carta Política, para ambas disposiciones, para su interpretación de violación o no de la información almacenada por un tercero, se hace necesaria la correlación con la Ley 1266 de 2008 o Ley de Habeas Data, en la cual se definen los niveles que categorizan el dato personal, que impacta el tema de la información delimitando su disponibilidad como Dato Público, Dato Semipúblico y Dato Privado.

d) CONPES 3701 del 14 de julio de 2011

Llama la atención que solo dos años y seis meses posterior a la expedición de la Ley de Delitos Informáticos en Colombia, el gobierno nacional se haya ocupado de una política pública de Estado, documentada en el CONPES 3701 donde se estudian la ciberseguridad y la ciberdefensa, política enmarcada bajo el análisis sobre el aumento de la capacidad delincuencial en el ciberespacio, así como de la utilización de nuevas tecnologías para generar amenazas informáticas y que constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado y en la sociedad civil.

En relación con la seguridad cibernética, Colombia ha sido objeto de ataques. Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo *hacktivista* autodenominado Anonymous atacó a los portales de la presidencia de la República, el Senado de la República, Gobierno en Línea y de los ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley “por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet”.

Colombia es uno de los países que actualmente no cuenta con una estrategia nacional en ciberseguridad y ciberdefensa, que incluya un sistema organizacional y un marco normativo e institucional lo suficientemente fuerte para afrontar los nuevos retos en aspectos de seguridad cibernética.

El creciente aumento de usuarios de Internet, la elevada dependencia de la infraestructura crítica nacional a los medios electrónicos, así como el notable incremento de incidentes y delitos contra la seguridad cibernética, ha permitido identificar el elevado nivel de vulnerabilidad del país ante amenazas cibernéticas, tales como el uso de Internet con fines terroristas, el sabotaje de servicios, espionaje y hurto por medios electrónicos, entre otros.

El entrenamiento y formación de los funcionarios públicos y privados para reaccionar como primeros respondientes ante la comisión de los delitos informáticos es deficiente. En muchas ocasiones se pierde la cadena de custodia de la evidencia digital y se generan dificultades en la realización de las investigaciones forenses.

Así mismo, existe una oferta limitada de programas de capacitación para entidades que realizan funciones de policía judicial en el tema. Pese a que existen instrumentos legales y regulatorios en seguridad de la información, persisten falencias que impiden responder oportunamente a incidentes y delitos cibernéticos.

A pesar de que se dan algunos esfuerzos institucionales (tanto privados como públicos), se ha identificado que no existen organismos a nivel nacional constituidos para coordinar y desarrollar operaciones de ciberseguridad y ciberdefensa. Por tanto, no ha sido posible implementar los mecanismos suficientes y adecuados para contrarrestar ataques cibernéticos y proteger los intereses del Estado en el ciberespacio.

Recientemente el Congreso de la República aprobó la Ley de Inteligencia y Contrainteligencia, estableciendo mecanismos de vigilancia y control para estas actividades. A pesar de ello, ésta es una regulación que requiere particularizarse para el ejercicio de la ciberseguridad y la ciberdefensa, sobre la cual existe muy poco en términos de alcance y operatividad.

Teniendo en cuenta lo anterior, se puede decir que la solución debe radicar en fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio. Para este fin es necesario involucrar a todos los sectores e instituciones del Estado con responsabilidad en el campo de ciberseguridad y ciberdefensa, creando un ambiente participativo donde todos los actores de la sociedad actúen con propósitos comunes, estrategias concertadas y esfuerzos coordinados. Igualmente, es de vital importancia crear conciencia y sensibilizar a la población en todo lo referente a la seguridad de la información; fortalecer los niveles de cooperación y colaboración internacional en aspectos de ciberseguridad y ciberdefensa; apoyar las investigaciones relacionadas con ataques informáticos y proteger a la ciudadanía de las consecuencias de estos ataques.[2]

[2] Texto elaborado por parte del equipo de semillero de la universidad IDEAS, en coordinación con el doctor Rodrigo Orlando Osorio, con la mirada sobre el impacto del CONPES en Colombia, extraído del informe presentado en diciembre de 2011.

e) Delitos informáticos: definiciones y concepto

A partir del rastreo bibliográfico realizado el delito informático es definido como aquel que representa:

> Aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático (…) implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho (…) puede comprender tanto aquellas conductas que recaen sobre herramientas informáticas propiamente tales, llámense programas, ordenadores, etc.; como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc. (García Espinal, marzo de 2009).

Jhon Jairo Echeverri Aristizábal define los delitos informáticos como "todas las conductas ilícitas realizadas por un ser humano, susceptibles de ser sancionadas por el derecho penal en donde hacen un uso indebido de cualquier medio informático, con la finalidad de lograr un beneficio". Por su parte, Noelia García Nogera (julio de 2002) afirma que con delito informático "se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes".

Pero sin duda, la definición más acertada y completa sobre la figura de los delitos informáticos se genera con la explicación del Juez Alexander Díaz García (enero de 2010), quien manifiesta que son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinada a producir un perjuicio a la víctima, atentados a la sana técnica informática, lo cual, generalmente producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

Cristian Andrés Meneses (septiembre de 2002), citando a Julio Téllez Valdés, menciona que los delitos informáticos se pueden conceptualizar de forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

También Cristian Andrés Meneses (septiembre de 2002), al citar a Marcelo Huerta y Claudio Líbano, expresa que estos delitos son,

> Aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de

> tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

Finalmente, menciona la definición de Ezequiel Zabale: "Toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, y el cual se distingue de los delitos computacionales o tradicionales informatizados" (Meneses, septiembre de 2002).

En su trabajo "Delitos informáticos: generalidades" el profesor Santiago Acurio del Pino presenta un valioso apartado del debate doctrinario por medio del cual se han definido los delitos informáticos desde distintas experiencias jurídicas. Desde Julio Tellez Valdés (1996), Acurio del Pino (2011) retoma a Nidia Callegari, que menciona que el delito informático es "aquel que se da con la ayuda de la informática o de técnicas anexas" (p. 10), criticando de este concepto la restricción que hace de la informática como medio de comisión de las conductas delictivas sin incluirla como objeto de la acción criminal.

A su vez el profesor Tellez Valdés (1996) acude a la explicación del delito informático según Davara Rodríguez, quien lo define como 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 vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" (Acurio del Pino, 2011, p.10).

El enriquecido debate da cuenta de una elaboración conceptual tan nutrida y variable como la tecnología misma, sirviendo de sustento a la figura de los delitos informáticos. En palabras de Carlos María Romeo Casabona (1987) se definía la realidad de los delitos informáticos desde la experiencia española en la década de los años ochenta de la siguiente manera:

> En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información (Acurio del Pino, 2011, p. 8).

Sin duda, vincular esta modalidad delictual exclusivamente a las computadoras es algo que esta revaluado desde los alcances conceptuales de la informática jurídica, pues la especialización en la materia, como ha sucedido en el caso colombiano, ha identificado una variedad de elementos

a partir de los cuales se configura la comisión de la variada gama de conductas tipificadas como delitos informáticos, como es el caso de los datos informáticos, un sistema informático o una red de telecomunicaciones.

Ello conduce a reiterar que la figura del delito informático no se refiere a solo una modalidad de tipo penal sino a una multiplicidad de comportamientos que pueden y deben ser tipificados de forma independiente, claridad que aunque obvia, ha contado con mucha fuerza en los aportes doctrinarios sobre la materia. En ello coinciden Acurio del Pino y Romeo Casabona, quienes son enfáticos en reiterar que el delito informático alude a una pluralidad de conductas que incurren en la acción ilícita desde diversos elementos informáticos.

Acurio del Pino (2011) acude a los chilenos Marcelo Huerta y Claudio Líbano para exponer la que estima es la mejor de las definiciones de los delitos informáticos. En su texto explican:

> Debido a que el concepto a definir es un concepto inmerso en el derecho, no nos cabe duda que son precisamente los expertos de este mundo-ciencia los llamados irrefutablemente a diseñar la definición de los delitos informáticos. El derecho es una ciencia llamada a regular todos los tópicos de la vida en sociedad y especialmente a salvaguardaría, sobre principios de justicia, de los atentados a la normal y pacífica convivencia. Desde esta perspectiva, el derecho debe entregar la definición del Derecho Informático y por ende de sus delitos, en relación de continente a contenido. Se podrá decir que el jurista no está capacitado para indagar en los fenómenos de la informática y que por lo tanto la definición debe provenir de aquellos que han abrazado ciencias relacionadas con ella. Sin ánimo de polemizar, decimos que el Derecho como expresión normativa de la Justicia regula todos los aspectos de la convivencia social, incluida la actividad informática que se aplica en toda actividad humana, con tanta trascendencia social y económica. Para tan alta empresa, el derecho, muchas veces se auxilia en los conocimientos propios de otras ciencias, a los cuales les aplica su sello distintivo constructor de normas y principios jurídicos. Pensar lo contrario, implicaría imposibilitar al mundo del derecho de normar sobre la medicina forense, las ingenierías, las ciencias que abarcan la expresión pública, etc. Aún más grave, se pondría al juez, que es un abogado, en la imposibilidad de administrar justicia en materias ajenas al derecho (p. 13).

Pero como asegura Heidy Balanta (2009) ningún organismo se ha atrevido a dar una definición concreta que integre todos los elementos de un delito informático, pues en ese intento se puede correr el riesgo de no incluir elementos propios de este delito, o confundirlo y caer en otro tipo de delito que no es el informático, adicional a los intensos cambios y variaciones de todos los soportes tecnológicos que sirven de elementos objetivos para que estos tipos se configuren.

Echavarría Aristizábal describe como características de los escenarios de comisión de los delitos informáticos la variación de la escena del delito (escenas virtuales), clandestinidad, efectividad, tiempos cortos en la ejecución, ganancias, falta de testigos, no rastro, la seguridad del delincuente, lo complejo de los hallazgos digitales, ingenuidad de las personas, falta de seguridad de los equipos en el domicilio, el trabajo, los cafés Internet, etc.

En el caso colombiano, los delitos informáticos comienzan a contar con varias disertaciones importantes que procuran delimitar y puntualizar su naturaleza y componentes. Varios aportes doctrinales comienzan a abordar el tema desde la experiencia nacional promovida con la Ley 1273 de 2009.

Yesica García Espinal (marzo de 2009) asegura que los delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático; asegura que esta modalidad delictiva implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, afirmando que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del Derecho, afirmación que se estima adelantada y poco profunda una vez se tienen presentes los alcances y dimensiones de la actividad delictiva promovida por medio de los soportes informáticos. Bien define la citada autora (marzo de 2009) que la comisión de un delito informático puede comprender tanto aquellas conductas que recaen sobre herramientas informáticas propiamente tales, llámense programas, ordenadores, etc.; como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, etc.

Esto nos lleva a reconocer que la modalidad delictiva tipificada como delito informático no reduce el campo de acción del sujeto activo al simple uso de una computadora, lo que desvirtúa imaginarios tradicionales que aferran estas categorías delictivas a solo esos implementos. ¿Qué más implica un delito informático? Esta pregunta conduce a la apertura de una posibilidad de conocimientos que desde el cúmulo de estudios y avances doctrinarios parece aún no haber sido explorada.

Si bien se exponen aproximaciones y algunas caracterizaciones sobre los denominados delitos informáticos, la experiencia internacional se encuentra en una etapa de exploración y descripción en materia jurídica que deja en un escenario incipiente los tratamientos sobre el tema. Dicha situación no es tampoco ajena en Colombia, lo que se ejemplifica en comentarios de doctrinantes como los citados de Heidy Balata, e incluso de García Espinal (marzo de 2009), quien asegura:

> La ley colombiana no define el delito informático como tal, lo que sí ha hecho es regular ciertos casos como acceso abusivo a redes y otros delitos derivados de corrientes internacionales. Es importante tener en cuenta que, sin perjuicio de que exista o no una definición de que es o que no es un delito informático, el Código Penal y el Código de Procedimiento Penal traen definidos, delimitados y regulados muchísimos delitos que son susceptibles de ser cometidos en un entorno informático. Y, es allí precisamente, donde el juzgador y los investigadores deben encontrar la relación.

Como menciona la cita anterior, y como se verá en la presente investigación, la legislación colombiana se aventuró en un esfuerzo por modernizar el ordenamiento jurídico penal, logrando disponer una reforma al Código Penal con la adición del Título VII denominado “De la Protección de la

información y de los datos". A continuación se presenta el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y de legislación complementaria, abordando los principales referentes internacionales y experiencias desde el Derecho Comparado.

f) Tipos penales a partir de la Ley 1273 de 2009

La denominada ley de delitos informáticos dispuso un total de nueve nuevos tipos penales destinados al bien jurídico de protección de la información y de los datos, y de la preservación integral de los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Para presentar un análisis de los tipos penales informáticos se procederá inicialmente con una leve recapitulación de la figura del tipo penal, posteriormente se clasifica cada una de ellas dentro de las modalidades doctrinales más comunes, y finalmente se describen los elementos objetivos que la integran. Posteriormente se hará un análisis del alcance y aplicación desde la informática a los diferentes verbos rectores que cada tipo penal consagra y que, tal como se evidencia en el resultado de las encuestas cerradas aplicadas como instrumentos, la terminología aplicada a los tipos penales genera problemas de interpretación jurídica y en algunos casos falencias para su judicialización.

El tipo penal es una figura estrechamente vinculada con la tipicidad, componente de la estructura del delito en el ordenamiento jurídico colombiano. Un tipo penal resulta del trabajo agotado por el legislador a partir de las condiciones evidenciadas de la realidad, si se tiene presente la corriente que propone la influencia y determinismo de la sociedad sobre el Derecho, haciendo del legislador el poder público encargado por mandato constitucional de normar por medio de la ley las conductas necesarias para mantener el orden y la convivencia pacífica.

De allí que sea el legislador el encargado de disponer por medio de leyes los tipos penales, regulando las conductas, notables socialmente, que atentan contra bienes jurídicos de relevancia, para el caso, la protección de la información y de los datos y de la preservación integral de los sistemas que utilicen las tecnologías de la información (T.I.) y las comunicaciones.

Así, el tipo penal se define como la fórmula o símbolo que utiliza el legislador para describir conductas, para individualizarlas; es el instrumento legal del que se vale el legislador para definir conductas que en caso de su comisión u omisión, atentan contra bienes jurídicos tutelables.

Es expresión del principio de legalidad, y con ello, es la descripción de la conducta socialmente relevante hecha por el legislador; por ello es un instrumento legal, lógicamente necesario y de naturaleza predominantemente descriptiva, que tiene por función la individualización de los comportamientos humanos.

Aquellos tipos penales reservados a la descripción de las conductas exaltadas frente al sector de la informática se han denominado delitos penales, siendo en el caso de la Ley 1273 la primera de esas conductas el acceso abusivo a un sistema informático.

CAPÍTULO I. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Acceso abusivo a un sistema informático

> Artículo 269A: *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, enero de 2009).

El Artículo 269A reúne varias clasificaciones a partir de los elementos que contiene. Inicialmente puede precisarse que se trata de un tipo penal simple, al limitarse a una sola acción por parte del sujeto activo encaminada a acceder un sistema informático. Adicionalmente se trata de un tipo penal cerrado, pues no conlleva una situación en la cual el juez o intérprete deba hacer una prolongación a normas que permitan acabar con una aparente indeterminación del tipo.

De ello resulta un primer caso detonante que es clarificado en la investigación respecto a los tipos penales dispuestos por medio de la Ley 1273 de 2009, pues bien los tipos penales están en la mayoría de los casos debidamente normados, esto es, descritos y concretos en su propósito regulador, siendo su debilidad aquella que se extiende a los medios probatorios por medio de los cuales las autoridades competentes deben acreditar su comisión.

El acceso abusivo a un sistema informático no requiere de sujeto activo cualificado, menos aún de un sujeto especialísimo, limitándose su comisión a la acción adelantada por un sujeto activo común. Además, es un tipo penal monosubjetivo, por requerir de una acción delictiva individual. Este tipo penal describe una conducta de ejecución instantánea, pues basta un acto abusivo de acceso a la totalidad o la fracción de un sistema informático para que se configure la acción; lo que no excluye que la misma pueda prolongarse en el tiempo con posteriores accesos al sistema.

A partir de la descripción conductual, el acceso abusivo a un sistema informático se considera un tipo penal de mera conducta, pues la acción concreta en el acceso representa la vulneración del bien jurídicamente tutelado sin que se haga necesario acreditar un menoscabo material en el sujeto pasivo.

Lo referente al aspecto objetivo del tipo requiere recordar que algunos lo llaman objetivado, porque el legislador indica en la mayoría de los hechos los actos perceptibles, pero algunos necesitan ser objetivados por parte del intérprete para ver si hacen parte del tipo. El tipo es objetivo si tiene los elementos perceptibles, determinados y aceptables del tipo.

Para el caso de los tipos penales informático tomaremos los siguientes elementos objetivos: sujeto, tanto activo como pasivo; acción, resultado, lugar, objeto de la acción, bien jurídico protegido, y momento de la acción en caso de presentarse en alguno de los delitos dispuestos en la Ley 1273.

En el caso del acceso abusivo a un sistema informático requiere, como ya se mencionó, de un sujeto activo simple, pero para determinar el sujeto pasivo es necesario comprender qué es sistema informático, debido a que el acceso abusivo se realiza sobre este, siendo el factor que permite la configuración del atentado contra la información como bien jurídico protegido.

Un sistema informático está conformado por un conjunto de componentes que requieren de un funcionamiento articulado, pues requieren de si para poder operacionalizar el sistema y alcanzar la función. Los componentes de un sistema informático son el hardware, el *software,* el *firmware* y las personas usuarias del sistema. El hardware hace referencia a cualquier componente tecnológico de naturaleza física, el cual cumple una función con una computadora; mientras este tiene materialidad, y se reitera, existe físicamente en elementos internos como el disco duro y externos como el teclado, la impresora o los cables; el software hace alusión a un bien intangible. El software es un programa destinado a la realización de actividades específicas.

El software puede ser clasificado en aplicaciones informáticas, sistemas operativos y lenguajes de programación. El hardware, por su parte, está integrado por la Unidad Principal o CPU, las redes y los componentes periféricos. Finalmente, el personal hace referencia a usuarios, desarrolladores y técnicos de computación.

De esta manera, cuando el tipo penal se refiere al acceso abusivo a un sistema informático, delimita la conducta por medio de la cual un individuo accede a la totalidad o parte de un conjunto funcional de software, hardware y personal usuario por medio del cual se trabaja o manipula una información determinada. Vale exaltar cómo el tipo penal protege el acceso a cualquiera de los componentes por separado o a todos de forma integral, pues bien se encarga de describir el acceso “en todo o en parte a un sistema informático”, lo que traduce a cada uno de los elementos integradores del sistema como una fracción de información objeto de tutela penal, y que para la adecuación típica del delito basta probar la conducta de acceso abusivo a una de las partes antes referenciadas.

Gracias a ello es posible identificar los posibles sujetos pasivos de esta modalidad de conducta punible, pues ante la descripción de un sistema informático puede aseverarse que el sujeto pasivo será su titular o titulares, esto es, propietarios o usuarios directos del mismo, quienes como beneficiarios del soporte de información que directamente manejan a través de un sistema informático puntual, pueden verse como sujetos pasivos de una conducta de acceso abusivo.

Piénsese por ejemplo en el sistema informático de una entidad financiera o bancaria que cuenta con uno o varios sistemas informáticos para la prestación de sus servicios. En caso de ser objeto de una conducta de acceso abusivo a su sistema informático, será el sujeto pasivo de dicha acción, y sus clientes, los perjudicados o víctimas de la misma.

Frente a la acción, si bien se considera dentro de la teoría del delito como un componente adicional y previo a la tipicidad, esta se retoma como elemento objetivo del tipo, traducida en el verbo rector que describe el comportamiento o conducta del sujeto activo. Para el caso, su análisis se articula con el objeto de la acción, elemento por medio del cual se representa la cosa o persona donde recae el actuar o accionar del autor, la cosa sobre la cual recae la acción del sujeto activo.

En dicho contexto la acción a la que se refiere el tipo penal dispuesto en el Artículo 269A es a la de acceder, palabra que conforme a la Real Academia de la Lengua Española (2001) significa: “Consentir en lo que alguien solicita o quiere”, “Ceder en el propio parecer, conviniendo con un dictamen o una idea de otro, o asociándose a un acuerdo”, “Entrar en un lugar o pasar a él”, “Tener acceso a una situación, condición o grado superiores, llegar a alcanzarlos”.

A partir de los significados expuestos, es claro que la acción busca el ingreso o entrada de un individuo a un sistema de información, por lo cual este último se constituye en el objeto de la acción. Adicionalmente debe exaltarse cómo el primer alcance del significado del verbo rector, definido por la Real Academia, compagina convenientemente con la naturaleza y finalidad del tipo penal, pues bien se hace alusión a un acceso “abusivo”, esto es, a un acceso no consentido por el titular del sistema informático.

Aquí encuentra especial cabida el apartado por medio del cual la norma menciona: “O se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo” (Congreso de Colombia, enero de 2009), haciendo de esta figura de protección una medida que abarca los ejercicios rutinarios o esporádicos surgidos de las relaciones laborales o de confianza que implican el acceso de varias personas a un solo sistema informático.

Finalmente, desde el campo legal, frente al momento de la acción no se detalla algo en la disposición del Artículo 269A; el lugar exige una locación con uso de un sistema informático, algo que en la era moderna es frecuente en diversos escenarios de la vida humana; y relacionado con el bien jurídico protegido, la información es el derecho primordial.

Desde una mirada informática podremos identificar que el tipo penal se analiza desde sus componentes tecnológicos, previamente analizando el cambio que ha sufrido el tipo penal. Empezando en la referencia de “acceso abusivo a un sistema informático”, cabe aclarar que anteriormente según el Artículo 195 de la Ley 599 de 2000 se excluían los sistemas que no estuviesen protegidos por una medida de seguridad (sin que ella se especificara).

Ahora se contempla en la penalización todo ingreso a un sistema, esté protegido o no por una medida de seguridad, siendo toda conducta objeto de violación del bien jurídico protegido con el tipo penal, salvo que exista autorización del propietario del sistema, el cual, como dice la norma, tiene el *derecho a excluir,* es decir, impedir que ingresen o continúen estando en su sistema informático. En pocas palabras, el alcance del tipo penal se da desde el momento de ingresar a un sistema sin autorización, constituyendo una falta al bien jurídico tutelado. Vale la pena aclarar que esto se refiere al fragmento que dice: "De quien tenga el legítimo derecho a excluirlo" (Congreso de Colombia, enero de 2009), ya que el propietario en primera instancia sería quien posea ese derecho, aunque puede ser delegado a un administrador o un moderador del sistema. También es importante resaltar que cuando el legislador se refiere a "acceda en todo o parte a un sistema informático", se refiere a que las partes pueden comprender por "acceso" a discos duros, carpetas, particiones o computadores; cuando estamos frente a una red, siendo analizado el término desde un ámbito más general, vemos que se trata de "todo el sistema" que conforma el entorno informático, y como "parte" de aquella división de dicho sistema específico, técnicamente se puede probar si un intruso accedió a un nivel del sistema restringido, siendo esto considerado acceso en parte, o si el ingreso se presenta a un nivel superior del sistema, siendo esto considerado acceso total (Arcesio Bolaños & Martínez, 2004).

Los cambios más notorios en el artículo son entre otros: a) En la Ley 599 de 2000: se definía como un abuso a un sistema *protegido* y se mencionaba de una multa no especifica, ahora en la Ley 1273 del 2009 se incluyeron todos los sistemas, protegidos o no por una medida de seguridad y se modificó la sanción pasando a una pena de prisión de 48 a 96 meses y una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes; lo que hubiese sido un cambio radical en la sanción fue regulado y por unos meses vigente, la Ley 1288 del 2009 se modificó para volver a excluir a los sistemas sin protección especificando la pena de prisión de cinco a ocho años (esta ley se ha "Declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia C-913 de 2010").

Obstaculización ilegítima de sistema informático o red de telecomunicación

> Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor (Congreso de Colombia, enero de 2009).

Al igual que el tipo penal de acceso abusivo a sistema informático, el delito dispuesto en el Artículo 269B es un tipo penal básico al describir de manera sencilla e independiente una conducta; es un tipo penal de conducta instantánea al reservarse la comisión del acto a la ejecución del acto obstaculizador, pero es un tipo penal compuesto al señalar adicional a la acción de obstaculizar, también la conducta de impedir el funcionamiento del sistema informático o de una red de comunicaciones.

Es un tipo penal cerrado y de sujeto activo común al no requerir especiales calidades de quien realiza la acción, y al igual que el tipo contenido en el Artículo 269A, se trata de un delito que para su realización no exige la presencia de varios sujetos, por lo que es monosubjetivo; y, como se verá más adelante, afecta no solo a la información como bien jurídico tutelado sino también el derecho a la comunicación, por lo que es un tipo penal pluriofensivo.

Respecto a los elementos objetivos del tipo de obstaculización ilegítima de sistema informático o red de telecomunicación son varios los aspectos a destacar. Este tipo penal es una figura complementaria desde la función sistematizadora del tipo penal, en la medida que el legislador consagra varias conductas alrededor de una unidad, y cada unidad protege un bien jurídicamente tutelado, en este caso puede proponerse como unidad de protección el sistema informático, y con él, la protección de la información como bien jurídico.

Mientras que el artículo anterior se dirige al acceso abusivo que se haga sobre un sistema informático, el presente delito abarca la conducta de aquel sujeto que sin contar con autorización busque obstaculizar el funcionamiento o normal acceso al sistema informático, la información contenida en él, o a una red de telecomunicaciones.

Esto quiere decir que mientras el acceso abusivo no cuenta con el consentimiento voluntario y libre del titular del sistema informático para permitir el ingreso a dicho sistema, el presente tipo penal contempla la acción del sujeto activo que sin hacer parte de la esfera de individuos facultados para tener acceso y hacer uso de cualquiera de los soportes protegidos en la norma, busca generar situaciones que impiden el cumplimiento de la finalidad para la cual está destinado el sistema informático, los datos que allí reposan, o una red de telecomunicaciones.

Se estima adecuado afirmar que el sujeto activo no se encuentra entre la esfera de los individuos facultados para ejercer labores sobre cualquiera de los tres soportes mencionados en el tipo, debido a que la misma disposición es tajante en encabezar la situación conductual tipificada con “el que, sin estar facultado para ello”, de donde se desprende una prohibición previa que puede ser jurídica o contractual para una persona específica, de actuar frente a los componentes informáticos protegidos.

Es así como el sujeto activo de la acción es un individuo común que tiene conocimiento del sistema informático, la información contenida en él, o de una red de telecomunicaciones; y el sujeto pasivo, al igual que en el acceso abusivo a sistema informático será su titular o titulares, esto es, propietarios o usuarios directos del mismo, quienes como beneficiarios del soporte de información que manejan a través de un sistema informático puntual, pueden verse como sujetos pasivos de una conducta de acceso abusivo.

No obstante, es necesario clarificar qué es una red de telecomunicaciones, pues para poder tipificar la conducta de obstaculizar o impedir es necesario comprender los soportes sobre los cuales se materializa. Una red de telecomunicaciones es una red de enlaces y nodos ordenados para permitir

la comunicación a distancia, donde los mensajes pueden pasarse de una parte a otra de la red sobre múltiples enlaces y a través de varios nodos. Un nodo es un punto de encuentro o de unión, en este caso una computadora constituye un nodo en una red de telecomunicaciones.

Como elementos objetivos del tipo penal en estudio, la acción se identifica en dos verbos rectores claramente determinados. De un lado obstaculizar acarrea al sujeto activo "impedir o dificultar la consecución de un propósito" (Real Academia Española, 2001), mientras que impedir alude a "imposibilitar la ejecución de algo" (Real Academia Española, 2001).

Desde las definiciones expuestas se estima que mientras la acción de obstaculizar describe la conducta por medio de la cual el sujeto activo despliega un comportamiento o serie de comportamientos dirigidos a generar eventualidades o circunstancias que impidan el adecuado funcionamiento de un sistema informático, del uso de la información contenido en él, o de una red de telecomunicaciones, impedir se refiere a perseguir el no funcionamiento de uno de los soportes en su totalidad.

El tipo penal no enfatiza en un momento específico de la comisión de la acción; el objeto sobre el cual recae se representa en el objeto físico del sistema informático o de la red de telecomunicaciones, o bien en el soporte inmaterial u objeto intangible representado en la información o en el software.

Desde una mirada informática el análisis sobre este tipo penal, Artículo 269B denominado Obstaculización ilegítima de sistema informático o red de telecomunicación, se establece que el individuo objeto de judicialización bajo esta conducta será únicamente el que no se encuentre facultado para ello, esto lo denota la expresión "sin estar facultado...".[3] En cuanto a impedir u obstaculizar se debe diferenciar el uno del otro. Cuando se impide el funcionamiento o el acceso normal a un sistema informático, los datos contenidos allí o una red de telecomunicaciones, se puede hablar de no permitir que la información fluya (es decir, que la información no pueda ser consultada, transferida, almacenada, enviada), lo cual es posible técnicamente con bloqueos de puertos, modificación de permisos, eliminación de archivos, y más. Con respecto a obstaculizar el funcionamiento o el acceso normal a un sistema informático, los datos contenidos allí o a una red de telecomunicaciones, se puede hablar de que se ralentice o impida el normal funcionamiento del flujo de información (es decir, que la información no pueda ser consultada, transferida, almacenada, enviada).

Interceptación de datos informáticos

> Artículo 269C: *Interceptación de datos informáticos.* El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses (Congreso de Colombia, enero de 2009).

[3] Según el diccionario de la Real Academia Española, el termino facultad se refiere a Poder, derecho para hacer algo.

La interceptación de datos informáticos es un delito penal básico o fundamental, de conducta instantánea, sin que pueda ser confundida como permanente, en la medida que la conducta individualizada puede permanecer en el tiempo pero como un acto individualizado que se reitera paulatinamente frente a un sistema informático o las emisiones electromagnéticas, pero basta con una sola interceptación para conducir a su configuración típica.

Es un tipo penal simple por acarrear solo una conducta como acción tipificada en la norma, y de aparente sujeto activo simple en la medida que si bien la disposición comienza con "El que" sin que denote calidad especial alguna del sujeto que incurre en la conducta tipificada, la misma norma se encarga de condicionar la calidad especial del sujeto activo pensado para el tipo penal.

Lo anterior se propone en la medida en que la interceptación a la que se hace referencia la presente norma interpone como imperativo hipotético la ausencia de orden judicial previa, lo que conduce a que el sujeto activo que incurre en el delito debe ejercer funciones concretas que no se generalizan en un sujeto común, debido a que su ejercicio requiere de una orden judicial previa como instrumento de garantía de la actividad desplegada por el agente.

Por lo tanto, el artículo conduce a que el sujeto activo de la interceptación debe ser un funcionario de la policía judicial encargado de labores de investigación judicial en un proceso penal, que para su legal ejercicio requiere de orden judicial previo para poder realizar las interceptaciones a los medios señalados, circunstancia que requiere ahondar en las normas al respecto.

No incurre así cualquier individuo en la comisión de la conducta descrita en la norma objeto de estudio, pues bien delimita y señala la ley quienes despliegan las labores de investigación judicial en Colombia, y con ello, están en la posibilidad de realizar interceptación de datos informáticos:

> LEY 906 DE 2004, ARTÍCULO 114. ATRIBUCIONES. La Fiscalía General de la Nación, para el cumplimiento de sus funciones constitucionales y legales, tiene las siguientes atribuciones:
>
> 1. Investigar y acusar a los presuntos responsables de haber cometido un delito.
>
> 2. Aplicar el principio de oportunidad en los términos y condiciones definidos por este código.
>
> 3. Ordenar registros, allanamientos, incautaciones e interceptaciones de comunicaciones, y poner a disposición del juez de control de garantías los elementos recogidos, para su control de legalidad dentro de las treinta y seis (36) horas siguientes.
>
> 4. Asegurar los elementos materiales probatorios y evidencia física, garantizando su cadena de custodia mientras se ejerce su contradicción.
>
> 5. Dirigir y coordinar las funciones de policía judicial que en forma permanente ejerce su cuerpo técnico de investigación, la Policía Nacional y los demás organismos que señale la ley. (Congreso de Colombia, agosto de 2004).

Con ello, la regulación que hace el Artículo 269C abre un campo trascendental que toca directamente con la actividad de investigación judicial, y en ella, con la recopilación del material probatorio de conductas investigadas por el ente constitucionalmente encargado.

Tan delicada actividad viene ampliamente desarrollada en la legislación nacional, puntualmente en la ya citada Ley 906 de 2004, especificando incluso que es deber de la Fiscalía General de la Nación "informar a la autoridad competente de cualquier irregularidad que observe en el transcurso de la actuación de los funcionarios que ejercen atribuciones de policía judicial" (Artículo 142, Ley 906 de 2004), lo que desde ahora implica asegurar que el sujeto activo de la acción citada en la interceptación de datos informáticos no es ni puede ser un sujeto común, debe ser un sujeto altamente cualificado que acredita los conocimientos suficientes para poder desplegar la acción en comento.

A partir del Artículo 200 de la Ley 906 de 2004 se describe cuáles son los órganos de indagación e investigación penal en Colombia, por lo tanto, los facultados para llegar a proceder con una interceptación de datos informáticos. Cita el Artículo 200:

> Corresponde a la Fiscalía General de la Nación realizar la indagación e investigación de los hechos que revistan características de un delito que lleguen a su conocimiento por medio de denuncia, querella, petición especial o por cualquier otro medio idóneo.
>
> En desarrollo de la función prevista en el inciso anterior a la Fiscalía General de la Nación, por conducto del fiscal director de la investigación, le corresponde la dirección, coordinación, control jurídico y verificación técnico-científica de las actividades que desarrolle la policía judicial, en los términos previstos en este código.
>
> Por policía judicial se entiende la función que cumplen las entidades del Estado para apoyar la investigación penal y, en ejercicio de las mismas, dependen funcionalmente del Fiscal General de la Nación y sus delegados (Congreso de Colombia, 2004).

Compaginado con el Numeral 3 del Artículo 114 de la citada ley, se delimita en la Fiscalía General de la Nación la tarea de indagar e investigar las conductas delictivas, clarificando que para ello se apoya en entidades del Estado que ella misma supervisa, las cuales desarrollan actividades de policía judicial, esto es, labores de investigación penal donde se incluyen las interceptaciones de datos informáticos como un medio para la obtención de información de naturaleza probatoria.

Señala la misma ley en su Artículo 201, que ejercen permanentemente las funciones de policía judicial los servidores investidos de esa función, pertenecientes al Cuerpo Técnico de Investigación de la Fiscalía General de la Nación, a la Policía Nacional y al Departamento Administrativo de Seguridad, por intermedio de sus dependencias especializadas.

También desempeñan funciones permanentes de policía judicial de manera especial dentro de su ámbito de competencia las autoridades mencionadas en el Artículo 202: Procuraduría General

de la Nación, la Contraloría General de la República, las autoridades de tránsito, las entidades públicas que ejerzan funciones de vigilancia y control, los directores nacional y regional del Inpec, los directores de los establecimientos de reclusión y el personal de custodia y vigilancia, conforme con lo señalado en el Código Penitenciario y Carcelario, los alcaldes, y los inspectores de policía.

Finalmente, el Artículo 203 señala que ejercen funciones de policía judicial, de manera transitoria, los entes públicos que, por resolución del Fiscal General de la Nación, hayan sido autorizados para ello. Estos deberán actuar conforme con las autorizaciones otorgadas y en los asuntos que hayan sido señalados en la respectiva resolución.

En ese sentido, la ley de procedimiento penal se encarga de delimitar la especial condición que requiere un sujeto activo que puede incurrir en la interceptación de datos informáticos, toda vez que la condición fáctica que exige la descripción de la conducta típica es la carencia de la orden judicial previa para adelantar la debida interceptación de datos informáticos.

Ante la implícita y necesaria exigencia de la calidad especial conferida por la ley para la adecuación típica de la interceptación de datos informáticos, debe indicarse en este punto que el objeto de la acción se mantiene en el sistema informático como soporte físico, o en las emisiones electromagnéticas que provengan de él, siendo el bien jurídico tutelado la información que reposa en aquel.

Debemos comprender entonces que la calidad del sujeto activo de la acción de interceptación conduce al escenario de la actividad judicial y de las labores de policía judicial ya descritas en los artículos anteriores. A este campo se llega por motivo de la exigencia de la orden judicial previa, requisito específico que determina la tipificación de la conducta.

El Código de Procedimiento Penal dispuso en sus artículos 213 a 245 las actuaciones que no requieren autorización judicial previa para su realización por parte de las entidades que cumplen las funciones de policía judicial. Entre esos artículos se identifican las disposiciones de los artículos 222 y 223, de donde resulta la primera restricción en materia de información a partir de datos informáticos; dispone el Artículo 222:

> ALCANCE DE LA ORDEN DE REGISTRO Y ALLANAMIENTO. La orden expedida por el fiscal deberá determinar con precisión los lugares que se van a registrar. Si se trata de edificaciones, naves o aeronaves que dispongan de varias habitaciones o compartimentos, se indicará expresamente cuáles se encuentran comprendidos en la diligencia.
>
> De no ser posible la descripción exacta del lugar o lugares por registrar, el fiscal deberá indicar en la orden los argumentos para que, a pesar de ello, deba procederse al operativo. En ninguna circunstancia podrá autorizarse por la Fiscalía General de la Nación el diligenciamiento de órdenes de registro y allanamiento indiscriminados, o en donde de manera global se señale el bien por registrar (Congreso de Colombia, agosto de 2004).

Seguidamente la ley trae como objetos amparados en la restricción de registro por parte de las autoridades que adelantan la investigación, los siguientes:

No serán susceptibles de registro los siguientes objetos:

1. Las comunicaciones escritas entre el indiciado, imputado o acusado con sus abogados.

2. Las comunicaciones escritas entre el indiciado, imputado o acusado con las personas que por razón legal están excluidas del deber de testificar.

3. Los archivos de las personas indicadas en los numerales precedentes que contengan información confidencial relativa al indiciado, imputado o acusado. Este apartado cobija también los documentos digitales, vídeos, grabaciones, ilustraciones y cualquier otra imagen que sea relevante a los fines de la restricción.

   PARÁGRAFO. Estas restricciones no son aplicables cuando el privilegio desaparece, ya sea por su renuncia o por tratarse de personas vinculadas como auxiliadores, partícipes o coautoras del delito investigado o de uno conexo o que se encuentre en curso, o se trate de situaciones que constituyan una obstrucción a la justicia (Congreso de Colombia, agosto de 2004).

A partir de las disposiciones citadas, la Fiscalía encuentra como limitante en la actividad investigativa la posibilidad de acceder a los datos de información contenidos en sistemas o soportes informáticos, restricción que inicialmente impide que en un registro o allanamiento ordenado o autorizado por la Fiscalía se tenga acceso a los datos informáticos, situación que se rompe en las circunstancias descritas en el parágrafo del Artículo 223 de la Ley 906 de 2004.

Reiteraremos al respecto, que la acción de interceptación de datos informáticos tipificada en el Artículo 269C quedaría restringida en las diligencias de registro y allanamiento de las autoridades que cumplen con funciones de policía judicial, garantía que no es absoluta por los casos de excepción legal.

No obstante, debemos recordar que el Artículo 269C dispone la ausencia de orden judicial previa para la interceptación, y que todas las disposiciones aludidas hasta el momento se amparan en el título de diligencias que no requieren autorización previa por parte de un juez. La Ley 906 detalla entre las actividades y elementos que pueden ser objeto de investigación sin autorización previa de un juez, aquella comprendida en el Artículo 235 modificada por el Artículo 52 de la Ley 1453 de 2011(Congreso de Colombia) que dispone:

> *Interceptación de comunicaciones.* El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la

> operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación.
>
> En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.
>
> Por ningún motivo se podrán interceptar las comunicaciones del defensor.
>
> La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron.
>
> La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.

Es esta disposición la que acarrea el pronunciamiento de la Corte Constitucional, y la consiguiente exigencia de orden judicial para adelantar la interceptación de datos informáticos como medio de comunicación. Al respecto señaló la Corporación en sentencia C-334 de 2010:

> Con la modificación introducida al Artículo 250 constitucional por el Acto Legislativo No. 3 de 2002, se contemplan, en términos generales, tres tipos de intervención por parte de la Fiscalía. Una primera, la habilitación legal para "realizar excepcionalmente capturas", la cual se somete, al tenor del numeral 1º, a un control de legalidad posterior dentro de las 36 horas siguientes a la práctica de la medida; otra, en la cual se contemplan los "registros, allanamientos, incautaciones e interceptaciones de comunicaciones", que también, conforme al inciso 2º, son controlados con posterioridad a su práctica y dentro de las 36 horas siguientes; y finalmente, las demás "medidas adicionales que impliquen afectación de derechos fundamentales", previstas en el numeral 3º, las que sí requieren "autorización por parte del juez que ejerza las funciones de control de garantías para poder proceder a ello", con lo que se quiere significar que, salvo la práctica de exámenes sobre la víctima de delitos o agresiones sexuales, las intervenciones de la Fiscalía que requieren autorización judicial, operan sobre la persona contra quien cursa la investigación.

En la citada sentencia de la Corte Constitucional, la interceptación de comunicaciones requiere de control judicial "posterior", diferente a la mencionada orden judicial "previa" dispuesta en la norma del tipo penal de interceptación de datos informáticos. Vale mencionar que al respecto también diferenció la Corte (2010) en esa providencia la naturaleza de las dos modalidades de control:

> Respecto de la oportunidad del control judicial sobre las actuaciones de la Fiscalía y de la policía judicial existen diferencias entre el que opera de modo previo y el que ocurre con posterioridad. En el caso del control previo, procede una actuación judicial que pondera entre los intereses de la investigación, las razones aducidas por la Fiscalía, el delito investigado y las condiciones del sujeto sobre quién o sobre cuyos intereses se practicaría la actuación, a fin de evitar una restricción excesiva, innecesaria o afrentosa, que en poco o nada asegure verdad al proceso y al contrario, afecte desproporcionadamente ámbitos de la intimidad y privacidad de la persona implicada. Lo

que hace el juez es proteger los derechos del sujeto investigado, impedir que las prerrogativas del Estado asignadas a la Fiscalía y a su aparato técnico, se usen sin finalidad concreta, sin justificación, inútilmente y de modo desproporcionado, desconociendo el carácter iusfundamental y especialmente protegido de los bienes jurídicos reconocidos en los derechos individuales sobre los que la actuación investigativa opera. En tanto que en el control judicial posterior, que es excepcional y procedente para las medidas que de modo taxativo señaló la Constitución en el numeral 2º del Artículo 250, se atienden no sólo aspectos formales sino materiales y por tanto relacionados con los derechos y garantías fundamentales en juego, y se produce sobre una diligencia que ya se ha ejecutado y en la que ya se han afectado derechos fundamentales. En tal sentido, la actuación judicial no previene la injerencia ilegítima sobre éstos, como sucede en el control previo, y en caso de encontrar que efectivamente la Fiscalía y/o la policía judicial han actuado con desconocimiento de las reglas y principios normativos que regulan las actuaciones correspondientes, la garantía judicial sirve es para reparar los derechos limitados en exceso pero en términos procesales, es decir, excluyendo del expediente la evidencia recaudada con violación de los protocolos, garantías y procedimientos.

La condición de legalidad de la disposición del Artículo 269C, de la Ley 1273 de 2009, es clara al referirse a una orden judicial previa, lo que requiere de la mención aclaratoria que se identifica en la sentencia C-131 de 2009. En el apartado relacionado con el tema comienza la Corte diferenciando las modalidades de vulneración del derecho a la intimidad:

Así, como fue señalado en la sentencia T-696 de diciembre 5 de 1996, M. P. Fabio Morón Díaz, el derecho a la intimidad puede llegar a ser vulnerado de tres formas:

'La primera de ellas es la intrusión o intromisión irracional en la órbita que cada persona se ha reservado; la segunda, consiste en la divulgación de los hechos privados; y la tercera, finalmente, en la presentación tergiversada o mentirosa de circunstancias personales, aspectos los dos últimos que rayan con los derechos a la honra y al buen nombre. La intromisión en la intimidad de la persona, sucede con el simple hecho de ingresar en el campo que ella se ha reservado. Es un aspecto material, físico, objetivo, independientemente de que lo encontrado en dicho interior sea publicado o de los efectos que tal intrusión acarree. Cabe en este análisis la forma en que el agente violador se introduce en la intimidad del titular del derecho y no tanto el éxito obtenido en la operación o el producto de la misma, que se encuentran en el terreno de la segunda forma de vulneración antes señalada'.

Aunado a lo anterior, en la sentencia C-626 de noviembre 21 de 1996, M. P. José Gregorio Hernández Galindo, **se puntualizó que las intromisiones en las comunicaciones de los particulares, sólo pueden adelantarse previa orden de la autoridad judicial, dentro de un proceso, con el cumplimiento de las formalidades establecidas en la ley.** Al respecto en el referido fallo se explicó:

'La Corte Constitucional, en guarda de la cabal interpretación y aplicación de las normas constitucionales enunciadas y de los tratados internacionales sobre derechos humanos, que han sido estrictos y celosos en la materia (Cfr. Convención Americana sobre Derechos Humanos, 'Pacto de

> *San José de Costa Rica', aprobada mediante Ley 16 de 1992, Artículo 11; Pacto Internacional de Derechos Civiles y Políticos, aprobado por Ley 78 de 1968, Artículo 17), debe declarar sin ambages que ninguna persona pública ni privada, por plausible o encomiable que sea el objetivo perseguido, está autorizada para interceptar, escuchar, grabar, difundir ni transcribir las comunicaciones privadas, esto es, las que tienen lugar entre las personas mediante conversación directa, o por la transmisión o registro de mensajes, merced a la utilización de medios técnicos o electrónicos aptos para ello, tales como teléfonos convencionales o celulares, radioteléfonos, citófonos, buscapersonas, equipos de radiocomunicaciones, entre otros,* ***A MENOS QUE EXISTA PREVIA Y ESPECIFICA ORDEN JUDICIAL Y QUE ELLA SE HAYA IMPARTIDO EN EL CURSO DE PROCESOS, EN LOS CASOS Y CON LAS FORMALIDADES QUE ESTABLEZCA LA LEY,*** *según los perentorios términos del Artículo 15 de la Constitución Política' (negrilla y mayúsculas del original).*

> 6.3. En la sentencia T-696 de 1996 previamente citada, frente a las excepciones a la inviolabilidad de las comunicaciones que establece el Artículo 15 Superior, y particularmente en el tema de la correspondencia pero extendiéndola a las comunicaciones privadas, la Corte Constitucional especificó que **interceptar** *'consiste en apoderarse de ella antes de que llegue a la persona a quien se destina, detenerla en su camino, interrumpirla u obstruirla, en fin, impedirle que llegue a donde fue enviada'.* Y, **registrar** *'implica examinarla con cierto cuidado para enterarse de cuanto contiene'* (negrilla del original).

Queda así, por vía de interpretación jurisprudencial, despejado el alcance de la acción a la que alude la interceptación tipificada en el Artículo 269C, y complementa la interpretación del tribunal y los alcances también dispuestos por la norma en relación a los tipos de violación del bien jurídicamente tutelado, en la medida que el tipo penal se refiere al origen, destino o interior de un medio informático, lo que se traduce en la movilidad posible de los datos informáticos entre los usuarios de un sistema informático, asunto al cual se refirió la Corte (2009) en los siguientes términos:

> En esa oportunidad también se indicó que ese tipo de violaciones *'pueden suceder bien por examinarla persona que no sea el destinatario o alguien a quien éste la muestre, en cualquiera de los momentos anotados, es decir, su elaboración,* ***curso del traslado o después de recibida;*** *bien con violencia o habilidad en la extracción y examen de su contenido; bien con destrucción del objeto portador de la información, quitándole alguna parte o tornándolo ininteligible'.*

Seguidamente, en la misma sentencia, la Corte Constitucional (2009) retoma el mandato legal del control judicial posterior que debe cumplir la Fiscalía en los casos de haber ordenado interceptación de comunicaciones en la etapa de investigación de un proceso penal, reiterando:

> Sin embargo, el legislador en materia penal al regular el tema ha señalado que el Fiscal puede ordenar, fundadamente y por escrito, la **interceptación** "mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético", para buscar elementos materiales probatorios y evidencia física, para la búsqueda

y ubicación de imputados o indiciados, **debiendo comparecer ante el Juez de Garantías dentro de las 24 horas siguientes al diligenciamiento de la orden, para que se realice la revisión de la legalidad de lo actuado, así como dentro de igual término una vez cumplida la misión, para que se adelante el mismo control** (Artículos 235 a 237 L. 906 de 2004 conc. L. 1142 de 2007) (negrilla del original).

Posteriormente, la concurrencia de la orden judicial previa para la realización de investigaciones por parte de las entidades encargadas de desplegar la función de policía judicial, y el control judicial posterior de la diligencia de interceptación ordenada por la Fiscalía, son abordadas y decididas por la Corte Constitucional (2009) en los siguientes términos:

6.4. Acorde con esos parámetros, procede la Corte a efectuar un estudio conjunto de sus implicaciones frente a los aspectos demandados de los artículos 15 y 16 de la Ley 1142 de 2007, sujetos al presente análisis (…)
El Artículo 14 de dicha Ley reitera el principio de reserva judicial para la afectación de garantías fundamentales dentro del proceso penal. Se consagra que **no podrán efectuarse registros, allanamientos ni incautaciones en domicilio, residencia o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo a las formalidades y motivos previamente definidos.**

Esta corporación, al interpretar sistemáticamente el Artículo 250 superior, concluyó que si bien por regla general las medidas que afectan derechos fundamentales requieren autorización previa del Juez de Control de Garantías, existe una excepción constitucionalmente válida, que debe confrontarse frente a la expresión “a juicio del fiscal”, objeto del presente análisis.

En la sentencia C-336 de mayo 9 de 2007, M. P. Jaime Córdoba Triviño, se estudió la constitucionalidad de algunos apartes de los artículos 14 (intimidad), 244 (búsqueda selectiva de bases de datos) y 246 (regla general aplicable a las actuaciones que requieren autorización judicial previa para su realización) de la Ley 906 de 2004. En ese pronunciamiento se indicó que el numeral 2° del Artículo 250 de la Constitución “adscribe directamente a la Fiscalía la potestad de ‘adelantar registros, allanamientos, incautaciones e interceptación de comunicaciones’, actuaciones que están sometidas al control posterior del Juez de Control de Garantías, a más tardar dentro de las 36 horas siguientes, a efecto de que se realice un control amplio e integral de esas diligencias”.

Acorde con esos planteamientos, para esta corporación esa regulación resulta distinta a la contenida en el subsiguiente numeral 3° del referido Artículo 250, como quiera que en él se establece que a la Fiscalía General de la Nación le corresponde, en ejercicio de sus funciones, asegurar los elementos materiales probatorios y garantizar la cadena de custodia mientras se ejerce su contradicción, al tiempo que **cuando sean necesarias medidas adicionales que impliquen afectación de derechos fundamentales, se requiere la autorización previa por el Juez de Control de Garantías para proceder a tal fin.**

Y, más adelante, además de concretar la importancia que tiene el funcionario encargado de velar por las garantías fundamentales dentro del proceso penal, tratándose de registros, allanamientos, incautaciones e interceptaciones de comunicaciones, se puntualizó que la

Constitución faculta a la Fiscalía para hacerlo directamente, sometiendo la orden y lo recabado a un control integral posterior, dejando los demás eventos sujetos al condicionamiento de una autorización previa del Juez (negrilla y subrayado del original).

Al respecto se expresó:

5. De tales previsiones constitucionales se concluye que fue voluntad del Constituyente: (i) radicar en cabeza de los jueces de control de garantías la adopción de las medidas necesarias para asegurar la comparecencia de los imputados al proceso penal; sólo excepcionalmente y previa regulación legal que incluya los límite (sic) y eventos en que procede, la Fiscalía podrá efectuar capturas; ***(ii) facultar directamente a la Fiscalía para adelantar registros, allanamientos, incautaciones e interceptación de comunicaciones, sometidos al control posterior del Juez de Control de Garantías;*** *(iii) disponer que en todos los demás eventos en que, para el aseguramiento de los elementos materiales probatorios, se requiera medidas adicionales que impliquen afectación de derechos fundamentales deberá mediar autorización (es decir, control previo) por parte del Juez de Control de Garantías (negrilla y cursiva del original).*

Con esos fundamentos se indicó que el control previo de las medidas que afecten derechos fundamentales se flexibilizada en el numeral 2° del Artículo 250 de la Carta Política, al permitir taxativamente algunas actuaciones que no requieren de la precedente autorización del Juez, debido al efecto que persiguen, pero cuyo control posterior es integral, esto es, abarca la orden proferida por el Fiscal y los elementos obtenidos en su ejecución. Ese análisis de avanzada llevó a concluir lo siguiente:

14. La relativa flexibilización que el numeral 2° del Artículo 250 de la Constitución introduce respecto de los registros (que pueden recaer sobre archivos digitales o documentos computarizados), allanamientos, incautaciones e interceptación de comunicaciones, en el sentido de permitir un control posterior del Juez de Control de Garantías, puede explicarse en la necesidad y oportunidad del recaudo de la información, en cuanto se trata de diligencias que generalmente están referidas a realidades fácticas que pueden estar propensas a cambios repentinos, o que podrían eventualmente ser alteradas en desmedro del interés estatal de proteger la investigación. No ocurre lo mismo con la información que reposa en las bases de datos, a que se refieren los preceptos impugnados, la cual tiene vocación de permanencia en cuanto ha sido recopilada, almacenada y organizada, de manera legítima y autorizada, para preservar una memoria con propósitos de uso muy diversos pero siempre legítimos y acordes a los principios que rigen la captación, administración y divulgación de esta información. Esa cualidad de permanencia actualizad del objeto sobre el cual recae la búsqueda selectiva de información, explica el que no se plantee la necesidad de hacerle extensiva la regla de flexibilización excepcional del control posterior *(negrilla y cursiva del original).*

15. Las intervenciones que se producen mediante los registros (que como se precisó pueden recaer sobre documentos digitales o archivos computarizados) y allanamientos con fines de investigación

penal entran en tensión con el derecho a la intimidad, en tanto que la (sic) intervenciones que se realizan sobre los datos personales pueden comprometer el derecho al habeas data y el derecho a la intimidad, que como se explicará a continuación, no obstante derivar uno y otro su validez del Artículo 15 de la Carta, conservan su propia autonomía.

16. De otra parte, la enunciación que contempla el numeral 2° del Artículo 250 de la Constitución es de naturaleza taxativa y de interpretación restrictiva, en cuanto contempla las excepciones a la regla general derivada de la misma disposición (numeral 3º), sobre la necesidad de autorización previa del Juez de Control de Garantías para la práctica de diligencias investigativas que impliquen afectación, mengua o limitación de derechos fundamentales (Corte Constitucional, 2009).

Así, queda claro que la Corte Constitucional fortaleció las medidas de protección y garantía de los derechos fundamentales que se relacionan con la actividad de investigación penal que adelantan las autoridades de la policía judicial en Colombia. Sin excluir la regla general del control judicial posterior que exige la Ley 906 de 2004, estimó la Corte que la interceptación de comunicaciones, especificando textualmente la inclusión de los archivos digitales y documentos computarizados, requieren de la previa autorización del juez para adelantar la diligencia, todo en virtud de la protección del derecho fundamental de la intimidad, haciéndolo, para el caso de las interceptaciones, regla general de procedimiento.

La Corte Constitucional en la sentencia C-336 de 2007 puntualizó que **la exigencia de ese control previo, como regla general, deviene del fortalecimiento que se da en el sistema acusatorio de investigación penal al principio de reserva judicial, cuando de la afectación de derechos fundamentales se trate** (reiterando lo expuesto en la C-1092 de 2003, ya referida, donde se declaró inexequible la expresión *'al solo efecto de determinar su validez',* del Numeral 2° del Artículo 2° del Acto Legislativo 03 de 2002 que modificó el Artículo 250 superior) (negrilla del texto original).

Igualmente, acudiendo a la precitada sentencia C-979 de 2005, también referida, se agregó que la creación de ese funcionario judicial encargado del control de garantías responde al *'principio de necesidad efectiva de protección judicial'*, como quiera que **ciertas actuaciones procesales adoptadas dentro de la investigación penal entran en tensión con el principio de inviolabilidad de los derechos fundamentales,** *'los cuales únicamente pueden ser afectados en sede jurisdiccional'.* **En otras palabras, los derechos del investigado y de la víctima** *'fungen así como límites de la investigación'* (negrilla del original) (Corte Constitucional, 2009).

No resulta así desmedida la interpretación y nueva orientación que proporciona la Corte Constitucional frente a la protección de los derechos fundamentales inmersos en esa etapa procesal, en la medida que a partir de las amplias prerrogativas con las que cuenta el Estado para adelantar las labores de indagación e investigación penal, debe el juez constitucional velar por la absoluta protección de los derechos inmersos en las situaciones donde el Estado despliega su poder investigativo.

> De esa forma, la interceptación de datos informáticos queda amparada por una doble garantía; inicialmente requiere de orden judicial previa en virtud a la naturaleza del derecho fundamental de intimidad que es puesto bajo observación de las autoridades de policía judicial; y al control posterior que por mandato de ley debe cumplir el funcionario una vez realice la diligencia de interceptación. Los sustentos jurisprudenciales del alto Tribunal se remiten incluso al bloque de constitucionalidad:
>
> Desde el Derecho Internacional de los Derechos Humanos, es claro que los Estados pueden adelantar actuaciones que supongan afectación o injerencia en ámbitos de libertad o de derecho protegidos. Sin embargo, tales actuaciones aunque no siempre deben estar respaldadas por orden de autoridad judicial, en todo caso sí deben ser reguladas por la ley, de modo tal que sólo puedan desplegarse cuando sea necesario, no implique una afectación ilegítima de otros derechos, se corresponda con las formas y exigencias propias de una sociedad democrática cuyo animus vivendi se encuentra en la preservación de los derechos de los individuos y grupos que la integran (…) Los objetivos por los cuales procede el control judicial, no son otros que i) asegurar la legalidad formal y sustancial de la actuación, ii) proteger los derechos fundamentales de quienes, por activa o por pasiva, son afectos al proceso o a la investigación preliminar; iii) verificar la corrección del operador jurídico de la Fiscalía, en las medidas ordenadas y adoptadas para la conservación de la prueba, la persecución del delito y la procura de reparar a las víctimas y de restituir la confianza de la comunidad. Estos elementos deben ser tenidos en cuenta por el juez de control de garantías bien cuando se ha allanado, registrado, incautado y cuando se han interceptado comunicaciones, como cuando estudia si debe o no autorizar toda otra afectación de derechos fundamentales que pueda implicar el desarrollo de la investigación del delito (Corte Constitucional, 2010).

A partir de la misma redacción del tipo penal en estudio, y de los amplios pronunciamientos jurisprudenciales generados en torno al tema, se estima necesario hacer una reflexión crítica y constructiva del tipo penal. Bien exige el Artículo 269C para la configuración de la conducta punible la ausencia de orden judicial previa, condición necesaria para la interceptación de datos informáticos contrario a lo perseguido por el ordenamiento jurídico, pero como se vio, la misma actuación también queda sujeta a un control judicial posterior que no figura como elemento del tipo penal.

La exigencia de los parámetros de la adecuación típica de una conducta queda claramente sometida a un vacío no previsto por el legislador al momento de crear el delito de la interceptación de datos informáticos, en la medida que bien puede atribuirse la comisión de la conducta típica al funcionario que intercepte datos informáticos sin orden judicial previa, más no al funcionario que cumpliendo dicho requisito de procedibilidad no agote el control judicial posterior.

La descripción típica de la conducta omitió incluir la ausencia del deber legal de someter la obtención de la prueba derivada de la interceptación de datos informáticos al control judicial posterior, quedando a nuestro criterio esta situación sujeta a una posible nulidad del acto procesal, por medio del cual se obtuvo la prueba, haciendo que se excluya esa información del acervo probatorio, pero dejándola librada a la atipicidad de la conducta del funcionario con labores de policía judicial, que habiendo actuado sobre la orden judicial previa no somete la diligencia a control posterior.

Finalmente, debe señalarse aquí que la actuación consistente en la búsqueda selectiva en bases de datos dispuesta en el Artículo 244 de la Ley 906 de 2004, por medio del cual: "La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público" (Congreso de Colombia), quedó sometido a la misma exigencia de requerir orden judicial previa, requisito fijado por la Corte Constitucional en sentencia C-336 de 2007: "Se requiere de orden judicial previa cuando se trata de datos personales organizados con fines legales y recogidos por instituciones o entidades públicas o privadas debidamente autorizadas para ello".

Adicionalmente, el mismo Tribunal dispuso mediante sentencia C-025 de 2009:

> El Artículo 237 precisa que dentro de las 24 horas siguientes al cumplimiento de las órdenes de registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por internet u otros medios similares, el fiscal debe comparecer ante el juez de control de garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado, incluida la orden. La misma norma precisa que *'durante el trámite de la audiencia sólo podrán asistir, además del fiscal, los funcionarios de la policía judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva, o que intervinieron en la diligencia'*. ***Sobre esto último aclara igualmente que: 'si el cumplimiento de la orden ocurrió luego de formulada la imputación, se deberá citar a la audiencia de control de legalidad al imputado y a su defensor para que, si lo desean, puedan realizar el contradictorio.*** *En este último evento, se aplicarán analógicamente, de acuerdo con la naturaleza del acto, las reglas previstas para la audiencia preliminar' (…)En punto al Artículo 244, el mismo dispone que la policía judicial, en desarrollo de su actividad investigativa,* ***puede realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público. Aclara que cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas, deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente,*** *'las disposiciones relativas a los registros y allanamientos'.* ***En los términos de las normas anteriores, también prevé el precepto el control posterior de legalidad sobre las diligencias de búsqueda en bases de datos, señalando que,*** *"estos casos, la revisión de la legalidad se realizará ante el juez de control de garantías, dentro de las treinta y seis (36) horas siguientes a la culminación de la búsqueda selectiva de la información'* (negrilla del original).

Con el objetivo de individualizar la tipología del delito consagrado en el tipo penal del Artículo 269C denominado *De la interceptación de datos informáticos*, es necesario realizar una evaluación del tipo desde el ámbito de conocimiento de la Ciencia Informática. En la descripción del tiempo de expresa el término "interceptar datos informáticos", ello se debe entender como la acción de extraer

datos que están en un proceso de movimiento cuando se identifica con acciones de envío, recepción, transferencia, y excluyendo de su alcance conceptual e interpretativo los datos estáticos.

Igualmente, se describe respecto de los datos objeto de interceptación que éstos pueden ser abarcar los datos en su origen (es decir el punto donde se envía), en su destino (es decir al punto donde llega) o en el interior de un sistema informático (hay que aclarar el concepto sistema informático como el "SISTEMA INFORMÁTICO: Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea."), sin que dentro del tipo penal se le pueda dar alcance de cobertura la etapa en el intermedio del receptor y el emisor a pesar de que tecnológicamente si es posible.

También habla de las emisiones electromagnéticas provenientes de un sistema informático, aunque hay muchas formas de comunicación por medio de emisiones electromagnéticas, entre ellas se encuentra la radio, el *wifi*, los celulares, entre otros), comunicaciones que para ser interceptadas basta solo hacerse pasar por el receptor. De otro lado si se refieren a un sistema informático también se incluye la intercepción de información entre la persona y el dispositivo informático que se incluya en el sistema de información.[4]

Daño informático

> Artículo 269D: *Daño Informático.* El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2009).

Se trata de un tipo penal básico o fundamental, de conducta instantánea por configurarse con la sola actuación del sujeto; es un claro ejemplo de un tipo penal compuesto al estar integrado por varias acciones que encarnan el comportamiento delictivo y cerrado al estar claramente determinado en sus componentes y cometidos, de sujeto penal común y monosubjetivo.

Respecto al sujeto activo de la acción, como primer elemento objetivo del tipo penal, se identifica una situación similar a la ya explicada en el acceso abusivo al sistema informático, donde la disposición presupone la autorización previa para ejercer la acción que se configura como daño informático. El individuo requerido para la comisión del delito es un sujeto común que no se caracteriza por calidades particulares, pero que sí está sujeto a la situación de contar con la facultad de destruir, dañar, borrar, deteriorar o alterar datos informáticos, pues solo en el caso de no estar facultado para ello por medio de disposición jurídica o contractual, puede incurrir en la mencionada conducta.

[4] Construcción conceptual del grupo de investigadores: EAFIT y FUNLAM.

El sujeto pasivo de esta modalidad de conducta punible será el titular o titulares de un sistema informático por medio del cual se gestiona y dispone de datos informáticos, esto es, propietarios o usuarios directos del mismo, quienes como beneficiarios del soporte de información que directamente manejan a través de un sistema informático puntual, pueden verse como sujetos pasivos de una conducta de acceso abusivo.

El resultado de la acción queda sometido a un aparente margen de claridad, en la medida que la denominación del tipo al hablar de daño conduce a la materialización de una pérdida o afectación. No obstante, los verbos rectores, por medio de los cuales se delimita la acción del sujeto activo del daño informático, abarcan diversas modalidades conductuales.

La primera forma de comportamiento tipificada que conduce al daño informático es la destrucción de datos informáticos, o un sistema de tratamiento de información, o sus partes o componentes lógicos. Por destrucción la Real Academia de la Lengua (2001) define “ruina, asolamiento, pérdida grande y casi irreparable”. Desde allí se configura el daño informático en la pérdida casi irreparable de los datos informáticos que versan en un sistema informático, de un sistema de tratamiento de información, o de sus partes o componentes.

En aparente redundancia, el artículo dispone como modalidades de acción la dirigida al daño, reiterando el propósito de desnaturalizar la cosa haciéndola perder la funcionalidad y finalidad para la cual estaba destinada. También señala la acción de borrar, de donde se desprende “hacer desaparecer por cualquier medio lo representado”, en este caso, los datos informáticos; deteriorar, que alude a “estropear, menoscabar, poner en inferior condición algo”, para el presente caso también los datos informáticos, un sistema de tratamiento de información o sus partes o componentes lógicos; alterar que se refiere al “cambio de la esencia o forma de algo”, y suprimir que se refiere a “hacer desparecer”.

El tipo penal no señala un momento específico para la comisión del delito, y el objeto de la acción puede ser los datos informáticos que plasman información y datos propios de la intimidad de una persona, el sistema de tratamiento de información o sus partes o componentes lógicos.

Este tipo penal, visto solo desde el campo informático, está contemplado en el Artículo 296D Del *daño informático.* Se indica que es sujeto activo de esta conducta cuando no se posee facultad (entiéndase el término como: derecho, poder) de destruir (entiéndase el término aplicable a la acción física sobre el dispositivo donde se encuentren los datos informáticos), dañar (entiéndase el término como: impedir o alterar el correcto funcionamiento del dispositivo físico que contenga datos informáticos), borrar (entiéndase el término como: “Desvanecer, quitar, hacer que desaparezca algo”, es decir, eliminar información), deteriorar (entiéndase el término como: empeore o estropee el estado de un sistema informático), alterar (entiéndase el término como: modificar los datos informáticos, su contenido, los metadatos), suprimir (entiéndase el término como: básicamente lo mismo que borrar,

eliminar información) de un sistema informático. También se habla de un sistema de tratamiento de información, "es el sistema o base electrónica donde estan almacenados, tratados y analizados los datos" (Marica, A., 2012).

Finalmente, cuando se habla de “sus partes o componentes lógicos” se puede hacer referencia a los dispositivos físicos que conforman el sistema.

Uso de software malicioso

> Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2009).

Reiterando las características más comunes que clasifican los tipos penales informáticos dispuestos en la Ley 1273 de 2009, el uso de software malicioso se refiere a un tipo penal monosubjetivo por requerir para su configuración a solo un individuo que despliegue la acción; dicho sujeto no es cualificado y tiene un comportamiento que se configura por medio de varias acciones, lo que lo convierte en un delito cerrado y compuesto.

Frente a los elementos objetivos del tipo penal en mención, se hace indispensable reconocer la figura del software malicioso para comprender la razón de por qué se tipifica su uso, y con ello, cada uno de los verbos rectores que tipifican la acción del sujeto activo simple o común exigido para la comisión de delito.

Carmen de Pablos Heredero, José Joaquín López Hermoso-Agius, Santiago Martín Romano Romero, Sonia Medina Salgado, Antonio Montero Navarro y Juan José Nájera Sánchez (2006) explican que el software malicioso también se conoce como código malicioso, y explican que estos pueden dañar un sistema o equipo, borrar datos, en este caso datos informáticos, generar denegación de servicios, corromper datos, bloquear accesos, enviar falsos mensajes o anuncios. Entre los software maliciosos que se pueden distinguir se destacan los virus informáticos y los troyanos (pp. 198-199).

Los virus informáticos los definen a partir del concepto establecido por Fred B. Cohen: “Un programa de ordenador que puede infectar otros programas modificándolos para incluir una copia de sí mismo”. Destaca que tienen diversas funciones, fundamentalmente la de propagarse y replicarse, pero además pueden contener carga viral (*payload*) que puede generar desde una broma virtual hasta daños del sistema informático (Heredero y otros, 2006).

Los virus a los cuales hacen referencia pueden ser de acción directa o residentes. Los primeros son aquellos que en el momento de su ejecución infectan a otros programas, y los segundos son

aquellos que al ser ejecutados se instalan en la memoria del ordenador, infectando los demás programas en la medida que se hace uso de ellos (Heredero y otros, 2006).

Por su parte, el Troyano es definido como un programa malicioso que se oculta en un programa de buena apariencia. Al momento en que ese programa aparentemente bueno se ejecuta, el troyano no realiza la acción o puede ocultarse en la máquina de la persona que hizo la ejecución.

A partir de la descripción especializada del software malicioso, se identifica que la necesidad de su tipificación radica en el peligro que acarrea el uso de soportes intangibles que afectan sistemas de información, atando el uso de dichos softwares a la autorización o facultad conferida de manera expresa en una situación determinada, lo cual, al igual que los tipos penales anteriores, deberá estar dispuesto en norma jurídica.

Se estima con ello que el objeto de la acción es un sistema informático como aquella integración de hardware, personal y software, siendo este último el detonante intencional del uso de un recurso dañino de la información. Sin que el tipo penal exija un momento específico para la comisión de la conducta, sí es amplio en disponer varias modalidades de comportamiento que tipifican el uso de este tipo de software.

Las acciones citadas son producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer, circunscritas al territorio nacional, sin que con ninguna de ellas se haga estricta referencia al uso directo de un software de naturaleza maliciosa. Nótese cómo las acciones dispuestas en la norma del Artículo 269E aluden a actividades de intercambio del bien con finalidades lucrativas, más no es su empleo directo frente en un sistema informático determinado.

Ello conlleva a que la finalidad del artículo se dirige más a contrarrestar las estructuras delictivas por medio de las cuales se disponen en el mercado los softwares maliciosos, más no atacan de forma directa el uso de estos soportes por parte de un individuo común desde la fase de desarrollo, toda vez que, si se judicializara la creación de la obra literaria en concreto, sería lo mismo que decir, un cuadro es ilegal si su contenido en la representación de un homicidio, es por ello que el operador judicial mal haría, para la aplicación del tipo penal, de judicializar a un sujeto por la creación literaria en la modalidad de soporte lógico, software.

La exclusión del uso como acción directa tipificada en la disposición se argumenta a partir de los alcances de los verbos rectores citados en la norma, pues la producción implica fabricar o elaborar algo, en este caso, un software con la potencialidad de desplegar su carga viral en un sistema informático. La producción de un bien implica su destinación a la finalidad para la cual fue creado, lo que hace que el mero acto de elaboración configure la acción del sujeto, sin que necesariamente este haya sido usado.

El tráfico implica la negociación ilegal del elemento creado, articulándose a las finalidades descritas con los comportamientos de venta, envío, adquisición y distribución, pues todas ellas se facilitan

o son posibles dentro de la actividad del tráfico de software malicioso. Por lo tanto incurre en la acción quien negocie ilegalmente con software malicioso, como el que venda, compre, distribuya, lleve o saque del territorio nacional, pero se reitera, ninguna de estas acciones implica el uso directo en un sistema informático del software de naturaleza maliciosa.

La ciencia informática permite analizar el tipo penal consagrado, Artículo 269E. *Del uso de software malicioso.* En este se habla de acciones que permiten incursionar en el comercio de software malicioso u otros programas con efecto dañino (en el que cabe aclarar que se trata de programas que intencionalmente están diseñados para afectar el correcto funcionamiento de los sistemas, causar fallos, daños informáticos u otro tipo de acción que atente contra la correcta funcionalidad de los sistemas informáticos).

Lo que parece incoherente es el título del artículo en el que se habla del uso del software malicioso pero solo se habla de su comercio, sin que alguno de los verbos rectores realmente judicialicen el uso, siendo mayor justificación a la premisa que se viene sosteniendo, con la cual, el desarrollo de software malicioso no es un delito, es la creación simplemente de una obra literaria, es por ello que solo se penaliza su producción, distribución y comercialización, es decir, ejercicio de una actividad mercantil con intencionalidad dañina, ya que lo contrario es precisamente el desarrollo de las herramientas informáticas necesarias para los expertos en seguridad informática.

Violación de datos personales

> Artículo 269F: *Violación de datos personales.* El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2009).

La violación de datos personales es un tipo penal de naturaleza compuesto por varias acciones que implican la comisión de la conducta; cerrado, de sujeto activo aparentemente común, y sin duda monosubjetivo. Pero una de las características más sobresalientes de este delito es su naturaleza pluriofensiva, en la medida que de manera más evidente se dirige a la protección de la intimidad personal y la información como bienes jurídicos protegidos.

A diferencia de los anteriores tipos penales informáticos, la violación de datos personales enfatiza con mayor especialidad el objeto de la acción y los bienes jurídicos contra los cuales atenta. Así, mientras que las conductas delictivas anteriores pueden verse dirigidas a la afectación de información de personas naturales y jurídicas, atentando contra escenarios de conglomerados sociales como empresas y compañías, la violación de datos personales individualiza el sujeto pasivo de la acción.

Por ello, el sujeto activo es un individuo común que no requiere de calidades o condiciones especiales para desplegar la conducta, y el objeto de la acción punible se relaciona de manera íntima con los bienes jurídicos tutelados, siendo para el caso una persona afectada en su intimidad y en su información.

Sobresale, de los elementos objetivos del tipo penal, un conjunto de componentes que es necesario analizar para comprender la finalidad reguladora del tipo. Habla la norma que el sujeto activo para incurrir en la conducta descrita no debe estar facultado para la obtención, compilación, sustracción, ofrecimiento, venta, intercambio, envío, compra, interceptación, divulgación, modificación o empleo de códigos personales o datos personales.

Ello nos conduce, una vez más, como en el caso de la interceptación de datos informáticos, a contemplar la postura por medio de la cual estamos en presencia de un tipo penal que no se refiere a un sujeto activo común, y que por el contrario requiere de un sujeto activo cualificado, pues al exigir la circunstancias de *no estar facultado* para adelantar cualquiera de las acciones que pueden constituirse como violatorias de datos personales, da lugar a que pueda darse la situación en la cual existan sujetos que estén facultados para desplegar cualquiera de las acciones mencionadas sobre los datos personales de un individuo sin que con ello configuren la acción tipificada en la norma.

Un segundo punto que debe ser resaltado radica en que el presente tipo penal incluye, entre los verbos que definen la acción, el de interceptar, comportamiento ya tipificado en el delito de interceptación de datos informáticos, generando una posible ambigüedad entre ambos consistente en la aparente regulación reiterada de una conducta.

Finalmente, también en relación con la interceptación de datos informáticos, mientras la violación de datos personales se dirige, como su denominación lo dice, a datos personales, el tipo de interceptación alude a datos informáticos, lo que debe acarrear una diferencia que facilite la comprensión de la disposición para su adecuación típica, por lo que se presentan tres elementos que requieren ser despejados.

Comenzaremos por el último de los puntos mencionados, que es establecer la diferencia entre los datos personales y los datos informáticos. Prevaleciendo en la doctrina especializada la definición de los datos personales desde la óptica de su protección, estos se definen por Efrén Santos Pascual e Iciar López Vidriero (2005) como: “Cualquier información concerniente a personas físicas identificadas o identificables” lo que le permite al autor afirmar que no todo dato debe ser protegido (pp. 29-30).

Por su parte, Sánchez Bravo (1998) los define como cualquier información concerniente a personas identificadas o identificables, aclarando que la persona física identificada no plantea problemas, pero sí los hay en las personas físicas identificables. Explica que el Derecho Comunitario Europeo considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular por medio de un número de identificación o uno o varios elementos específicos carac-

terísticos de su identidad física, fisiológica, psíquica, económica, cultural o social; definición que es compartida por Renato Alberto Landeira Prado, Víctor R. Cortizo Rodríguez e Inés Sánchez Valle (2006) en su obra *Derecho de las nuevas tecnologías.* Así, en palabras de Concepción Conde Ortiz, la protección de los datos personales se define de la siguiente manera:

> Protección jurídica de las personales en lo que concierne al tratamiento de sus datos de carácter personal, o de otra forma, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para confeccionar una información que, identificable con él, afecta su entorno personal, social o profesional, en los límites de su intimidad, incide en un derecho fundamental de elevado contenido (Conde Ortiz, 2006).

Señala, como características de la protección de datos personales, que estos sean susceptibles de tratamiento o se encuentren en soportes que sean igualmente susceptibles de manejo y que deben tener la posibilidad de identificar el resultado del tratamiento de los datos con su titular, y el manejo o acceso a los datos debe resultar sin su consentimiento.

Desde esas definiciones los datos personales hacen alusión a los pertenecientes a la intimidad e identidad de cada persona, provenientes o contenidos en distintos medios y relacionados con diferentes ámbitos de la vida, permitiendo englobar datos de naturaleza sentimental, laboral, crediticia o familiar. Dichos datos son susceptibles de ser consultados, pero no necesariamente deben estar depositados en un sistema informático o soporte similar, pudiendo ubicarse en soportes físicos como archivos o libros. Por contener información propia de la persona, su manejo estará restringido y no será de público acceso o consulta.

Así pueden clasificarse los datos que identifican a una persona, como su nombre, domicilio, documento de identidad y teléfono; datos laborales: lugar o lugares de trabajo, historial de actividades, modalidades de contrato y jornadas; datos económicos como su historial crediticio, su afiliación a entidades financieras, préstamos y gravámenes vigentes, etc.

Con escasa doctrina al respecto, se encuentra que los datos informáticos son cualquier dato creado o procesado de manera que pueda ser tratado por un sistema informático (Landaria Pradro, Cortizo Rodríguez y Sánchez Valle, 2006, p. 94). De allí resulta una información importante para clarificar y delimitar los alcances de los tipos penales expuestos. La interceptación de datos informáticos se reserva solo a la acción de interceptar datos informáticos como objeto de la acción, esto es, aquellos que pueden ser administrados o tratados por medio de un sistema informático; por su parte, la violación de datos personales no se limita a los datos que pueden ser tratados por medio de un sistema informático sino a códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, esto es, una amplia gama de medios en los cuales pueden reposar los datos personales de una persona, y que por tanto, un sujeto específico, sin estar facultado, puede ejercer cualquiera de las acciones tipificadas sobre ellos.

La interceptación de los datos informáticos se reserva a medios y acciones muy concretos, pues bien define ese tipo penal que la interceptación da sobre "datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas", por lo que puede tratarse de datos informáticos que contengan datos o información personal de una persona, o bien pueden ser datos informáticos referentes a un tema diferente a información personal y que de igual forma son objeto de interceptación.

La violación de datos personales, si bien se puede manifestar en múltiples modalidades conductuales, requiere que el sujeto no facultado para su manipulación este desplegando su actuar delictivo sobre datos de naturaleza personal, lo que engloba los diferentes soportes en los cuales pueden reposar estos, incluyendo la modalidad de datos informáticos. Es así como la interceptación es una de las modalidades de violación de datos personales, informáticos o no, por parte de un sujeto que no está facultado para proceder con ese comportamiento sobre esa fuente de información.

De forma adicional, es importante mencionar que la violación de los datos personales por parte de un sujeto no facultado debe acarrear provecho para él o para un tercero, aspecto que no se exige en la interceptación de datos informáticos. El provecho implica la obtención de un beneficio extraído del dato personal. El provecho no necesariamente será pecuniario, pues el poder de la información violada podrá alcanzar esferas de otra naturaleza que representen perjuicio o menoscabo para el titular del dato personal.

Por último debemos retomar la calidad del sujeto activo de la acción, el cual como ya hemos mencionado no debe ser en estricto sentido un sujeto común, pues varios de los verbos rectores que orientan la acción punible del tipo de violación de datos personales exigen la calidad de un sujeto cualificado. Sobre este punto Acurio del Pino (2011) explica:

> Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.
>
> Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que "desvía fondos" de las cuentas de sus clientes.

Se estima oportuno sostener en este punto que el elemento objetivo del tipo penal referido al sujeto activo de la acción acarrea una posible variabilidad de calidad en el tipo de violación de datos personales. La calidad de dicho sujeto podrá estar condicionada por la acción que determina la conducta típica descrita en la norma, haciendo que para casos como la interceptación se aluda

a integrantes con funciones de policía judicial, pero que quien divulgue u ofrezca datos personales sea un sujeto común de confianza al titular de la información.

El alcance de los verbos rectores, Artículo 269F. *De la violación de datos personales.* Que con fines de obtener beneficio propio (o beneficiar a un tercero), se comercie, obtenga, publique, modifique o utilice información que no es de su propiedad, entre ellos los códigos personales (sin que pueda entenderse como término genérico no especifica se trata de códigos tipo software (cod. fuente, cod. objeto) o códigos tipo contraseñas o *passwords)*, y por otro lado, se habla de *datos personales,* los cuales deben estar almacenados en "ficheros, archivos, bases de datos o medios semejantes", en consecuencia, es necesario aclarar la diferencia o sinonimia entre la palabra *fichero y archivo.*

Según la Real Academia Española (2001), el término fichero para la informática significa: "Conjunto organizado de informaciones almacenadas en un soporte común", mientras que archivo se define como "Espacio que se reserva en el dispositivo de memoria de un computador para almacenar porciones de información que tienen la misma estructura y que pueden manejarse mediante una instrucción única" (Real Academia Española, 2001). Cabe resaltar que para la nueva versión del Diccionario de la Real Academia Española el término "fichero", en el campo de la seguridad informática, es sinónimo del término "archivo", en el que se explica que es un conjunto de información.

Aclarado el concepto, el uso del archivo y del fichero, de la norma, proporcionan una incomprensión en la interpretación del tipo, toda vez que existe redundancia de dos términos que tienen el mismo significado.

En igual sentido de incomprensión para la interpretación correcta del tipo, no se permite, desde la lectura del tipo, saber a qué se refiere el legislador cuando expresa "medios semejantes"; no se sabe si abarca los dispositivos de almacenamiento (memorias, discos duros) que no necesariamente siempre están o hacen parte de un computador o si está hablando de forma diferenciadora del término frente a archivo, fichero, base de datos. Por lo visto sería pertinente aclarar qué tipos de medios deben tenerse en cuenta para la aplicación de este artículo, y qué dispositivos se ven afectados por la regulación de los datos personales, pues solo así el juez control de garantías podría válidamente establecer la garantía de las medidas y órdenes de obtención de la evidencia digital, en medios informáticos, si es que a esto se refiere el legislador.

Suplantación de sitios web para capturar datos personales

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

> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito. (Congreso de Colombia, 2009).

De manera uniforme con el espíritu normativo de los demás delitos informáticos, el tipo penal de suplantación de sitios web para la captura de datos personales puede considerarse como un importante avance en la tipificación de conductas efectuadas por medio de las nuevas tecnologías, en este caso, de los medios informáticos.

De naturaleza dolosa, monosubjetiva y de sujeto activo simple, la suplantación de sitios web para la captura de datos personales se clasifica también como un delito cerrado que no requiere remisión a otra disposición del articulado, mas sí exige la comprensión de los soportes informáticos de los cuales se vale para la obtención del resultado, en la medida que en este caso son el medio de la conducta delictiva.

Es un claro ejemplo de tipo penal compuesto al contemplar la comisión de la acción a través de varios verbos rectores, y junto con el delito que le precede; es también pluriofensivo, pues atenta contra los mismos bienes jurídicos ya protegidos por la violación de datos personales.

En la descripción típica de la conducta sobresalen inicialmente dos componentes de necesaria mención. En primer lugar el tipo penal explicita la modalidad dolosa de la conducta al establecer la finalidad ilícita de la suplantación del sitio web. En el caso debe especificarse que dicha finalidad depende del sujeto activo, en donde tanto profesionales y especialistas en informática, así como personas del común, se cualifican en la actualidad con mayor facilidad en la elaboración y gestión de sitios web, lo que hace de estas plataformas objetos de negociación cotidianos en la sociedad que pueden verse sujetos a este tipo de atentados.

En el presente tipo penal se hace absolutamente necesario articular el objeto ilícito que guía el comportamiento del sujeto activo a la suplantación del objeto de la acción. En ese sentido se considera necesario diferenciar dos situaciones hipotéticas posibles reguladas por la órbita normativa del tipo en mención.

De un lado debe contemplarse la comisión de la suplantación de forma autónoma e independiente por parte del sujeto activo, esto es, iniciada por motivación propia y exclusiva del sujeto, dando lugar a cualquiera de los verbos rectores delictivos tipificados en la norma, y con ellos, capturando datos personales de un tercero. En la situación mencionada, el objeto ilícito citado en la disposición se configura en el móvil desviado que debe guiar el comportamiento de alguien que por medio de un sitio web tenga acceso a los ya definidos datos personales de una persona.

Sin embargo, una segunda situación hipotética permite proponer un nuevo alcance del objeto ilícito como elemento objetivo del citado delito. El diccionario dice: "Ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba" (Real Academia Española, 2001), situación que conduce al nacimiento de la suplantación, ya no por la estricta iniciativa del criminal sino por la relación que puede ser establecida entre el sujeto activo con el sujeto pasivo de la acción.

La segunda hipótesis abre campo a la comisión de la acción típica por efectos de una relación preestablecida entre los dos sujetos, sea de índole gratuita u onerosa, pero sin duda, donde un individuo acude a otro que tiene conocimiento para el diseño, desarrollo, tráfico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes.

En el acuerdo de voluntades entre los sujetos, frente al propósito que será cumplido por medio del sitio web, se configura la calidad del objeto de la relación jurídica que los vincula, aspecto que se determina por la facultad que puede otorgar o no el posible afectado de la acción. Esto es, si en la relación el sujeto titular de los datos personales faculta a alguien para el diseño, desarrollo, tráfico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes donde se disponga de los datos personales, no habrá lugar a tipificación de la conducta punible en la medida que se cuenta con autorización del titular de esos datos, y con ello, ejerce sus derechos fundamentales de intimidad e información.

Pero de otro lado, la celebración de un acto jurídico se reitera gratuito u oneroso; debe estar siempre amparado por la presunción de la buena fe que soporta el acuerdo de voluntades de las partes, haciendo que los actos jurídicos se acoplen a los mandatos jurídicos que proporcionan la naturaleza lícita que exige el ordenamiento jurídico. Por lo tanto, el diseño, desarrollo, tráfico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes donde se disponga de los datos personales podrá convertirse fácilmente en objeto de un acto jurídico en donde un individuo será facultado por el titular de los datos personales para cumplir labores puntuales por medio de unos de los medios informáticos citados, evitando así resultados contrarios a su voluntad, y en lo posible, al ordenamiento jurídico.

Desde el supuesto en mención, en caso que el sujeto facultado para ejercer labores sobre los medios informáticos que posibilitan la manipulación de datos informáticos desconozca o sobrepase la autorización de las acciones posibles otorgadas por el titular de la información, desnaturaliza la licitud del objeto del acuerdo jurídico previo, tipificando la conducta descrita como suplantación de sitios web para capturar datos personales.

Las razones para asegurar esta tendencia radican en el concepto de objeto jurídico y de su rol en el acto jurídico. Todo acto jurídico es manifestación de la voluntad discernida, intencionada y reflexionada de las partes, encaminada a buscar el cumplimiento de efectos jurídicos prácticos, que a su vez se encuentran protegidos por el Derecho, esos efectos son el objeto del acto que tiene dos clases, uno genérico y otro específico.

El objeto genérico incluye no solamente lo que concreta y prácticamente se proponen las partes, sino también lo que la ley le agrega, o lo que por naturaleza le pertenece al contrato, incluso forman parte del objeto genérico del contrato las cláusulas de uso común, aunque no se expresen. El específico radica en el propósito particular que cada acto jurídico tiene según el querer de las partes o lo que la ley de manera supletoria o imperativa establezca.

Poder asegurar el objeto en un acto jurídico como elemento de validez implica que este reúna unos requisitos irrenunciables. Adicional a que se presente en la vida del acto, es indispensable que el objeto sea posible, sea determinado o determinable y sea lícito. El objeto lícito de la prestación o la cosa material del acto o negocio jurídico en sí no es bueno, ni es malo, su calificación ética, moral y jurídica es totalmente indiferente.

La licitud de un objeto debe hacerse teniendo en cuenta la destinación del mismo en el acto jurídico; es necesario identificar el contenido intrínseco de la prestación que han convenido las partes en el acto, o la finalidad de la prestación. Pero en este último caso la finalidad ya no será el objeto sino la causa; por lo que se considera la licitud o ilicitud a partir de la prestación aisladamente y en su conjunto, considerando de manera muy importante el propósito, la intención, el querer que tuvieron las partes de darle a ese objeto una u otra destinación, uno u otro propósito.

Es por ello que la finalidad de las partes, como se propuso más arriba, resulta determinante; la facultad de hacer que puede conferir el titular de la información al sujeto que podrá accionar con ella por medio de un sitio web determina la licitud o ilicitud del objeto. Finalmente, basta señalar que para la licitud o ilicitud en el objeto hay que tener en cuenta el concepto del orden público, si el objeto de esa destinación aisladamente y en su conjunto está de acuerdo con el orden público es lícito, como lo señala el Artículo 1518 del Código Civil, y si riñe con esto el objeto es ilícito.

Otro aspecto para analizar sobre el Artículo 269G es el siguiente: se deben de aclarar términos como “página electrónica”, donde al parecer se quiere hacer referencia a una página web, ya que el término como tal no está bien definido o generalmente reconocido, aunque podría entenderse como referencia a una página digital (término que a su vez tampoco está claramente contextualizado).

En este artículo se sanciona al que “con objeto ilícito y sin estar facultado...” diseñe, desarrolle, programe (esos tres términos son muy similares, pero determinan partes diferentes de la producción de un software), trafique, venda (dejando excluido tácitamente la penalización sobre el acto de adquirir o comprar), ejecute o envíe (sin dar claridad si la acción o acto de envío es voluntario o involuntario, y en consecuencia, si es posible probarlo) páginas electrónicas (que no está claro el término y aunque se podría dar lectura e interpretación como página web, solo por la denominación otorgada al tipo penal), en igual sentido se habla de enlaces o ventanas emergentes.

En la redacción del tipo penal se describen acciones que enmarcan medios de ataque reconocidos internacionalmente como phishing, soopfing y pharming, y que no se individualizan en el texto

del tipo, generando una brecha conceptual con el contexto internacional en la denominación, aceptada ya de forma genérica, para la identificación de conductas realizadas por los ciberdelincuentes, lo cual podría eventualmente tener una implicación negativa al momento de la judicialización de conductas por no establecer el alcance de la conducta en términos generalmente aceptados.

Circunstancias de agravación punitiva

Culmina el capítulo con el Artículo 269H que contiene circunstancias de mayor punibilidad en los siguientes términos:

> Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
>
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
>
> 2. Por servidor público en ejercicio de sus funciones.
>
> 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
>
> 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
>
> 5. Obteniendo provecho para sí o para un tercero.
>
> 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
>
> 7. Utilizando como instrumento a un tercero de buena fe.
>
> 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. (Congreso de Colombia, 2009).

Deben destacarse de la anterior disposición varios aspectos que resultan relevantes frente a los tipos penales ya analizados. En primer lugar es circunstancia de mayor punibilidad de los delitos informáticos su realización sobre soportes informáticos de dos sectores en particular: el Estado y el sector financiero, nacional o extranjero. ¿Por qué aumentar la punibilidad por tratarse del Estado? La respuesta que puede englobar todas las variables que argumenten esta causal es: por el interés público.

De manera tradicional, los sistemas jurídicos asociaron, y aún lo hacen, la defensa y garantía del interés público a manos exclusivas del Estado, lo que implicó que era el Estado quien determinaba

y priorizaba aquellos ámbitos de la vida del conglomerado social, siendo de interés público aquel que adoptaba el Estado frente a un tema como razón de gestión e intervención.

> La voluntad estatal soportada en el interés público se difumina en el cumplimiento de intereses vinculados a programas de gobierno, generando los flagelos que debilitan su ejercicio y valoración por parte de la sociedad, absorbiendo el interés público al concepto de interés del Estado, desfigurando con ello, el ejercicio y finalidad del derecho (Vásquez Santamaría, 2009, p. 21).

Pero bien esa visión ha cambiado, y el interés público se escinde del interés de la idea de ser del Estado, para ubicarse en una esfera amplia e incluyente que viene siendo perfeccionada desde los nuevos fundamentos como la participación y la representatividad del Estado Social de Derecho, y del Derecho como medio para la materialización del interés público, mas no del Derecho como instrumento para la materialización de los intereses de relevancia para el Estado.

> En esta perspectiva, el interés público es un elemento innato a la esencial del derecho, sustentado en la dinámica social que se ubica como sustrato desde el cual se origina, transforma y vivencia el derecho; que ubica al individuo como sujeto de derechos individuales y colectivos, valorando su importancia como actor social y político, participe del ejercicio democrático, activo frente a la protección y reconocimiento de derechos, el control del ejercicio del Estado, atento y sensible frente a las dinámicas y problemáticas sociales que lo involucran, donde se supera la sinonimia entre el interés público y el interés del Estado, así como las visiones tradicionales que enfocan el derecho únicamente como una emanación del Estado, materializado en un conjunto de normas para garantizar la institucionalidad en una sociedad.
>
> El interés público (…) es concepto dinamizador y valorativo que hace de los ordenamientos jurídicos, mecanismos efectivos que dinamizan y reconfiguran la mentalidad de los actores jurídicos y judiciales, que requiere de los espacios académicos, investigativos y profesionales, la máxima atención en momentos de problemáticas sociales tan complejas como las actuales.
>
> Interés público es una fuerza que puede y debe redimensionar la esencia del derecho. Implica reorientar la visión al interés general como elemento que siempre ha estado presente en el derecho, y con él, redimensionar al hombre como destinatario de la norma, como parte inherente de la sociedad y de la cultura (Vásquez Santamaría, pp. 25-26).

Así radica y radicará en el Estado la defensa y garantía del interés público, sin que este sea el que determine en actos unilaterales frente a la colectividad, sino el que identifique como relevante del ejercicio social. En ese contexto, la información, las comunicaciones y la salvaguarda de los derechos fundamentales directamente relacionados con esas materias son un objeto relevante que sigue estando a cargo de las autoridades oficiales, motivo por el cual, al convertirse en objeto de actos delictivos, deben acarrear aumento de punibilidad. A estos fundamentos se considera necesario articular la disposición contemplada en el numeral sexto del Artículo 269H.

Frente al sector financiero, el mismo artículo, en las causales de agravación, llama la atención sobre las circunstancias previstas en los numerales dos y cinco. La circunstancia del numeral dos dispone "por servidor público en ejercicio de sus funciones", implicando una posible revaluación de algunos de los tipos penales antes analizados. Se afirmó, en el apartado referente al delito de interceptación de datos informáticos y el de violación de datos personales, la necesaria intervención de un sujeto activo cualificado por las especiales situaciones que se han originado en el ámbito jurídico nacional, así como la existencia de disposiciones jurídicas puntuales dirigidas a las acciones que tipifican la norma penal, recordando adicionalmente la exigencia de la orden judicial previa en el caso de la interceptación de datos informáticos, medida que atiende a dicha realidad.

Siendo así la disposición consagrada en la norma ¿cómo tipificar en un sujeto común una conducta que requiere orden judicial previa y control judicial posterior? Con un cometido propositivo se estima necesario mantener la naturaleza de sujeto activo cualificado en los tipos penales en mención, pues las actividades ejecutadas conforme a la descripción conductual del tipo penal atienden la realidad colombiana en un ejercicio mayormente delictivo de parte de funcionarios públicos que ejecutan funciones de policía judicial, razón con la que se reitera la disposición de una orden judicial previa para adelantar una interceptación.

Ello no excluye la posibilidad de que un sujeto común pudiese desplegar una conducta como las dispuestas en el delito de violación de datos personales, pues bien debe reconocerse que conteniendo el verbo rector de interceptación, el tipo dispone de otra serie de verbos que caracterizan las acciones delictivas tipificadas como violatorias de datos personales.

Fuera de todo lo anterior, es altamente relevante poder encontrar en la misma disposición de la Ley 1273 de 2009, una norma que cierre el vacío dispuesto en la redacción de los tipos penales informáticos que quedan en una aparente apertura frente a la interpretación de cuál es el sujeto activo que puede incurrir en la comisión del delito.

No obstante, ello no puede entenderse como la regulación de conductas de forma amplia y caprichosa, dispuestas para cualquier individuo que incurra en las descripciones típicas mencionadas, pues si bien se ha identificado cómo la interceptación de datos informáticos se reserva a sujetos cualificados y es un factor no estimado por la norma, en los demás tipos penales se hace imprescindible desentrañar la situación en la cual actúa el sujeto que reúne calidades especiales, pues distinta resulta la comisión de la conducta de parte de un funcionario público en ejercicio de sus labores sin contar con la autorización o facultad exigida por la ley, razón que lo conduciría a un aumento de la pena conforme a la circunstancia de mayor punibilidad, a la comisión de la conducta por parte de un funcionario público que por fuera de las labores determinadas legalmente para su cargo, se valga de los medios oficiales para la comisión del delito, o que por fuera de su jornada laboral incurriera en la conducta criminal o se valiera de los conocimientos adquiridos en razón a su cargo para la comisión de la misma.

En relación con la circunstancia cinco que reza “obteniendo provecho para sí o para un tercero” cabe preguntarse si siendo dolosas las conductas tipificadas en la ley, su comisión ¿no acarrea un provecho para el actor? ¿Cuándo no podría aseverarse el provecho del actuar del sujeto activo o de un tercero en estas conductas?

Frente a esta temática vale destacar, desde una visión informática, en el Artículo 269H: *De las circunstancias de agravación punitiva,* en donde se habla de condiciones en las que se aumenta la sanción por un delito cometido en esta ley, el numeral 5, el cual establece que se debe aumentar la pena si se *obtiene para sí o para un tercero,* tal y como inicia el tipo penal reglado 269F cuando desde el inicio de descripción de la conducta tipificada se refiere a: “El que, sin estar facultado para ello, con provecho propio o de un tercero...”, es decir, que realizar la conducta en este tipo penal depende del provecho para sí o para un tercero, en consecuencia, ¿se aplicaría o no la agravación?, pues su aplicación aparentemente sería una doble sanción, toda vez que, como ya se indicó, se agrava es el provecho, mas no la conducta informática desplegada.

CAPÍTULO II. De los atentados informáticos y otras infracciones

El bien jurídico tutelado, en el campo penal, funciona como mecanismo de materialización para el legislador al momento de tutelar la protección de derechos del ciudadano frente a conductas constitutivas de conductas delictuales o con miras de catalogarse como tal, partiendo del impacto social que pueden llegar a generar, especialmente en la huella del daño social.

No es ajeno a ello el impacto que se genera con las conductas violatorias de un bien jurídico como el patrimonio, sin embargo, como muchas veces se evidencia en la parte motiva de fallos condenatorios o absolutorios en el tratamiento de delitos informáticos, los siguientes dos tipos penales objeto de análisis poseen en su estructura un direccionamiento patrimonial, aunque en ocasiones, el bien hurtado o transferido no consentida, constitutiva de información o dato informático, estos últimos son bienes jurídicos tutelados en esencia por esta ley.

> Artículo 269I: *Hurto por medios informáticos y semejantes.* El que, superando medidas de seguridad informáticas, realice la conducta señalada en el Artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el Artículo 240 de este Código.
>
> Artículo 269J: *Transferencia no consentida de activos.* El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción

se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. (Congreso de Colombia, 2009).

Merece un análisis sustentado la reciente postura interpretativa de la doctrina colombiana, liderada por el doctor Alexander Díaz (noviembre de 2010) en su artículo académico en el cual establece el campo y límite de interpretación, la aplicación de las conductas, del cual se extractan los apartes más importantes que permiten sustentar la tesis que arroja la investigación, con la cual se plantea una doble utilidad respecto del bien jurídico tutelado, toda vez que admite no solo el bien jurídico tutelado, en muchas ocasiones denominado patrimonio, y en otras el bien jurídico integrado por la ley sometida al análisis, como son la información y el dato informático, así:

Según investigación del periodista de la revista Enter Luis Iregue, afirma que de acuerdo con el más reciente estudio realizado por The Economist Intelligence Unit para Kroll –una empresa de inteligencia empresarial–, titulado Global Fraud Report, Colombia ocupa el segundo puesto en los países más victimizados por el fraude, sólo detrás de China y por delante de Brasil. Afirma el columnista que el estudio de Kroll establece que el fraude y el hurto de información por primera vez en la historia han superado los otros tipos de fraude en el mundo, y dice que 'el 94% de los negocios colombianos sufrió algún fraude en el último año, en comparación con el 88% global'. El 21% está en la categoría de fraudes electrónicos, que incluyen hurto de información y ciberataques (a sitios web e infraestructura de las empresas), y el porcentaje podría crecer en los próximos años.

Las cifras de fraudes electrónicos en Colombia y Latinoamérica son un poco menores que en China y otros países de Oriente, pero no dejan de ser preocupantes y superan el 20% de las empresas, una cifra importante si se tiene en cuenta que sólo 30 de cada 100 latinoamericanos tiene acceso a Internet.

Después de este prolegómeno periodístico, haremos unas pequeñas reflexiones sobre el tema, el que me ha generado preocupación desde el punto de vista de mi experiencia en Nuevas Tecnologías, Juez Informático y en especial como autor del texto original del proyecto de ley (hoy Ley 1273 de 2009) de delitos informáticos. He observado que algunos empresarios (de la vieja generación) no le han puesto aún la atención debida a la calidad de bien que tienen con la información, pues le restan mucha importancia al considerarla un intangible aparentemente sin valor. Éstos incurren en un lamentable error porque ignoran tal vez, que amén de todos los bienes físicos, ésta constituye también parte de sus activos (fijos), tal vez uno de los primordiales sino el principal, pues es un verdadero activo, el que se debe sumar indudablemente al patrimonial, como parte de los haberes de éstos en la empresa.

Dentro de la ley de delitos informáticos, además de los otros tipos que protegen el bien jurídico tutelado de la Información y el Dato, redactamos uno denominado: 'Artículo 269 J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática

o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad'.

Como observamos en su sintaxis el término 'transferencia no consentida de cualquier activo', implica precisamente eso, cualquier otro activo (además de los conocidos como patrimoniales clásicos), esto es, también la información. Lamentablemente algunos especialistas judiciales (Delegados del Fiscal y Jueces) y algunos Abogados no lo han entendido y creen que dicha transferencia sólo se refiere a dinero almacenado (desocupar cuentas bancarias) en bases de datos electrónicas (cuentas como vg. tesorerías, pagadurías o bienes muebles como los existentes en un almacén), incurriendo así en una desatinada apreciación. ¿Cómo nos explicaríamos qué clase de tipo penal incurrirían los sub judices si éste (os) ordena (n) la transferencia de una base de dates de clientes, proveedores, perfiles u otros, de una dirección (cuenta) a otra? ¿Cuál sería su adecuación típica? Estos comportamiento los están adecuando o subsumiendo en tipos clásicos y en forma exclusiva contra el patrimonio económico.

Observamos también con beneplácito como las empresas nacionales han pronosticado invertir más en sistemas de gestión de riesgos, entrenamiento del personal, controles financieros y herramientas de seguridad informática. El sistema judicial colombiano por ello no puede quedarse rezagado en implementar verdaderas políticas de seguridad en la información, pues a medida que pasa el tiempo los ficheros con los datos judiciales de los sub judice, estarán más expuestos y serán vulnerables para propósitos diferentes a las verdaderas políticas criminales del Estado.

Por eso y acertada se torna que la nueva generación de ejecutivos colombianos (lo afirma el columnista arriba citado) hayan modificado su otrora pensamiento y le han dado un nuevo valor a la información y por ello tienen planeado invertir en mejores soluciones de protección (dispositivos electrónicos, políticas de seguridad en la información, las ISO 27001, 27002, 27005, capacitación).

Observamos también con beneplácito como las empresas nacionales han pronosticado invertir más en sistemas de gestión de riesgos, entrenamiento del personal, controles financieros y herramientas de seguridad informática. El sistema judicial colombiano por ello no puede quedarse rezagado en implementar verdaderas políticas de seguridad en la información, pues a medida que pasa el tiempo los ficheros con los datos judiciales de los sub judice, estarán más expuestos y serán vulnerables para propósitos diferentes a las verdaderas políticas criminales del Estado.

Implementando efectivas herramientas para evitar intrusiones, garantizaremos la seguridad, integridad y confidencialidad de la información y por ende estará y se mantendrá incólume la información, la que servirá, si ese es el uso que le piensa dar (casi siempre lo es), en una excelente evidencia digital. Recordemos como hoy por hoy, la evidencia digital se ha ubicado en lugares pri-

> vilegiados en el ámbito probatorio, constituyéndose en muchas oportunidades en la prueba reina, en cualquier proceso judicial. Ello implica que su errado manejo forense o semi-forense (rol que algunos ingenieros están asumiendo sin ser especialistas en las ciencias forenses) malogran ésta y para cuando se sube al proceso el Juez la excluyen por ilegal (su extracción y fijación) declarándola nula; una vez declarada judicialmente nula (la evidencia digital) no sirve para absolutamente nada, entendiéndose que a futuro no se podrá usar ésta para ningún fin (tal vez para enseñanza académica y poner en conocimiento qué es lo que no se debe hacer con ella) porque una prueba nula no existe.
>
> A guisa de conclusión hemos de concienciarnos que debemos ofrecerle especiales, serias y verdaderas garantías de protección a la información y más la que se almacena en dispositivos electrónicos, como un verdadero activo del capital de una empresa, sin olvidar la información guardada en los protocolos digitales de los organismos del Estado (pp. 1-3).

Permitiendo, entre otras cosas, hacer afirmaciones con fundamento legal, cuando una empresa posea un software como activo de su empresa (entiéndase el programa con el código fuente, como titular de derechos patrimoniales de autor, no una simple licencia de uso que es lo habitual en cualquier empresa no desarrolladora), si el código fuente es transferido de una máquina a otra por medio de una red, atendiendo al requerimiento que el ciberdelincuente realiza al custodio del programa, donde lo induce a la transferencia sin que el verdadero propietario lo autorice, lo primero que se debe catalogar es que el software es un activo, y así se debe encontrar registrado incluso en la contabilidad de la entidad; esta transferencia es constitutiva de una sanción de tipo 269J, la información que ha sido materializada en un soporte lógico, obra literaria, o software, tal y como desee catalogarse, pero que sigue siendo una compilación de información, se ha afectado y puesto en vulneración al transferirse, y la empresa ha perdido la obra y los datos contenidos en este.

Vale la pena terminar el análisis de estos tipos penales con la interpretación de los tipos desde una visión informática (Artículo 269I: *Del hurto por medios informáticos y semejantes*). Se habla del hurto a partir de los artículos tradicionales 239 (de hurto simple) y 240 (de hurto calificado). Se habla de la manipulación de un sistema informático con estos fines y también de una red de sistema electrónico, telemático u otro medio semejante.

Con respecto al sistema informático se aclara en la parte de términos clave, por otro lado, la definición de *red* de sistema *electrónico* no queda clara, se podría interpretar el sistema electrónico como “un conjunto de circuitos que interactúan entre sí, siguiendo programación para un fin común. Las partes se componen por bloques, de entrada, de procesamiento y de salida (IES Tiempos modernos), lo que nos lleva a que la unión de varios de estos sistemas nos generaría una red de sistemas electrónicos, aclarando un poco la referencia que se desea hacer con respecto a la manipulación de hardware con el fin de hurtar; lo que no queda claro son los programas, la violación de programas, permisos y otros medios de *hacking* con el fin de hurtar información o datos personales, que son aquí vagamente posibles de incluirse dentro de bienes jurídicos sobre los cuales puede recaer la conducta, permitiendo dar mayor fundamento a lo planteado para el 269J.

Frente al Articulo 269J. En concreto y bajo una lectura no juiciosa, y ligera del tipo, es decir, sin el más mínimo análisis hermenéutico, pareciera que este tipo penal denominado “de la transferencia no consentida de activos” trata conductas constitutivas de robo por medios informáticos, es decir, quien manipule sistemas informáticos o programas con el fin de realizar transferencias no consentidas de activos estará violando la ley.

También se condena a quienes fabriquen, programen o faciliten este tipo de programas. Pero como ya se indicó arriba, esta tipificación no es sobre el hurto, es de otras transferencias que contienen principalmente información de quien es víctima de la conducta, pero no en el marco de la intimidad personal, es del campo empresarial, financiero, comercial, en fin, de todo campo donde el propietario de la información la valore como un bien y la haga parte de su activo fijo que impacta de forma significativa el patrimonio económico del afectado.

g) Protecciones jurídicas

El sustento fáctico que se presenta en la era moderna con el avance de las tecnologías refleja a su vez un incremento en la capacidad delictiva de los seres humanos, que valiéndose de los mismos soportes tecnológicos despliegan nuevas modalidades conductuales que deben ser sancionadas por las normas jurídicas.

En ese sentido, las constituciones políticas reconocen generalmente en su parte dogmática el secreto de las comunicaciones como un derecho fundamental de aplicación inmediata y exigible judicialmente. Las disposiciones que regulan tal derecho garantizan al ciudadano la libertad para despojar del conocimiento ajeno las comunicaciones postales, telegráficas y telefónicas en las que él intervenga.

Pero por su misma naturaleza de derecho subjetivo, el secreto de las comunicaciones no posee carácter absoluto, viéndose sujeto a límites jurídicos que el mismo constituyente o el legislador establecen con miras a lograr la armonización del mismo con otros derechos o libertades, como también con la preservación de intereses igualmente significativos para el normal funcionamiento del Estado Democrático.

Por ello es necesario hacer referencia al bien jurídico protegido por la nueva ley de delitos informáticos, inicialmente desde las disposiciones constitucionales que lo articulan con la protección y defensa de otros derechos ciudadanos directamente compenetrados con el mencionado bien, y posteriormente desde las normas legales en materia penal.

h) El derecho a la intimidad

El Artículo 15 de la Constitución Política de Colombia de 1991, respecto al derecho a la intimidad, establece:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Como puede verse, este artículo comprende varios aspectos importantes a tener en cuenta. En primer término se establece la protección a la intimidad de los seres humanos y de la familia, así como al buen nombre por lo que se establece el derecho a la protección por parte del Estado y de los particulares a la intimidad, y al buen nombre y el deber de respeto para estos derechos.

Se crea la reserva de la correspondencia y la posibilidad de que exista reserva sobre las relaciones familiares, de amistad, de amor, sobre la economía familiar, sobre la información relacionada con la salud de las personas, entre otras, siempre y cuando no se atente contra el interés general de la sociedad. Esto quiere decir que si por ejemplo un padre está atentando contra los derechos de su hijo no puede alegar el derecho a la intimidad para evitar el control del Estado sobre sus actos.

Adicionalmente, este artículo hace referencia al denominado Habeas Data o derecho al adecuado manejo de la información que se tiene de las personas en bancos de datos o en archivos de cualquier naturaleza. Como excepción a este adecuado manejo y reserva de información debemos entender que en los casos tributarios, judiciales o de control y vigilancia que el Estado ejerce sobre determinadas actividades se puede exigir la presentación de información que se maneja en forma privada, como en el caso de los libros de contabilidad que las personas deben llevar cuando así lo señala la ley.

Solo en ciertos casos, y bajo determinadas condiciones, resulta legítima y válida la afectación del secreto de las comunicaciones por medio de una injerencia estatal sobre la libertad del individuo, buscando obtener por esta vía pruebas que permitan demostrar la materialidad de un hecho delictivo, e identificar o descubrir sus autores y partícipes. El Artículo 14 de la Ley 906 de 2004 estipula que sólo en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos, podrá realizarse la búsqueda selectiva en bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones.

El mencionado supuesto legal trasgrede el derecho a la intimidad de forma transitoria pero con el fin de garantizar el interés público que existe en torno a la investigación de los delitos y la sanción a

los responsables, como otra manera de preservar los derechos y libertades fundamentales, con lo cual el Estado cumple de igual manera un deber de garantía. Desde ese contexto, el ordenamiento jurídico a través de la Constitución Política y las Leyes Procesales permiten la injerencia en el ámbito privado de las comunicaciones, cuya legitimidad y validez probatoria deriva de la existencia de determinados requisitos y presupuestos, que para el efecto se consideran estándares mínimos amparados por el principio de legalidad y del debido proceso. Los requisitos generales para que proceda la intervención en comunicaciones son los siguientes:

1. Que exista una ley interna que permita a la autoridad pública adoptar la medida de interceptación que implica una injerencia en el derecho al secreto de las comunicaciones e intimidad.

2. Que se autorice a través de Resolución Judicial, ya que la autoridad judicial es la única investida constitucionalmente para interferir el derecho al secreto de las comunicaciones, en el marco de la investigación penal o disciplinaria.

3. Observamos también con beneplácito como las empresas nacionales han pronosticado invertir más en sistemas de gestión de riesgos, entrenamiento del personal, controles financieros y herramientas de seguridad informática. El sistema judicial colombiano por ello no puede quedarse rezagado en implementar verdaderas políticas de seguridad en la información, pues a medida que pasa el tiempo los ficheros con los datos judiciales de los sub judice, estarán más expuestos y serán vulnerables para propósitos diferentes a las verdaderas políticas criminales del Estado. en el evento concreto el sacrificio del derecho. La motivación debe fundarse en la existencia de indicios de la comisión del delito, más allá de las sospechas o conjeturas (Justificación Fáctica), y en la debida ponderación del caso, a la luz del Principio de proporcionalidad (Juicio Jurídico), lo que comprende sólo las medidas que persigan un fin constitucionalmente legítimo, y resulten además necesarias, en cuanto no pueda acudirse a otro medio de investigación de menor incidencia para los derechos y libertades individuales; y proporcionales en sentido estricto, pues la restricción del derecho puede acordarse únicamente cuando se trate de investigar delitos graves, aspectos que más adelante serán explicados en detalle. A la luz de la doctrina Constitucional queda claro que la motivación resulta esencial, pues representa el vehículo que permite conocer las razones de la decisión judicial, y brinda la posibilidad, por tanto, de ejercer cabalmente el derecho de contradicción frente a la misma, como garantía de los sujetos investigados.

4. Existencia previa de un procedimiento de investigación penal y finalidad exclusivamente probatoria de las intervenciones que han de encaminarse a establecer la existencia del delito y el descubrimiento de las personas que puedan ser responsables del mismo. Con lo anterior, quedan proscritas las escuchas prospectivas o predelictivas, y de ahí que se exija, para la práctica de esta diligencia reservada, la existencia de un procedimiento en cualquiera de las modalidades que las leyes arbitran.

5. Exclusividad y concreción del hecho delictivo que se investiga, pues no resulta admisible decretar una intervención telefónica para descubrir indiscriminadamente la existencia de hechos delictivos.

6. Afectación de la medida tan solo a los teléfonos de las personas indiciariamente implicadas, ya sean titulares de los mismos o usuarios habituales.

7. Limitación temporal de la medida de interceptación, que no podrá aplicarse en forma indefinida o excesiva.

8. Control judicial previo, concomitante y posterior de la actividad que desarrolla la Policía Judicial con respecto a la intercepción, y entrega de los originales íntegros de las grabaciones al juez que autorizó la medida (Durán Climent, 1999, p. 957).

Para completar la validez probatoria de la mencionada intervención, al plano de referencia Constitucional antes descrito se añaden otros requisitos de legalidad ordinaria, tales como:

a) Entrega íntegra que ha de realizar la Policía Judicial a la autoridad de los soportes originales donde se hayan recogido las conversaciones detectadas.

b) Ofrecer a las partes la posibilidad de intervenir en la audición y selección de las grabaciones con relevancia probatoria, que van a ser utilizadas como medio de prueba en el Juicio Oral. De esta manera se garantizan los principios de publicidad, contradicción e inmediación de la prueba preconstituida.

c) En caso de duda sobre la identidad de las personas intervinientes en las conversaciones detectadas, resulta necesario ordenar la práctica de pruebas periciales u otras idóneas para completar el efecto probatorio del resultado de los escuchas (Durán Climent, 1999, p. 957).

Conforme al Artículo 15 de la Constitución Política, al Estado le corresponde respetar y velar porque no se vulnere el derecho a la intimidad personal y familiar; la correspondencia y demás formas de comunicación son inviolables y sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Es por esto que el Artículo 192 del Código Penal establece que quien ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de dieciséis a cincuenta y cuatro meses, siempre que la conducta no constituya delito sancionado con pena mayor. Junto a él, la norma penal procesal dispone en su Artículo 14 que toda persona tiene derecho al respeto de su intimidad.

Nadie podrá ser molestado en su vida privada. No podrán hacerse registros, allanamientos, ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este código. De la misma manera deberá procederse cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones.

Se tiene pues que una de las atribuciones de la Fiscalía General de la Nación es la de ordenar registros, allanamientos, incautaciones e interceptaciones de comunicaciones, y poner a disposición del juez de control de garantías los elementos recogidos para su control de legalidad. El fiscal podrá ordenar, con el único objeto de buscar elementos materiales probatorios y evidencia física, que se intercepten mediante grabación magnetofónica o similar a las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación.

En dicho escenario las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden. En todo caso, deberá fundamentarse por escrito, y las personas que participen en estas diligencias se obligan a guardar la debida reserva.

i) Derecho comparado

A raíz de los ataques a las torres gemelas, las organizaciones públicas y privadas se dieron cuenta de las múltiples falencias que poseían en cuanto a seguridad informática, por lo que han tratado de desarrollar mejores estrategias de seguridad, sin embargo, estas no han podido contrarrestar la gran mayoría de los ataques on line que se presentan en la actualidad.

Cabe resaltar que la situación latina frente a la norteamericana es totalmente diferente y que en esta primera, apenas hace unos años, tanto los gobiernos como las empresas tomaron cartas en el asunto, aunque no del modo que se debiera. Al respecto explica Jeimy Cano (Septiembre de 2001):

> Las organizaciones han adelantado análisis de su seguridad, instalado múltiples mecanismos de protección y efectuado múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad de una intrusión o incidente.

Asimismo, es tan poca la importancia que se le da a la seguridad informática que las mismas aseguradoras no consideran dentro de sus pólizas de seguro a los ataques informáticos actuales, pues estas establecen cláusulas para los bancos y demás entidades con base en elementos tecnológicos de hace veinte años.

Cano explica que estas cláusulas aseguran y se refieren a pérdidas de información, transferencias de mensajes vía telex, conexiones por fax o vía telefónica y otras modalidades que ya no son funcionales para los atacantes virtuales; mientras que el phishing, la manipulación de la página web, el robo de identidad y la suplantación, los nuevos y poderosos delitos informáticos, no son cubiertos por las pólizas que ofrecen en la actualidad los entes aseguradores.

Estos dos casos de desconocimiento, tanto de las empresas como de las aseguradoras, reflejan que Colombia, al igual que otros países latinos, no está del todo consciente de lo poderosos que son los ataques virtuales de los hackers del país, quienes cuentan con toda la tecnología y el conocimiento para engañar y estafar.

Cabe aclarar que Colombia está preparada humana y tecnológicamente para enfrentar los ataques informáticos y capturar a los culpables, sin embargo, la legislación del país y el poco compromiso y confianza de las empresas dificulta el proceso, ya que muchos de los casos reportados por las diferentes organizaciones no son analizados por la falta de información y conocimiento del área.

La ley colombiana no define el delito informático como tal, lo que sí ha hecho es regular ciertos casos como acceso abusivo a redes y otros delitos derivados de corrientes internacionales. Es importante tener en cuenta que, sin perjuicio de que exista o no una definición de que es o que no es un delito informático, el Código Penal y el Código de Procedimiento Penal traen definidos, delimitados y regulados muchísimos delitos que son susceptibles de ser cometidos en un entorno informático.

No obstante lo incipiente del tema y los esfuerzos nacionales e internacionales por especializar las fuentes normativas y las autoridades competentes, en el Derecho Comparado se encuentran amplios ejemplos de Estados que han dado mayor desarrollo a estas figuras. A continuación nos aproximaremos a algunas experiencias internacionales y se presentará un mapa de la evolución histórica que ha tenido la ciencia forense desde 1850 al siglo XXI, donde se denota la evolución comportamental de la sociedad como ha hecho que la ciencias forenses deban evolucionar y responder a nuevas formas de comportamiento delictual:.

Mapa 1 – Evolución de la Ciencia Forense 1850 - Siglo XXI (no hay autor conocido y el sitio de consulta desapareció de la web), (se le advierte al lector que el mapa se encuentra dividido en dos secciones consecutivas Pág. 87 y 88):

PROLIFERATING SPECIALTIES

Prior to 1850

IN THE EARLY 1800S, FORENSIC MEDICINE WAS NOT DIVIDED INTO DISTINCT DISCIPLINES. Physicians and surgeons who performed autopsies and testified in court depended on a variety of sources for their income and provided expertise as needed. No regular system of payment was provided for expert testimony, laboratory analysis, or postmortem examination. Toxicology and forensic pathology were just emerging as distinct fields, and most autopsies were performed by physicians without any special training.

Today, forensics includes many disciplines, with dozens of specialties and subspecialties drawing on expanding scientific knowledge and technological expertise.

PROFESSIONAL SPECIALTIES

There were very few occupations dedicated solely to forensic pursuits.

I. Coroner

II. Coroner's Physician/ Surgeon

ANALYTICAL & ACADEMIC SPECIALTIES

There were no scientific societies or technical positions dedicated solely to forensic work. Anatomical academics and scientists provided forensic analysis on occasion.

I. Professor of Medical Jurisprudence

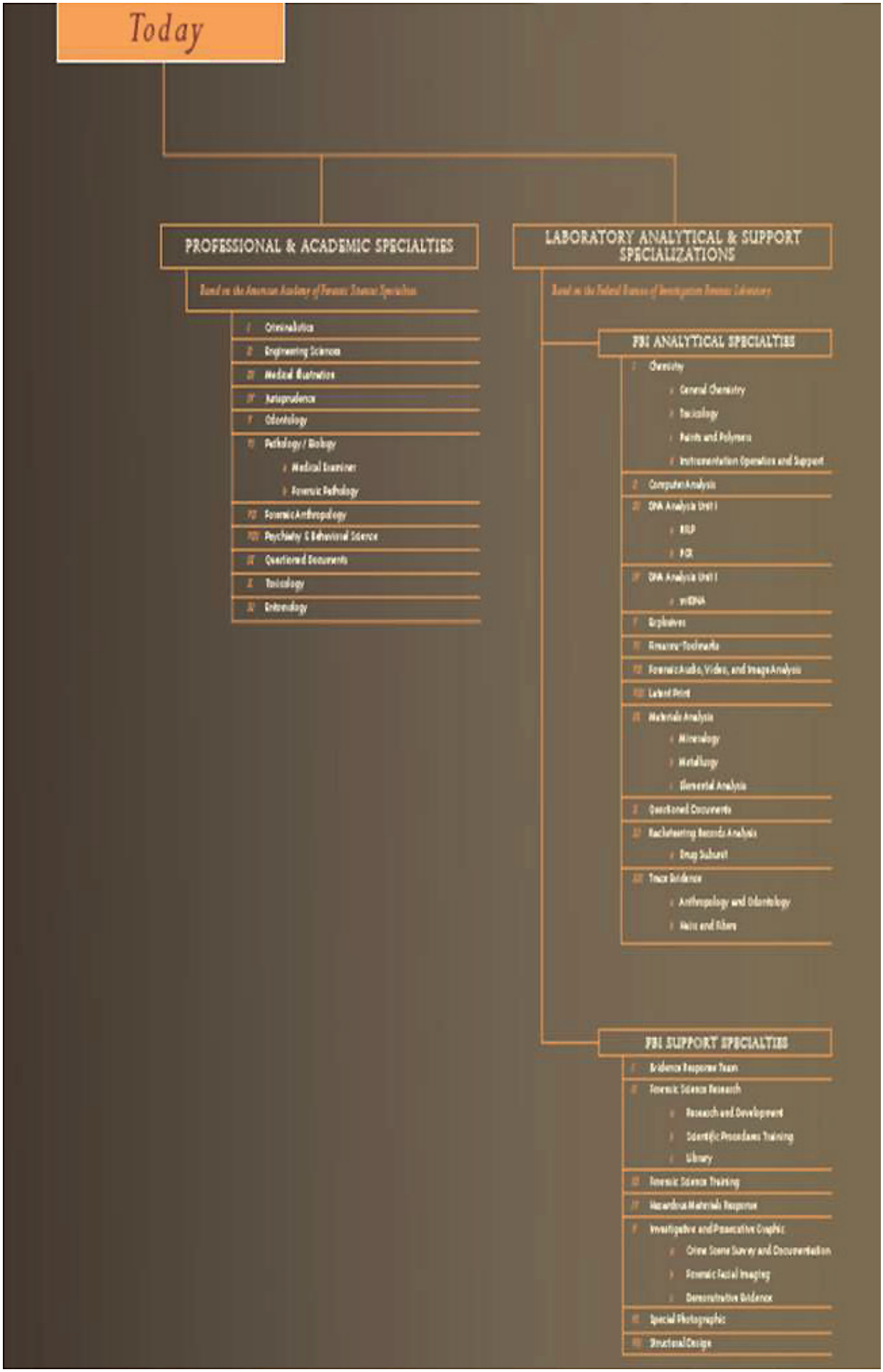
II. Pathological Anatomist

- Professor of Anatomy or Pathological Anatomy

III. Toxicologist

- Professor of Toxicology, Medical Chemistry or Materia Medica

IV. Examining Physician/ Surgeon


Today
PROFESSIONAL & ACADEMIC SPECIALTIES
Based on the American Academy of Forensic Science Specialties
Criminalistics
Engineering Sciences
Medical Illustration
Jurisprudence
Odontology
Pathology / Biology
Medical Examiner
Forensic Pathology
Forensic Anthropology
Psychiatry & Behavioral Science
Questioned Documents
Toxicology
Entomology
LABORATORY ANALYTICAL & SUPPORT SPECIALIZATIONS
Based on the Federal Bureau of Investigation Forensic Laboratory
FBI ANALYTICAL SPECIALTIES
Chemistry
General Chemistry
Toxicology
Paints and Polymers
Instrumentation Operation and Support
Computer Analysis
DNA Analysis Unit I
RFLP
PCR
DNA Analysis Unit II
mtDNA
Explosives
Firearms-Toolmarks
Forensic Audio, Video, and Image Analysis
Latent Print
Materials Analysis
Mineralogy
Metallurgy
Elemental Analysis
Questioned Documents
Racketeering Records Analysis
Drug Subunit
Trace Evidence
Anthropology and Odontology
Hairs and Fibers
FBI SUPPORT SPECIALTIES
Evidence Response Team
Forensic Science Research
Research and Development
Scientific Procedures Training
Library
Forensic Science Training
Hazardous Materials Response
Investigative and Prosecutive Graphics
Crime Scene Survey and Documentation
Forensic Facial Imaging
Demonstrative Evidence
Special Photographic
Structural Design

España

Noelia García Noguera (julio de 2002) explica que en España el Código Penal de 1995 ha introducido nuevas figuras y modalidades delictivas. Son ellas el descubrimiento y revelación de datos (Artículo 197),[5] daños informáticos o sabotaje (Artículo 264)[6] y el espionaje informático (Artículo 278).[7]

Relacionado con el primero, explica García Noguera que se trata de un delito contra la intimidad, lo cual no había sido previsto en las modalidades comisivas relacionadas con el uso de tecnologías de la información dirigidas a sobrepasar la intimidad de las personas o para violar, acceder o descubrir sus secretos.

Conforme a la disposición referente al daño informático o sabotaje, debe resaltarse cómo el objeto material del mencionado tipo penal se constituye por datos, programas o documentos electrónicos ajenos, esto es, de propiedad de un tercero, contenido o depositado en redes, soportes o sistemas informáticos. Esos datos no pueden ser leídos o percibidos de forma directa, exigiendo la intervención de máquinas y soportes capaces de interpretar las señales digitales que lo integran.

En el denominado espionaje informático empresarial el bien jurídico protegido es el secreto empresarial, la información almacenada informáticamente que supone un valor económico para la empresa porque confiere al titular una posición ventajosa en el mercado respecto de las demás empresas que desarrollan la actividad o una similar.

En el caso de destrucción, alteración, inutilización u otra modalidad de daño de datos, programas o documentos electrónicos de un individuo que reposen en redes, soportes o sistemas informáticos. Se trata de los daños causados en el sistema informático mediante la introducción de virus y bom-

[5] "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

[6] "1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a dos años.
2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años.
3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1. Se hubiese cometido en el marco de una organización criminal. 2. Haya ocasionado daños de especial gravedad o afectado a los intereses generales.
4. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrán las siguientes penas: a. Multa del doble al cuádruple del perjuicio causado, si el delito cometido por la persona física tiene prevista una pena de prisión de más de dos años. B. Multa del doble al triple del perjuicio causado, en el resto de los casos. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b a g del apartado 7 del artículo 33".

[7] "1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos".

bas lógicas. Explica Noguera (abril de 2001) que el código penal anterior sólo preveía la destrucción de bienes materiales, por lo que los daños causados a bienes inmateriales no estaban incluidos en este delito.

Los delitos descritos se encuentran en el Código Penal de España; los tipos denominados delitos contra la propiedad industrial (Artículo 273),[8] publicidad ilícita (Artículo 282),[9] falsedad de documento público (Artículo 390), falsedad de documento privado (Artículo 395),[10] pornografía infantil (Artículo 189)[11] caso en el que se incluye la expresión "el que por cualquier medio", con el fin de incluir Internet como medio para cometer este delito.

Adicionalmente, exalta Noelia García Noguera, son delitos tradicionales vigentes de posible comisión por medios informáticos la difusión y exhibición de material pornográfico a menores (Artículo

[8] "1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos. 2. Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.
3. Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados en favor de tercero por un modelo o dibujo industrial o artístico o topografía de un producto semiconductor".

[9] " Los que, como administradores de hecho o de derecho de una sociedad emisora de valores negociados en los mercados de valores, falsearan la información económico-financiera contenida en los folletos de emisión de cualesquiera instrumentos financieros o las informaciones que la sociedad debe publicar y difundir conforme a la legislación del mercado de valores sobre sus recursos, actividades y negocios presentes y futuros, con el propósito de captar inversores o depositantes, colocar cualquier tipo de activo financiero, u obtener financiación por cualquier medio, serán castigados con la pena de prisión de uno a cuatro años, sin perjuicio de lo dispuesto en el artículo 308 de este Código.
En el supuesto de que se llegue a obtener la inversión, el depósito, la colocación del activo o la financiación, con perjuicio para el inversor, depositante, adquiriente de los activos financieros o acreedor, se impondrá la pena en la mitad superior. Si el perjuicio causado fuera de notoria gravedad, la pena a imponer será de uno a seis años de prisión y multa de seis a doce meses".

[10] "El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390, será castigado con la pena de prisión de seis meses a dos años".

[11] "1. Será castigado con la pena de prisión de uno a cinco años: a. El que captare o utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas. b. El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.
2. El que para su propio uso posea material pornográfico en cuya elaboración se hubieran utilizado menores de edad o incapaces, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.
3. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes: a. Cuando se utilicen a niños menores de 13 años. b. Cuando los hechos revistan un carácter particularmente degradante o vejatorio. c. Cuando los hechos revistan especial gravedad atendiendo al valor económico del material pornográfico. d. Cuando el material pornográfico represente a niños o a incapaces que son víctimas de violencia física o sexual. e. Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades. f. Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho o de derecho, del menor o incapaz.
4. El que haga participar a un menor o incapaz en un comportamiento de naturaleza sexual que perjudique la evolución o desarrollo de la personalidad de éste, será castigado con la pena de prisión de seis meses a un año.
Observamos también con beneplácito como las empresas nacionales han pronosticado invertir más en sistemas de gestión de riesgos, entrenamiento del personal, controles financieros y herramientas de seguridad informática. El sistema judicial colombiano por ello no puede quedarse rezagado en implementar verdaderas políticas de seguridad en la información, pues a medida que pasa el tiempo los ficheros con los datos judiciales de los sub judice, estarán más expuestos y serán vulnerables para propósitos diferentes a las verdaderas políticas criminales del Estado.
5. El que tuviere bajo su potestad, tutela, guarda o acogimiento, a un menor de edad o incapaz, y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o incapaz, será castigado con la pena de prisión de tres a seis meses o multa de seis a 12 meses.
6. El ministerio fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.
7. Será castigado con la pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada".

186) que penaliza el hecho de exhibir material pornográfico a menores a través de cualquier medio, por ejemplo el correo electrónico. Figuran también la calumnia (artículos 205 y 206) y la injuria (artículos 208 y 209) los cuales son realizables por medio de correo electrónico.

También existe el delito por calumnias e injurias hechas con publicidad (Artículo 211), con la difusión de mensajes injuriosos o calumniosos a través de Internet; el robo (Artículo 237) que implica el uso de la fuerza en las cosas, a lo cual parte de la doctrina estima que no es posible el delito de robo ni de hurto de datos porque no tienen naturaleza corpórea, tangible y no son susceptibles de aprehensión. García Noguero incluye también las defraudaciones de fluido eléctrico (Artículo 255) al usar energía eléctrica, gas, agua, telecomunicaciones (televisión, teléfono, etc.) u otro elemento, energía o fluido ajenos; la defraudación a través de equipo terminal de comunicaciones (Artículo 256) que se dirige al uso no autorizado o abusivo de terminales de telecomunicaciones ocasionando un perjuicio superior a trescientos euros, y finalmente los delitos contra la propiedad intelectual (Artículo 270).

Argentina

Por medio de la Ley 26.388 de 2008, la legislación argentina incorpora nuevas disposiciones en torno a las modalidades delictivas informáticas. Sin que sea una ley especial, la Ley 26.388 de 2008 hace una modificación a varios tipos penales vigentes en el Código Penal argentino, incorporando apartados que regulan las nuevas modalidades conductuales.

Los delitos dispuestos son: pornografía infantil por Internet u otros medios electrónicos (Artículo 128),[12] violación, apoderamiento y desvío de comunicación electrónica (Artículo 153, párrafo 1),[13] intercepción o captación de comunicaciones electrónicas o telecomunicaciones (Artículo 153, párrafo 2º), acceso a un sistema o dato informático (Artículo 153),[14] publicación de una comunicación

[12] "Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

[13] "Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena".

[14] "Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

electrónica (Artículo 155),[15] acceso a un banco de datos personales (Artículo 157 (bis), párrafo 1º), revelación de información registrada en un banco de datos personales (Artículo 157 (bis), párrafo 2º),[16] inserción de datos falsos en un archivo de datos personales (Artículo 157 (bis), párrafo 2º CP, anteriormente regulado en el Artículo 117 (bis) (párrafo 1º, incorporado por la Ley de Hábeas Data);[17] fraude informático (Artículo 173, inciso 16), daño o sabotaje informático (Artículos 183 y 184, incisos 5º y 6º).

Vale destacar como, de los tipos penales mencionados, la legislación colombiana se iguala en varios de ellos, como es el caso del tipo penal de interceptación o captación de comunicaciones electrónicas o telecomunicaciones, caso en el cual el tipo en Colombia se limita al verbo de interceptación así como a los datos informáticos como objeto sobre el cual recae la acción delictiva.

De igual forma dispone la nueva legislación argentina el acceso a un sistema o dato informático, el cual en el caso colombiano debe cargar con la naturaleza de ser abusivo, mientras que la legislación del país austral contempla la acción de abrir un sistema informático de forma indebida, ampliando los soportes de acceso o apertura a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza.

Finalmente, dos tipos penales más pueden ser mencionados en este ejercicio de comparación legislativa entre los dos ordenamientos jurídicos en estudio: la violación de datos personales en el caso colombiano y el delito de revelación de información registrada en un banco de datos personales, y el daño informático o daño o sabotaje informático en el caso argentino.

En el caso del primero, la nueva norma argentina dispone: “El que (…) ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley” frente a: “El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes”; donde ambos pueden recaer sobre un sujeto común o cualificado. Ambos parten de un supuesto común que se

[15] “Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público”.

[16] Observamos también con beneplácito cómo las empresas nacionales han pronosticado invertir más en sistemas de gestión de riesgos, entrenamiento del personal, controles financieros y herramientas de seguridad informática. El sistema judicial colombiano por ello no puede quedarse rezagado en implementar verdaderas políticas de seguridad en la información, pues a medida que pasa el tiempo los ficheros con los datos judiciales de los sub judice, estarán más expuestos y serán vulnerables para propósitos diferentes a las verdaderas políticas criminales del Estado. “Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos”.

[17] “Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años”.

expresa de forma diversa consistente en la comisión de la conducta por parte del sujeto activo desde una postura de ilegitimidad o desautorización.

Sin embargo, es mucho más amplia y englobante la disposición colombiana, que con mayor cantidad de verbos traza finalidades conductuales que quedan sometidas al imperio de la regulación legal, superando la esfera argentina meramente concentrada en la revelación o proporción de datos, esto es, de darlos a conocer a un tercero.

Frente al daño o sabotaje informático es importante destacar parte del análisis doctrinario generado en torno al tipo penal. Dispuesto en el Artículo 10 de la Ley 26.388 de 2008, la norma señala: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

Martín Carranza Torres y Horacio Bruera mencionan que el motivo por el cual se promovió esta disposición estaba claramente enunciado en el texto del Artículo 183 del Código Penal, que tipificaba el delito de daño en general, el cual era sólo aplicable cuando la acción dañosa recayera sobre un bien tangible, no cuando lo hiciera sobre un bien intangible, y tanto los datos como el software encuadran en esta última categoría. Según los Fundamentos del Proyecto de Ley la figura de daño tal como estaba tipificada en el Artículo 183 no es aplicable al daño informático.

Para tener mayor claridad sobre este punto resulta conveniente transcribir el mencionado Artículo 183, que dice lo siguiente: "Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado".

Señalan los autores citados que lo mismo se daba en caso de la aplicación de la figura de estafa al fraude informático, siendo lo correcto afirmar que el Artículo 183 no fuera aplicable al daño informático, sino que, tal como estaba redactado, no era claro que lo fuera, y como en materia penal rige el principio de legalidad y la prohibición de la analogía, esa falta de claridad da lugar a interpretaciones encontradas.

También de la doctrina argentina se identificó un importante trabajo relacionado con algunos parámetros probatorios en casos de comisión de delitos informáticos. Claudio Alejandro Fernández (noviembre de 2002), en su texto *Delitos y tecnología de la información. Prueba pericial delitos y tecnología de la información características y valoración en el proceso penal argentino,* retoma el contexto problematizador aquí ya mencionado, en el cual, las nuevas dinámicas globales y la acelerada evolución de la tecnología al servicio de la humanidad se traducen en una realidad de vulnerabilidad e inseguridad para gran cantidad de actividades humanas.

Dice que la tecnología delimita en la informática el medio para el manejo de la información que es posible dominar desde diversas modalidades, siendo el bien jurídico sujeto a posibles afectaciones y atentados criminales. En ello encuentra las siguientes observaciones:

Existe la generalizada creencia de que este sistema, entendido como "un conjunto único y ordenado cuyos componentes son coherentes y solidarios entre sí" es, a su vez, falible, pues al basarse en razonamientos inductivos que no abarcan la generalidad de los casos los resultados son, en esencia, falibles; no obstante ello, la base técnica de análisis es tan confiable como la de otras disciplinas criminalísticas que hoy no merecen cuestionamiento. Si bien este principio general es aplicable a la totalidad de la actividad pericial, la incidencia de la falibilidad en cuanto a la valoración jurisdiccional de los resultados adquiere especial relevancia por diversas razones:

- Existe un generalizado desconocimiento respecto de las modificaciones tecnológicas.
- La exposición de resultados, por su intangibilidad, elevado nivel de abstracción y terminología técnica, resulta sumamente dificultoso.
- La inexistencia de apoyo jurisprudencial suficiente, que permite al juzgador moverse sobre bases más o menos seguras, fundadas en la experiencia judicial, tal como ocurre con otras disciplinas criminalísticas.

De forma particular, el análisis realizado sobre la normativa generada en el ordenamiento jurídico argentino coincide con las apreciaciones que se han generado desde la experiencia colombiana. Los ordenamientos jurídicos nacionales se han esforzado por cumplir con la actualización de sus disposiciones frente a esta nueva modalidad delictual, y los trabajos por tipificar de manera puntual y certera esas conductas han degenerado en varios delitos que mantienen vigencia dentro de cada estructura legislativa. No obstante, aún no se evidencia la eficacia de los mismos, como tampoco una actividad y apreciación segura de cada figura que dé cuenta de su comprensión, aprehensión, interpretación y sentido.

Siguiendo el mismo sentido de Fernández (noviembre de 2002), los delitos informáticos comienzan a arrojar elementos para aseverar su existencia, conveniente tipificación, su función garantizadora y valorativa, pero su desprovista base probatoria y técnica que acredite su comisión. Desde la ausencia de jurisprudencia, la abstracción del tema y la carencia de comprensión son debilidades que pueden comenzar a ser subsanadas desde la formación y el ejercicio de especialistas en la materia.

> De la aplicación práctica del conocimiento específico se desprende la existencia de tres grandes campos de la labor pericial que podrían definirse como: a) pericias de autenticidad b) pericias de contenido, funcionamiento y recuperación de datos y c) pericias sobre internet. En el primero de los casos nos encontraríamos ante la necesidad de tener a disposición el patrón material de comparación, ya sea de 'hard' o 'soft', entendido como 'indubitable' que permitirá el análisis comparativo

determinante de la autenticidad o no del elemento sospechado. En segundo término, el espectro es mucho más amplio pues, abarca tan diversos aspectos como el almacenamiento de datos, el análisis y determinación de estructuras de diseño de sistemas, la medios de comunicación y transferencia de datos, métodos de entrada, acceso, procesamiento y salidas, etc. que en su conjunto requieren la colaboración interdisciplinaria de profesionales en la materia. Y por último, la investigación de ilícitos cometidos a través de la www o bien mediante redes privadas o BBS constituyen un constante desafío para el profesional informático que lo obliga a poseer y mantener permanentemente actualizadas las más modernas herramientas (software) para la detección de intrusiones en sistemas remotos, utilización indebida del correo electrónico, etc. (…) Como ya expresara, la volatilidad de los datos en lo que a prueba informática se refiere exige las máximas precauciones a la hora de obtener el corpus instrumentorum. Dicha actividad comienza desde el momento del allanamiento mismo. Los métodos tradicionales de búsqueda y el hallazgo de la prueba en todas las investigaciones, no resultan suficiente para el éxito en los procedimientos por delitos informáticos. Aquello que se halló en el lugar del hecho, debe ser exactamente lo que llegue al ámbito del perito, para su análisis y dictamen.

No escapa a la lógica más simple suponer que, al procederse el diligenciamiento de una orden de allanamiento, quienes resultan afectados y, de alguna manera se saben partícipes de una actividad delictual, intentarán por todos los medios evitar que los funcionarios intervinientes obtengan elementos probatorios que pudieren incriminarlos. Partiendo de esta natural reticencia a que prospere la medida judicial, debe tenerse en cuenta que, cuando aquello que resulta de interés se halla almacenado en computadoras, por lo general, sus operadores conocen las rutinas que deben llevarse a cabo rápidamente para eliminar los registros comprometedores o bien inutilizar completamente los sistemas.

Atento a ello, a fin de no echar por tierra la labor investigativa previa es menester como primera medida disponer el alejamiento de toda persona que se halle en presencia de los computadores, servidores o tableros de suministro eléctrico, para proceder, inmediatamente a desconectar la totalidad de los teclados hasta que cada uno de los terminales sea examinados por los expertos.

Francia

Conocida como la “loi Godfrain”, la Ley 88-19 de 1988 es en Francia la disposición que da inicio a la regulación de los delitos informáticos. Con dicha legislación el país galo creó las normas relativas al fraude informático, incluyendo un nuevo Capítulo del Código Penal, bajo la denominación o titulación “Sobre ciertas infracciones en materia informática”.

Aquellas disposiciones implican una diferenciación aclaratoria de las nuevas normas previstas, pues el uso reiterado del término “informatisé” (informatizado) sobre el de “informatique” (informático) generó para la opinión de especialistas la idea de que el legislador se ha preocupado por proteger la información en su conjunto y no sólo aquella en soporte informático, es decir, que su preocupación se ha centrado en las conductas fraudulentas de acceso y uso ilícito de los sistemas de tratamiento automatizado de datos, absteniéndose de regular las manipulaciones informáticas con ánimo de lucro y en perjuicio patrimonial de tercero, núcleo principal del fraude informático.

Por ello se enfrenta una aparente ambigüedad entre el título del Código Penal frente a la situación hipotética creada por medio de la tipología dispuesta, pues el título de la ley se refiere al fraude informático sin que en el enunciado aparezca referencia específica al mismo. Se debe aclarar que la norma se dirige a la falsedad informática sólo en los supuestos que el dato alterado se encuentre sobre un soporte informático.

Desde la jurisprudencia de la Corte de Casación de Francia se estimó que las defraudaciones patrimoniales por medios informáticos quedan por esa disposición sin regulación alguna, pues aquellas venían siempre subsumidas en la figura clásica de estafa del Artículo 405 del Código Penal, que sanciona al que,

> Haciendo uso de falsos nombres o de falsas cualidades, bien empleando maniobras fraudulentas para simular la existencia de falsas empresas, de un poder o crédito imaginario, o por hacer nacer la esperanza o la creencia de un suceso, de un accidente o de cualquier otro acontecimiento imaginario, se haya hecho reintegrar o traspasar, o hubiera intentado hacerse reintegrar o traspasar fondos, muebles, obligaciones, disposiciones, billetes, promesas, deducciones o desgravaciones, y hubiera por uno de estos medios, defraudado o intentado defraudar la totalidad o parte de la fortuna de otro (Biblioteca del Congreso Nacional de Chile, 2004, p. 35).

La subsumisión es posible al recogerse en la descripción de la conducta típica la cláusula "maniobras fraudulentas" y el "perjuicio", debiéndose entender estas como formas de engaño, siendo las manipulaciones informáticas integrables en aquellas, y la omisión del texto a referencias genéricas sobre el "engaño", el "error" y al "acto de disposición" (Biblioteca del Congreso Nacional de Chile, 2004, p. 35).

> Según la doctrina de Francia, la ley de reforma se concibe materialmente como una vía para reprimir accesos abusivos a los sistemas informáticos y actuaciones ilícitas sobre datos informatizados y su tratamiento, se produzca o no perjuicio, lo que implica el rechazo expreso en el parlamento de las propuestas de subsumir las agresiones patrimoniales por medios informáticos en los tipos recogidos por esta ley. La reforma penal de 1992, Ley 92-683, vigente a partir de marzo de 1994, introdujo cambios en el texto legal de las disposiciones informáticas y las trasladó a otra parte del Código, esto es, al "Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos". La falsificación informática que estaba regulada en los artículos 462-5 y 462-6, sobre la falsificación y uso de documentos electrónicos falsificados, actualmente se encuentra en el nuevo Artículo 441-1, que se refiere a todas las posibles formas de un documento, incluyendo el electrónico. El acceso fraudulento en sistemas informáticos se encuentra en el actual 323-1, sabotaje informático en el Artículo 323-2 (Biblioteca del Congreso Nacional de Chile, 2004, p. 35).

Italia

El Código Penal de este país dispone una amplia gama de tipos penales en materia informática. Iniciando por el acceso abusivo a un sistema informático o telemático, la legislación italiana se equipara en ese tipo penal a la creada en Colombia, con una diferencia inicial identificada en el acceso abusivo al sistema telemático, algo no contemplado por el tipo penal nacional. Consagrado en el Artículo 615, la modalidad de acceso abusivo se configura de manera exclusiva en sistemas informáticos o telemáticos protegidos, y estar protegidos implica contar con dispositivos de seguridad representados en contraseñas o llaves de hardware que destacan e identifican la privacidad del sistema y la voluntad de su titular de reservar el acceso al mismo sólo a aquellas personas que él faculte.

Seguidamente, dispone la ley italiana la "difusión de programas dirigidos a producir daños o interrumpir un sistema informático o telemático (Artículo 615 quinto) el atentado contra un sistema informático o telemático de utilidad pública (Artículo 420) donde reaparece el interés público que figura como agravante de punibilidad en Colombia; el abuso de la calidad de operador de sistema, el cual se estima como un" agravante del delito de acceso abusivo por quedar dispuesto para su comisión a quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de comisión del delito.

"Se disponen también la detentación y difusión abusiva de códigos de acceso a sistemas informáticos o telemáticos (Artículo 615 cuarto), la difusión de programas dirigidos a dañar o interrumpir un sistema informático (Artículo 615 quinto), la violación de la correspondencia electrónica (Artículo 616) y la ya mencionada intercepción abusiva. (Artículo 617, cuarto, quinto). Este último tipo penal por la relevancia que tiene en el caso colombiano, se explica a la luz de las normas italianas en consonancia a la naturaleza de los delitos" de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. Incluyendo además de la interceptación de sistema informático la posibilidad de su tipificación por interceptación de sistema telemático, el delito es explicado desde la acción de intercepción fraudulenta, impedimento o intrusión de comunicaciones relativas a los citados sistemas informáticos o además de la revelación al público, de todo o parte, por cualquier medio del contenido de la comunicación.

Finalizan las disposiciones normativas del Código Penal de Italia con la falsificación informática (Artículo 617 sexto) entendido como la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas; el espionaje informático, el fraude informático (Artículo 640 tercero) y el ejercicio arbitrario de la propia razón con violencia sobre programas informáticos (Artículo 392).

REFERENTES TEÓRICOS

CAPÍTULO 4.

MIRADA HOLÍSTICA A LA INFORMÁTICA FORENSE EN COLOMBIA[1]

Ana María Mesa Elneser

Juan David Pineda Cárdenas

Juan Guillermo Lalinde Pulido

Es imposible que un criminal actúe, especialmente en la tensión de la acción criminal, sin dejar rastros de su presencia (Manuel de Technique Policière)

Siempre que dos objetos entran en contacto, transfieren parte del material que incorporan entre ellos (Edmon Locard, 1877 - 1966)[2]

[1] Ver Mapa 1 (Anexos): en este gráfico se explica la evolución histórica de la ciencia forense desde la medicina y sus diferentes disciplinas. Es de allí de donde surge, por la necesidad investigativa del comportamiento social, la disciplina forense digital.

[2] Criminalista francés. Este principio es aplicado como fundamento de la investigación en materia de ciencias forenses, es por ello que la premisa de un investigador siempre se fundamenta en el rastro, toda vez que el victimario al ponerse en contacto con la escena del crimen siempre deja una evidencia y sólo le queda al investigador hallarla por medio de la aplicación de técnicas y protocolos forenses, y su experiencia para el tratamiento de la escena.

En la comunidad científica se ha pensado que la aplicación del *Principio de Transferencia* de Edmon Locard, como principio universal de las ciencias forenses, da sentido a la investigación científica criminal, ya que el trabajo criminal de un delincuente exige su presencia física y por lo tanto deja rastro; otra cosa es su aplicación en la disciplina forense digital, pues su campo de acción en la escena de un cribercrimen imprime retos a la investigación científica porque el trabajo criminal es digital, no existe presencia física del sujeto sino transmisiones de datos, emisiones electromagnéticas, impulsos eléctricos, entre otros.

Por lo anterior, para su validación frente a la disciplina forense digital, este principio es reinterpretado, a fin de ser aplicado en el campo de la *computación forense,* toda vez que su formulación objetiva y estática aparentemente parece no ser posible, sin embargo, los expertos de la computación forense (entiéndase sinonimia con la informática forense) han determinado que la aplicación del principio sí se presenta, teniendo en cuenta que existe una *evidencia* la cual fundamenta la escena del crimen, la cual involucra una *víctima* y un *sospechoso,* donde la escena del crimen presenta *las alertas de los equipos monitoreados,* frente a la víctima se evidencia en la *traza de ficheros,* es decir, se requiere el análisis de toda la actividad y eventos que ocurren en nuestro equipo y se encuentran almacenando, en cuanto al *sospechoso,* lo evidencia el histórico de las últimas conexiones, finalmente, de ambos sujetos y como fundamento de la evidencia digital, los ficheros o archivos, son obtenidos y validados bajo el mismo valor hash (Bonilla, 2009).

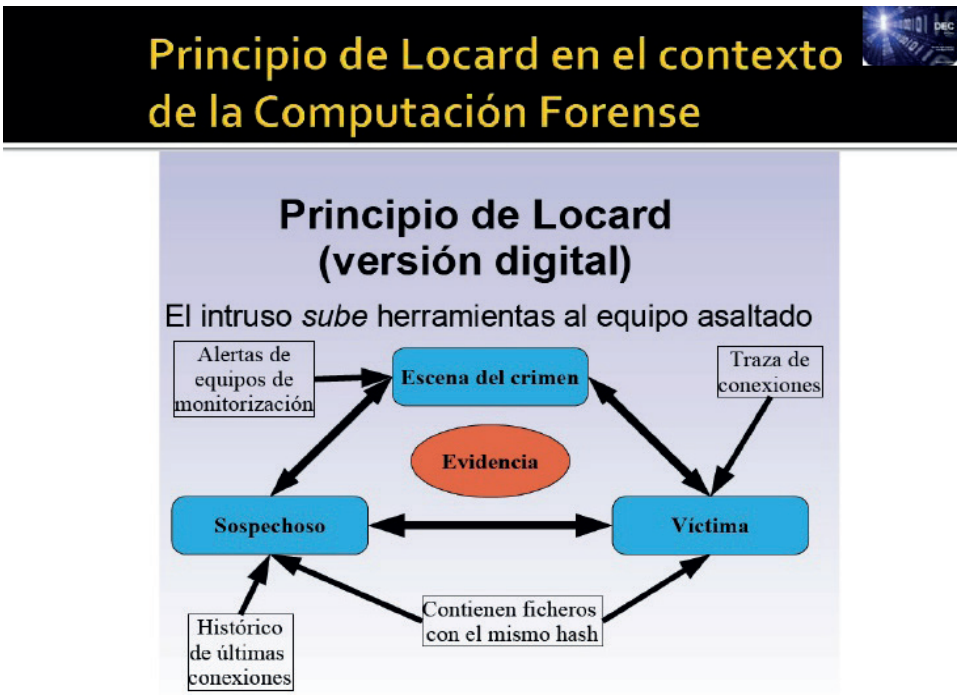


Imagen Diagrama: http://www.slideshare.net/joseber/computacin-forense, Autor Jorge Ebert Bonilla O. MSc. Creado 8 noviembre 2009. Consulta 15 febrero 2012.

Para abordar la estructura de este capítulo se iniciará con la identificación de las pruebas que involucran el mundo digital que son: *prueba pericial, testimonial, documental,* de forma principal, sin

que por ello se puedan excluir los demás medios de prueba, sin embargo, son de más difícil aplicación para el campo digital, lo cual merece una investigación diferente a la ejecutada en el proyecto. Posteriormente se hará un análisis a los aspectos más relevantes del perito forense digital, los laboratorios forenses digitales, protocolos, herramientas e instituciones forenses digitales, y finalmente los informes forenses digitales.

En Colombia existe libertad probatoria,[3] donde se validan medios probatorios debidamente regulados en el estatuto o en su defecto, previendo la evolución tecnológica, científica y disciplinar constante, se admiten medios de prueba no contemplados en el estatuto, siempre y cuando estos no violen los derechos humanos, fundamento legal que valida la existencia de la *evidencia digital* como medio probatorio válido y eficaz en Colombia.

Para el campo de la informática forense el medio de prueba *pericial* se valida con otros elementos de tipo *documental,* que permiten fortalecer el informe pericial dictaminado por el experto forense digital, y finalmente, la prueba *testimonial,* que es el medio probatorio que permite al experto sustentar ante el juez control de garantías y el juez de conocimiento su informe, donde logra certificar el protocolo y las herramientas forenses aplicadas para la obtención de la evidencia digital y permite la demostración de que la técnica forense aplicada valida las características fundamentales de la evidencia digital que son: autenticidad, originalidad, confiabilidad, integridad y no repudio.

Pruebas pertinentes en un caso penal

a) Prueba pericial

La Ley 906 de 2004, estatuto procesal penal vigente, regula en los Artículos 405 y subsiguientes la prueba pericial, teniendo en cuenta aspectos fundamentales para su contrastación con la informática forense, lo regulado en los siguientes artículos dice:

> Artículo 405: *Procedencia.* La prueba pericial es procedente cuando sea necesario efectuar valoraciones que requieran conocimientos científicos, técnicos, artísticos o especializados. Al perito le serán aplicables, en lo que corresponda, las reglas del testimonio (Congreso de Colombia, 2004).

Es por ello que la evidencia digital se entiende incluida de forma tácita en el estatuto procesal penal, sin que por esto se pueda manifestar que cuando en la norma se expresa de forma clara "evidencia física", sería más pertinente que la norma indicara igualmente evidencia digital, lo cual presentaría menos errores y ambigüedades en la interpretación y aplicación normativa. Lo importante para la aplicación de la prueba pericial, para el campo digital, es que el perito sea realmente competente para ello, toda vez que su inexperiencia puede generar, como efecto, en muchos de los casos, la exclusión de la prueba por falta de técnica pertinente o sustento científico, o en el escenario más complejo, que se decrete la nulidad de esta y no sólo la exclusión.

[3] Artículo 373: *Libertad.* Los hechos y circunstancias de interés para la solución correcta del caso se podrán probar por cualquiera de los medios establecidos en este código o por cualquier otro medio técnico o científico, que no viole los derechos humanos.

> Artículo 406: *Prestación del servicio de peritos.* El servicio de peritos se prestará por los expertos de la policía judicial, del Instituto Nacional de Medicina Legal y Ciencias Forenses, entidades públicas o privadas, y particulares especializados en la materia de que se trate. Las investigaciones o los análisis se realizarán por el perito o los peritos, según el caso. El informe será firmado por quienes hubieren intervenido en la parte que les corresponda. Todos los peritos deberán rendir su dictamen bajo la gravedad del juramento (Congreso de Colombia, 2004).

Frente a este artículo vale destacar que la norma de forma directa está validando la legalidad de una prueba pericial por expertos forenses del campo privado, la legalidad de su informe y la legalidad de laboratorios donde desarrolla su experticio.

> Artículo 408: *Quiénes pueden ser peritos.* Podrán ser peritos, los siguientes:
>
> 1. Las personas con título legalmente reconocido en la respectiva ciencia, técnica o arte.
>
> 2. En circunstancias diferentes, podrán ser nombradas las personas de reconocido entendimiento en la respectiva ciencia, técnica, arte, oficio o afición aunque se carezca de título.
>
> A los efectos de la cualificación podrán utilizarse todos los medios de prueba admisibles, incluido el propio testimonio del declarante que se presenta como perito.

Reafirma el artículo que la esencia de la prueba pericial es la cooperación de expertos en otras ciencias y disciplinas para que el Derecho pueda esclarecer y probar la verdad fáctica, o al menos se pueda llegar a la verdad procesal.

> Artículo 413: *Presentación de informes.* Las partes podrán presentar informes de peritos de su confianza y solicitar que estos sean citados a interrogatorio en el juicio oral y público, acompañando certificación que acredite la idoneidad del perito (Congreso de Colombia, 2004).

Tal y como consagra la regulación, el informe pericial tiene validez y fuerza probatoria en tanto que posea certificación profesional o experiencia por parte del perito que lo realiza, toda vez que la idoneidad sólo se demuestra con sustento respecto del conocimiento que se posee en el tratamiento de la prueba pericial, sea esta de la naturaleza que sea; para el campo de la evidencia digital el perito podrá adjuntar a su informe dos cosas, las certificaciones que lo califiquen como experto o entrenador forense, dadas por instituciones certificadoras como se presenta más adelante en este capítulo, y la certificación de casos tratados de forma exitosa, lo cual tiene como objetivo dar asertividad a la experiencia en el campo; estos casos pueden ser certificados por empresas nacionales e internacionales, en caso de ser una empresa dedicada a pruebas forenses es esta misma entidad quien certifica la experiencia del perito asignado al caso.

> Artículo 414: *Admisibilidad del informe y citación del perito.* Si el juez admite el informe presentado por la parte, en la audiencia preparatoria del juicio oral y público, inmediatamente ordenará citar al

> perito o peritos que lo suscriben, para que concurran a la audiencia con el fin de ser interrogados y contrainterrogados (Congreso de Colombia, 2004).

Es con esta norma donde se articula el informe pericial con la prueba testimonial, donde el sujeto interrogado es el perito, oportunidad procesal donde demuestra su experiencia y profesionalidad en la prueba pericial y el manejo de casos.

> Artículo 415: *Base de la opinión pericial.* Toda declaración de perito deberá estar precedida de un informe resumido en donde se exprese la base de la opinión pedida por la parte que propuso la práctica de la prueba. Dicho informe deberá ser puesto en conocimiento de las demás partes al menos con cinco (5) días de anticipación a la celebración de la audiencia pública en donde se recepcionará la peritación, sin perjuicio de lo establecido en este código sobre el descubrimiento de la prueba. En ningún caso, el informe de que trata este artículo será admisible como evidencia, si el perito no declara oralmente en el juicio (Congreso de Colombia, 2004).

Este artículo valida la existencia de un informe pericial, donde se documenta el trabajo forense digital que realizó el experto al momento de la obtención de la evidencia digital, el cual debe sustentarse en juicio; es apenas obvio que el perito es experto en una ciencia o disciplina y que el juez, quien debe esclarecer los hechos que sustenten su fallo, no conoce y requiere ser conducido por un experto al campo del conocimiento del caso.

> Artículo 417: *Instrucciones para interrogar al perito* (Congreso de Colombia, 2004).
>
> Artículo 420: *Apreciación de la prueba pericial* (Congreso de Colombia, 2004).
>
> Artículo 423: *Presentación de la evidencia demostrativa* (Congreso de Colombia, 2004).

Son normas que de forma más específica indican la importancia que la prueba pericial este soportada en un testimonio dado por el perito, validando, inicialmente, su experiencia en el manejo de casos, su profesionalidad por medio de certificaciones expedidas por entidades autorizadas para ello, la idoneidad de los protocolos y las herramientas aplicadas para la obtención de la evidencia digital. Igualmente, son direccionadas para indicar que la evidencia digital se valorará respecto del análisis pericial, el cual se convierte en el sustento probatorio para esclarecer los hechos fácticos que permitan al juez llegar a la verdad, al menos procesal.

Es por ello que el perito forense digital debe tener experiencia, pues de lo contrario se invalidaría fácilmente su análisis pericial, situación que ocurre en forma reiterativa en los procesos ante el juez control de garantías o en su defecto ante el juez de conocimiento, pues en Colombia se cuenta con pocos peritos forenses digitales verdaderamente expertos, incluso certificados.

b) Prueba testimonial

Esta prueba está regulada en los Artículos 383 y subsiguientes del estatuto procesal penal, con fundamento de pertinencia en la categoría de pruebas como medio de conocimiento indicado en el Artículo 382 del mismo estatuto. A través de este medio probatorio se faculta a las partes procesales y eventualmente al juez[4] para contrastar o esclarecer el contenido del informe, teniendo como consecuencia que dicho informe sea excluido, anulado o en el mejor de los casos, admitido.

c) Prueba documental

En un informe pericial presentado por un experto forense digital, se identifica el protocolo y las herramientas forenses digitales aplicadas para la obtención de la evidencia digital, muchos de estos elementos que soportan el informe están categorizados como prueba documental, es por ello que se valorará la lista de los elementos indicados en el Artículo 424 del estatuto procesal penal como prueba documental y se indicará su incidencia en un informe forense.

> Artículo 424: *Prueba documental.* Para los efectos de este código se entiende por documentos, los siguientes:
>
> 1. Los textos manuscritos, mecanografiados o impresos.
>
> 2. Las grabaciones magnetofónicas.
>
> 3. Discos de todas las especies que contengan grabaciones.
>
> 4. Grabaciones fonópticas o videos.
>
> (...) 6. Grabaciones computacionales.
>
> 7. Mensajes de datos.
>
> 8. El télex, telefax y similares.
>
> (...) 15. Cualquier otro objeto similar o análogo a los anteriores. (Congreso de Colombia, 2004)

Se extrajeron los numerales que se analizan a continuación por su aplicación en la elaboración y presentación de un informe pericial; frente al primer numeral (los textos manuscritos, mecanografiados o impresos) el informe puede ser elaborado por el perito forense de forma autógrafa, o en formato impreso, a su elección, pues no existe norma alguna que indique cómo tiene que hacerlo, sin embargo, lo usual es que el perito forense lo presente en formato impreso, sin que ello invalide un informe hecho a mano.

[4] Artículo 397: *Interrogatorio por el juez.* Excepcionalmente, el juez podrá intervenir en el interrogatorio o contrainterrogatorio, para conseguir que el testigo responda la pregunta que le han formulado o que lo haga de manera clara y precisa. Una vez terminados los interrogatorios de las partes, el juez y el Ministerio Público podrán hacer preguntas complementarias para el cabal entendimiento del caso.

El numeral segundo (las grabaciones magnetofónicas),[5] aclara que en el campo computacional existen varios dispositivos que pueden realizar este tipo de grabaciones y que son susceptibles de entrar en el análisis forense digital, no sólo para analizar su información sino para recuperarla en ciertos casos si se ha borrado. Hay que tener en cuenta que una gran variedad de dispositivos son los que pueden realizar la tarea de un magnetófono, incluso un computador de escritorio común y corriente puede pasar la voz que es un registro análogo y volcarlo a un archivo que es un registro digital.

Frente al numeral tercero (discos de todas las especies que contengan grabaciones), en el campo computacional existen varios medios de almacenamiento de información que permitirían contener las grabaciones, lo importante es entender el formato y tener el medio o dispositivo de lectura donde está almacenada la información, de ahí que sea fundamental en un laboratorio de forense digital tener todos los medios o dispositivos necesarios para leer distintos formatos, por ejemplo, varias clases de cintas y además conocer los distintos tipos de formatos de archivos que se puedan almacenar en distintos medios, incluyendo discos duros.

El numeral cuatro (grabaciones fonópticas o videos)[6] también es susceptible de análisis en los términos del numeral tercero, se asemeja a una grabación ya que para recuperar la información, borrada o no, es fundamental conocer el medio con el cual se debe acceder a la información y en el formato en el que está, sin importar la naturaleza de la información, ya bien sea un archivo de sonido o una imagen.

El numeral quinto (películas cinematográficas), debe entenderse, para el campo computacional, igual al análisis realizado para el numeral cuatro, toda vez que tiene importancia en tanto que se trata de grabaciones audiovisuales.

El numeral sexto (grabaciones computacionales) habla de las grabaciones realizadas sobre un dispositivo que forma parte de un computador, y que cumplen las mismas características ya mencionadas, siendo lo único diferenciador el hecho de que están en un medio de almacenamiento externo que podría ser un disco duro o una memoria USB, pero que se encargan exactamente de lo mismo, almacenar, mientras que un computador lo hace de forma digital; por ejemplo, el computador convierte la voz analógica a digital, otro ejemplo sería cuando se graban archivos, cuando se utilizan para hacer *backups.*

En el numeral séptimo (mensaje de datos) se habla de los verdaderos documentos electrónicos, los cuales pueden ser almacenados en varios medios de una naturaleza tecnológica muy variada, desde correo electrónico hasta celulares, también de ahí la importancia que en un laboratorio forense se tengan todos los medios necesarios para el análisis, no sólo de computadores y discos duros

[5] Según la Real Academia Española es relativo al magnetófono. (Del al. *Magnetophon,* marca reg.). 1. m. Aparato que transforma el sonido en impulsos electromagnéticos destinados a imantar un alambre de acero o una cinta recubierta de óxido de hierro que pasa por los polos de un electroimán. Invertido el proceso, se obtiene la reproducción del sonido.

[6] Según la Real Academia Española (2001) fonóptico, ca. (De *fono- y óptico*). 1. adj. Dicho de una cinta magnetofónica: Que, además del sonido, registra imágenes ópticas.

sino de cualquier tipo de dispositivo que almacene información, incluyendo celulares, asistentes personales, entre otros.

El numeral octavo (el télex, telefax y similares) debe entenderse de una manera más precisa, es decir, que el computador puede emular fácilmente la funcionalidad de un télex o un telefax siempre y cuando posea la aplicación (software) que cumpla dicha tarea específica. Cuando un computador cumple esta función imita un medios de transmisión de información, realizado por medio de dispositivos electrónicos o electromecánicos, permitiendo el registro de la información, igualmente, algunas copias de la información enviada o información acerca de la información enviada, como hora de envío, tamaño, destinatario.

Y el numeral quince (cualquier otro objeto similar o análogo a los anteriores) aclara que igual que con los télex puede pasar con cualquier otro dispositivo, como con las impresoras, algunas de ellas dejan marcas de agua con información (metadatos) acerca del documento que fue impreso para poder rastrearlo posteriormente (Tuohey, 2004).

Finalmente se extraen fragmentos de la entrevista realizada al operador judicial Alexander Díaz (Octubre, 2011), juez penal de Rovira Tolima, el cual indicó que los medios de prueba para investigar delitos informáticos, entre otros, son:

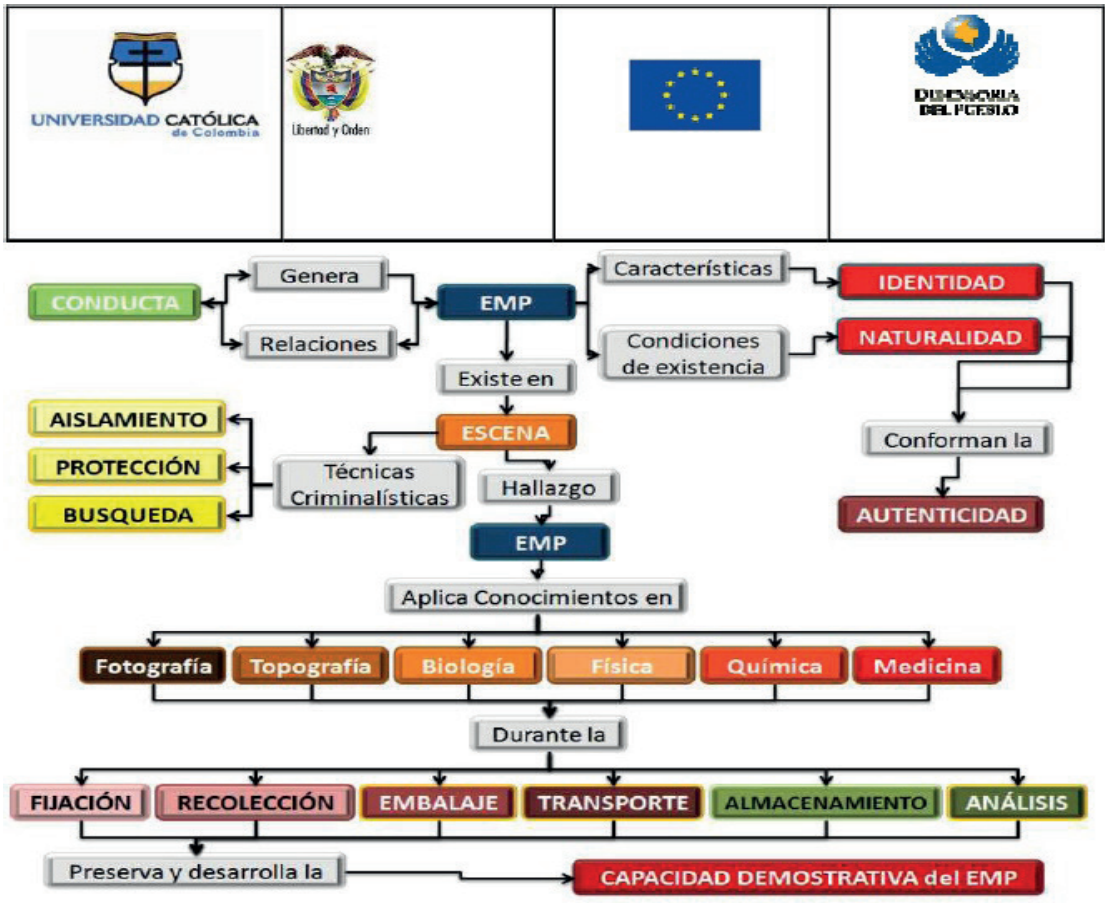
1. Grabaciones de voz.
2. Grabaciones de imágenes fijas.
3. Grabaciones de imágenes móviles.
4. Mensaje de texto sms, mms, ems.
5. Log transaccional.
6. Discos duros u otros medios de almacenamiento masivo.
7. Mensaje de datos.
8. Registros o archivos generados por computadora u otro medio equivalente.
9. Registros o archivos no generados sino simplemente almacenados por o en computadoras
10. Registros o archivos híbridos que incluyen tanto registros generados por computadora o medio equivalente como almacenados en los mismos.
11. Impresiones de imágenes fijas publicadas en el monitor.
12. Otros.

Los cuales se obtienen en gran parte por medio de evidencia digital, o medios de almacenamiento físico, y se equiparan, en muchos casos, a pruebas documentales, como también lo afirma el mismo entrevistado:

> Absolutamente toda la evidencia digital es un documento y se encuentra en soporte electrónico, y es éste el medio que sirve para defender a una persona o en el caso de los especialistas judiciales, como fundamento para imputarle una acusación a un ciudadano. El problema no radica sólo y simplemente en el documento electrónico que soporta la evidencia digital, sino cómo y de qué manera se presenta en el juicio, esto es, se deberá verificar si su extracción y fijación son legales y que tampoco se violó ningún derecho fundamental (Díaz, 2011).

Análisis por ejes temáticos en la ciencia forense y su disciplina forense digital[7]

Antes de adentrar al lector en el estudio de la ciencia forense y su disciplina científica digital es importante generar en el lector un panorama holístico del comportamiento que esta ciencia y disciplina han estructurado en la dinámica de la investigación digital, la imagen usada es publicada por la Universidad Católica de Colombia sin que se conozca otro autor diferente, por ello se aclara que el referente autoral es corporativo como lo denota la imagen:



[7] Ver Anexos: Mapa 3: se elaboró por el grupo de investigación el mapa mental, donde se estructura la generalidad de la disciplina forense digital, con el fin de dar estructura holística a la aplicación, existencia y estructura de esta disciplina.

d) Forense informático: perfil y rol investigativo

A la disciplina que se encarga de la investigación sobre medios informáticos se le conoce con variadas denominaciones, siendo las más frecuentes investigación digital, forense digital, computación forense, informática forense, entre otras, pero su derivación científica al tener origen en la Ciencia Forense, han legado a esta "nueva" disciplina de la investigación forense, donde se utilizan técnicas adaptadas de las ciencias, partiendo de los mismos principios, como el *Principio de Transferencia* de Edmond Locard, considerado el padre de las ciencias forenses, la denominación de Investigación Forense Digital o Informática Forense.

Como se define en el libro *Manual de técnica policíaca*,[8] la presentación de la prueba ante un juez ha cambiado con el devenir de los tiempos, incluso las exigencias, protocolos y formatos de presentación cambian; en un mundo en el cual ya hablamos de mundos virtuales, transacciones bancarias a través de redes de computadores de área global, se hace necesario trasladar los conceptos de las técnicas forenses del mundo físico hacía el ciberespacio, para poder conservar la cadena de custodia y de esta manera mantener la existencia de una evidencia digital que permita ser valorada por el juez en la categoría de prueba, conservando propiedades como la trazabilidad, confidencialidad, integridad, disponibilidad, privacidad, autenticidad, usabilidad, confiabilidad, completitud y no repudio, entre otras características (basándonos en el modelo CIA-PAU) que debe tener la información contenida en la evidencia digital, la cual a su vez será valorada como prueba digital en juicio.

Una de las definiciones comúnmente aceptadas en los distintos círculos de investigación de evidencia digital es la establecida por parte del Instituto Nacional de Estándares y Tecnologías (por sus siglas en inglés NIST), en la publicación especial SP 800-86 "Guía para la integración de técnicas forenses en la respuesta a incidentes" (Kent, Chevalier, Grance y Dang, 2006) donde dice que:

> La ciencia forense es generalmente definida como la aplicación de la ciencia a la ley. Forense Digital, también conocido como Computer Forensics o Network Forensics, tiene muchas definiciones. Generalmente es considerada la aplicación de la ciencia a la identificación, recolección, tratamiento y análisis de los datos mientras se preserva la integridad de la información y se mantiene una estricta cadena de custodia de la información. Datos se refiere a las distintas piezas de información que han sido formateadas en una manera específica... Por ejemplo, los datos pueden ser guardados o transferidos por sistemas de computación estándar, equipo de red, periféricos de cómputo, asistentes personales digitales (PDA), dispositivos electrónicos y varios tipos de medios entre otras fuentes.

A pesar de existir esta definición y ser la más aceptada, ya se hacían esfuerzos para definir las implicaciones de la evidencia digital y la investigación forense digital. En el año 2002 se presenta el RFC 3227 "Directrices para la recolección y archivado de evidencia" (Brezinski y Killalea, 2002), en

[8] "Manual de Técnica Policíaca - Edmond Locard", sitio web: Google Books, disponible en: http://books.google.com.co/books?id=kjIs1nquYEYC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false, 4 septiembre 2011.

el cual se definen los principios fundamentales para la recolección de evidencia y también se especifican cuáles son los procedimientos con las consideraciones mínimas para conservar la cadena de custodia.

Una vez definido lo que la investigación forense digital comprende, es importante dejar claro cuáles son las habilidades y conocimientos requeridos por el personal forense informático y los roles que deben desempeñar. En la publicación especial del NIST SP 800-61 “Guía de manejo de incidentes de la seguridad computacional” (Scarfone, Grance y Masone, 2008), se establece cómo deberá ser la estructura de un equipo de respuesta a incidentes, los modelos propuestos en este documento son:

- Equipo de respuesta a incidentes centralizado.
- Equipo de respuesta a incidentes distribuido.
- Equipo coordinado.

El equipo de profesionales relacionados con la atención a incidentes puede ser contratado a partir de distintos modelos:

- Empleados.
- Outsourcing parcial.
- Outsourcing completo.

Los profesionales pertenecientes a los distintos equipos, independientemente del modelo de contratación que se haya utilizado e incluso del modelo de equipo que se haya seleccionado, deberán tener una serie de características y habilidades necesarias a la hora de atender y manejar los incidentes informáticos. A continuación se presentan las habilidades mencionadas en el documento (Scarfone et al., 2008):

- Team Manager (director del equipo).
- Deputy Team Manager (director del equipo adjunto o auxiliar).
- Technical Lead (responsable técnico).
- Incident Lead (conductor de incidentes).
- Handlers (manipulación).

Debe tenerse en cuenta que la existencia de estos roles dentro de la organización dependerán directamente del tamaño y del impacto del incidente en la entidad.

Algunas de las habilidades técnicas que deberá tener todo el equipo de manejo a incidentes son (Scarfone et al., 2008):

- Administración de sistemas informáticos.
- Administración de redes.
- Programación.
- Soporte técnico.
- Detección de intrusos.

También existen habilidades no técnicas que serán fundamentales en todo el personal asociado debido a la naturaleza (Scarfone et al., 2008):

- Facilidad para la resolución de problemas.
- Trabajo bajo presión.
- Habilidades de comunicación: escritura y orales.

Finalmente, aclarados los conceptos de investigación digital, evidencia digital e incidente informático, y para poder llegar a una definición del rol de Forense Informático, es necesario exponer que existen tres roles que se desempeñan en este ámbito, cada uno de los cuales tiene una función distinta en todo el proceso de recogida, análisis e informe de la evidencia. A continuación se detallan dichos roles:

1. Digital Evidence Collection Specialist: las habilidades que debe tener este rol son las que debe tener cualquier profesional que se encuentre primero en la escena del crimen (First Responder). Es quien se encarga de capturar y presevar la evidencia encontrada en los distintos medios computacionales.

2. Computer Investigator: este tipo de rol requiere más experiencia en este medio, posee conocimientos acerca del funcionamiento de Internet, redes, rastreo de computadores, comunicaciones, entre otros.

3. Computer Forensic Examiner: es quien examina los medios originales donde se encuentra la evidencia, extrae la información para la posterior revisión por parte del investigador (Computer Investigator o Investigador Forense Computacional). Se entiende que este es el experto en el campo de análisis de la evidencia digital obtenida, toda vez que la evidencia no habla por sí sola, se hace necesaria la valoración analítica de la evidencia.

En el SP 800-86 del NIST (Kent et al., 2006) se establece que “prácticamente cada organización debe tener alguna capacidad de llevar a cabo un proceso de forense digital”; para los fines del protocolo definen tres roles equivalentes a los previamente vistos:

- Investigador: responsable de investigar las denuncias de mala conducta o mal comportamiento, o como tal, del incidente. Es quien se hace cargo inmediatamente de cualquier evento en el cual se sospeche la existencia de actividad criminal. Normalmente usa técnicas y herramientas forenses digitales. Tiene la capacidad de incluir en el proceso a consultores legales y personal de recursos humanos que pertenezcan a la organización.

- Profesionales de las tecnologías de la información: este grupo incluye el personal de soporte técnico, sistemas, redes y administradores de seguridad. Podrían usar un pequeño número de técnicas forenses y herramientas específicas a su área de experticia.

- Manejadores de incidentes: este grupo atiende una variedad de incidentes como el acceso no autorizado a datos, uso inapropiado de los sistemas, infecciones de código malicioso y ataques de denegación de servicios. Los manejadores de incidentes normalmente usan una gran variedad de técnicas forenses y herramientas durante sus investigaciones.

e) Competencia profesional del Investigador Forense Digital

El perito informático debe tener formación profesional en técnicas para aplicar protocolos y herramientas forenses, al igual que experiencia en el manejo de casos que le permitan desarrollar una tarea de prueba pericial encargada.

Su profesionalidad debe dar cuenta de conocimientos específicos y experiencia, al momento de obtener la prueba pericial e incluso la relación con el órgano judicial, toda vez que el perito no sólo elabora un informe, también debe asesorar a quien lo contrata, antes del litigio, igualmente debe levantar documentos, evidencias y dar testimonio en juicio.

Las funciones principales del perito son, entre otras, las siguientes: a) Recoger, registrar y archivar las solicitudes de informe pericial que encarguen los órganos judiciales o las partes; b) Analizar y examinar los elementos objeto de la prueba pericial; c) Pedir los datos para determinar las especificaciones que deban incluirse en el informe pericial; d) Elaborar el informe pericial; e) Entregar el informe pericial de quien provenga el encargo de la prueba; f) Rectificar el informe o dar aclaraciones, sea por solicitud de las partes procesales o el juez; g) Custodiar la documentación de la prueba pericial; h) Firmar el informe (en Colombia es tan válida la firma autógrafa –ante notario público–, como la firma digital –otorgada por certificadora del tipo abierta–) y las demás funciones, sean legales o administrativas, que permitan dar cumplimiento a las tareas necesarias para la obtención de la prueba pericial.

El perito está obligado, por la ley, a tener *competencia* en el conocimiento específico de la ciencia o disciplina, al igual que debe actuar bajo *principios de independencia y autoridad profesional.* Igualmente, el informe pericial debe dar cuenta de todos los elementos, tanto teóricos como los procedimientos empleados, y el razonamiento lógico aplicado.

Es por ello que la habilidad del perito se reduce a conocimiento, método y habilidades, de rutinas legales, verbales y de comunicación no verbal, que le permita darse a entender a todo público, sea este competente o no sobre el tema de las TIC o con conocimientos básicos.

Finalmente, podemos decir que el trabajo pericial es muy exigente y requiere habilidades en varias temáticas, inicialmente desde el nivel estrictamente técnico del campo forense como en otras capacidades del entorno judicial. Otras capacidades son para el desarrollo de la investigación y elaboración del informe pericial e incluso una competencia para testificar verbalmente en juicio.

f) Entorno colombiano

En Colombia existen peritos forenses informáticos en el campo público y privado. En ambos frentes profesionales la información es bastante reservada y clasificada, muchas veces como información privilegiada o información confidencial o clasificada (de propiedad del Estado). Esta información no compartida es sobre varios tópicos temáticos entre los cuales encontramos: cuántos funcionarios forenses poseen las unidades de delitos informáticos, tanto de la policía judicial como de la fiscalía, las cuales se encuentran en las principales ciudades del país como son: Bogotá, Cali, Medellín, entre otras.

También la reserva de información recae de forma especialmente confidencial sobre los protocolos y herramientas forenses digitales que utilizan en los laboratorios, la cadena de custodia aplicada por las unidades estatales de la fiscalía y la policía, situación que dificulta la conceptualización del entorno colombiano en el campo de lo público.

Un poco más fácil de conceptuar, sin que podamos decir que es del tipo abierta, es la información sobre el campo forense privado, donde las empresas, sean estas entidades sin ánimo de lucro, o sucursales extranjeras o sociedades comerciales nacionales, se dedican a prestar sus servicios de pruebas forenses a quien lo requiera y en muchos casos realizan labores forenses para el Estado, debido a su experiencia y certificación profesional.

g) Policía Judicial

Este ente estatal con funciones de Policía Judicial posee unidades de delitos informáticos, centralizadas en Bogotá, con dependencia en las ciudades principales; para la policía judicial ha sido de relevancia e importancia el campo de las ciencias forenses digitales, es por ello que cuentan con un laboratorio especializado, personal capacitado y certificado a nivel internacional, aunque cabe aclarar que no es el suficiente visto en comparación con el nivel de cibercriminalidad en Colombia, pues, tal y como lo indica el CONPES 3701, Colombia se encuentra en el puesto quinto del *ranking* mundial de Estados con cibercriminalidad.

En materia de protocolos y herramientas no se alejan de la realidad mundial, toda vez que aplican los protocolos certificados del NIST como se indicará más adelante; y como herramientas forenses aplican las herramientas ENCASE, por ser el equipo más completo en el manejo, obtención y análisis de la evidencia digital.

h) Fiscalía General de la Nación

Esta institución se encuentra dentro de la rama judicial que tiene dentro de sus funciones la investigación judicial, se ha ocupado del tema y posee unidades de delitos informáticos, sin embargo, se encuentra centralizada en Bogotá, con dependencia en las ciudades principales; también para la fiscalía, y de forma primordial, es importante estructurar la unidad general de delitos informáticos, ahora cuentan con laboratorio especializado, personal capacitado y certificado a nivel internacional, aunque igualmente no es la cantidad suficiente que se requiere para dar apoyo en la investigación y participación en juicio con pruebas de tal tipo.

Es importante que la fiscalía crezca no sólo en la estructura sino en el personal capacitado, sobre todo por la necesidad de bajar los índices de impunidad; aunque nunca no es posible fundamentar en datos oficiales estadísticos sobre la impunidad que se genera en Colombia, tanto en el ámbito policial como de la fiscalía con certeza, de ello si existe un fundamento que orienta la política pública nacional como son los documentos, para la temática se expidió el CONPES 3701[9]. La información en éste contrasta con la información que los expertos forenses, funcionarios judiciales y abogados conocen, en su quehacer profesional, ambas fuentes referentes de información son concurrentes al dar cuenta que el nivel de impunidad en Colombia es alto y que una de las causas es la ausencia de pruebas forenses, o en casos más complejos, la prueba pericial aportada es obtenida y presentada por personas que se hacen llamar “investigadores forenses” aunque realmente no se encuentren capacitados y menos cuenten con certificación por institutos reconocidos como SANS o NIST; este tema ha sido investigado y expuesto por el juez Alexander Díaz en muchos de sus escritos permanentemente publicados y de referente doctrinal y jurisprudencial en Colombia.

i) Entidades certificadoras en general

A nivel mundial existen varias entidades que pueden certificar conocimientos concernientes al campo forense digital, a su vez, poseen diversidad de certificaciones que podrían ser tanto de un forense digital como de seguridad informática, sobre esta última existe una mayor cantidad que tiene como finalidad satisfacer las necesidades y habilidades requeridas dentro del proceso de atención a incidentes; a continuación se describen algunas reconocidas a nivel internacional y que están relacionadas con la computación forense:

[9] Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación, LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA (3701). Bogotá D.C., 14 de julio de 2011.

1. Sans Institute (www.sans.org): es una de las instituciones a nivel mundial más reconocidas en la capacitación y entrenamiento en todas las ramas de la seguridad informática, incluyendo la rama forense digital. Las certificaciones más acordes a forense digital son:

   a) GIAC Forensic Examiner Certification (GCFE)

   b) GIAC Certification Forensic Analyst (GCFA)

   c) GIAC Malware Analysis Certification (GREM)

2. NIST – Computer Security Division: el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) es una agencia norteamericana encargada de la definición y el mantenimiento de estándares y recomendaciones que promueven la innovación y la competencia industrial dentro de los Estados Unidos. La división de seguridad computacional fue creada gracias a la ley de gobierno electrónico donde se reconoce la importancia de la seguridad de la información para la seguridad económica y la seguridad nacional. Su trabajo incluye proveer especificaciones para los requisitos mínimos de seguridad para los sistemas de información y la información federal, utilizando una aproximación basada en el análisis de riesgos, entre otras tareas relacionadas con la seguridad de la información, incluyendo el manejo de evidencia digital.

3. International Association of Computer Investigative Specialist - IACIS (www.iacis.com): es una corporación internacional sin ánimo de lucro compuesta por profesionales de las fuerzas de la ley dedicados a la educación en el campo forense digital.

   a) Certified Forensic Computer Examiner (CFCE)

   b) Certified Adavanced Windows Forensic Examiner (CAWFE)

4. Cybersecurity Institute (www.cybersecurityforensicanalyst.com): es una compañía dedicada completamente a servicios de forense digital, desde 1997, y provee servicios a compañías, gobierno, abogados e individuos.

   a) CyberSecurity Forensic Analyst (CSFA)

5. The International Society of Forensic Computer Examiners (www.isfce.com): es el resultado de los esfuerzo del señor John Mellon quien recibió formación en forense digital desde el año 1991 en IACIS.

   a) Certfied Computer Examiner Certification (CCE)

6. International Information Systems Security Certification Consortium - ISC2 (www.isc2.org): consorcio sin ánimo de lucro dedicado a la educación y certificación en seguridad informática. A pesar de no tener una certificación en forense digital explícitamente, la certificación CISSP tiene como uno de sus dominios “Legal, Regulsations, Investigations and Compliance”, este dominio incluye procedimientos forenses. CISSP es una de las certificaciones que tiene más relevancia, desde la necesidad de aprendizaje y su aplicación, en Colombia, afirmación extraída de un sinnúmero de documentos y publicaciones en ACIS.

   a) Certified Information Systems Security Professional (CISSP)

7. EC-Council (www.eccouncil.org): Consejo de Consultores de E-Commerce es una organización que certifica individuos en varias habilidades relacionadas al comercio electrónico y seguridad de la información. Tiene varias certificaciones pero una de ellas es específicamente del tema forense.

   a) Computer Hacking Forensic Investigator (CHFI)

   Estas instituciones son abiertas al público general y funcionan bajo criterios de elegibilidad para los candidatos a aplicar, dichos criterios no exigen que hagan parte de alguna agencia de seguridad nacional o ente gubernamental como los departamentos de policía, departamentos de seguridad, etc.

   Igualmente se deben relacionar algunas certificaciones que son exigidas por estamentos gubernamentales a nivel internacional para permitir que profesionales integrantes del Estado sean asignados para cumplir la función pública en investigación como lo es sobre el manejo de incidentes informáticos, evidencias digitales y el campo forense digital en general.

8. Federal Law Enforcement Training Center - FLETC (www.fletc.gov): adscrito al Departamento Homeland Security Norteamericano, se encarga de proveer servicios de entrenamiento a más de noventa agencias federales, además de agencias internacionales de soporte a la ley. Tienen una gran cantidad de certificaciones y programas de entrenamiento, a continuación algunos de los más importantes.

   a) Digital Evidence Acquisition Specialist Training Program (DEASTP)

   b) Internet Protocol Camera Program (IPCP)

   c) Computer Network Investigations Training (CNITP)

   d) Seized Computer Evidence Recovery Specialist (SCERS)

   e) Macintosh Forensics Training Program (MFTP)

9. National Policing Improvement Agency (www.npia.police.uk): agencia en el Reino Unido para proveer servicios críticos a la seguridad nacional, también entrena los departamentos de policía suministrándoles la experticia necesaria para cada caso.

   a) Hi-tech crime: First responder e-learning course

   b) Hi-tech crime: Masters in Cybercrime Forensics

   c) Hi-tech crime: Applied NT Forensics

   d) Hi-tech crime: Core Skills for Network Investigations

   e) Hi-tech crime: Core Skills in Data Recovery Analysis

   f) Hi-tech crime: Core Skills in Mobile Phone Forensics

g) Hi-tech crime: Covert Internet Investigations

h) Hi-tech crime: High Tech Crime First Respodner E-learning Programme

i) Hi-tech crime: High Tech Crime Managers Workshop

j) Hi-tech crime: High Tech Crime Scene Searching

k) Hi-tech crime: Researching, Identifying and Tracing the Electronic Suspect

10. SEARCH - National Consortium for Justice and Statistics (www.search.org): es una organización sin ánimo de lucro creada por y para los Estados Unidos.

a) High Tech Crime Investigative Training.

11. National White Collar Crime Center - NW3C (www.nw3c.org): algunos de los cursos impartidos son:

a) Identifying and Seizing Electronic Evidence (ISEE)

b) Secure Techniques for Onsite Preview (STOP)

c) Basic Cell Phone Investigations (BCPI)

d) Basic On-Line Technical Skills (BOTS)

e) Cell Phone Interrogation (CPI)

12. Forward Edge II - Interactive Training & Resources to Combat Electronic Crimes (www.forwardedge2.com): es un programa de entrenamiento basado en el computador, el cual da el siguiente paso en el entrenamiento de los oficiales de las fuerzas de la ley para llevar a cabo investigaciones de crimen electrónico. Este programa de entrenamiento es llevado a cabo por el Servicio Secreto Norteamericano.

Ante la ausencia de conocimiento especificado para el campo forense digital, que aún se encuentra en desarrollo, existen decenas de entidades, gubernamentales y no gubernamentales, que ofrecen servicios de entrenamiento y certificación en esta área, cursos y evaluaciones; como base de la estructura de los programas de entrenamiento incluyen ejes temáticos básicos con los que se permite cumplir el objetivo de generar una base conceptual en el campo de la disciplina forense digital, sin embargo, en el ámbito de la especificidad de temas como técnicas y métodos para la obtención, almacenamiento, administración y análisis de la evidencia digital, no responden a una estructura de materias definida para todos los institutos, por el contrario, se estructuran a partir de las necesidades de cada gobierno o Estado, los cuales definen los mecanismos y procedimientos que el estudiante debe conocer, además de las habilidades y conceptos que debe adquirir tanto a nivel legal como técnico.

Es de anotar que no existe en Colombia un documento legal donde se especifique una entidad certificadora en laboratorios, protocolos y herramientas forenses digitales, y menos con reconocimiento por el Estado o el Gobierno, sólo se cuenta con el Instituto Nacional de Medicina Legal y Ciencias Forenses,[10] donde el único documento en el campo digital, de acuerdo a la información almacenada en su sitio oficial, es el que incluye la "Resolución N.º 001036 de 2004: Por la cual se adopta el instructivo para la documentación fotografía digital en la investigación de delitos sexuales y lesiones personales".

A causa de la ausencia regulatoria sobre protocolos forenses, laboratorios, herramientas, peritos certificados, entre otras temáticas, en Colombia, tiene como consecuencia nociva principal el quedar en manos del perito forense digital, la certificación, para cada caso donde tenga participación, sobre su experiencia como perito forense digital, el protocolo, la metodología y herramientas forenses aplicadas en la obtención de evidencia digital, igualmente el laboratorio o escenario que ocupe durante la ejecución de su actividad investigativa. El vacío normativo permite tal inseguridad jurídica ya delimitada, toda vez que no están regulado los criterios formales y materiales que deben cumplirse para poder avalarse y certificar la competencia profesional y de experiencia de un profesional en el campo forense digital relacionado con el manejo de incidentes informáticos e igualmente de la certificación en el montaje, implementación y funcionamiento de laboratorios forenses digitales respondiendo a los requerimientos de certificación y calidad, ésta última dando aplicabilidad de las normas técnicas de ISO.

Es importante tener en cuenta que a pesar de que algunas de las certificaciones anteriores son abiertas al público, muchas son para el entrenamiento del campo Estatal, y que se exige dentro de los departamentos de policía o entidades que atienden delitos informáticos, como son entre otras, las otorgadas por SANS y NIST.

j) Laboratorio forense digital

En materia de laboratorios forenses existen directrices nacionales e internacionales; en Colombia se acogen las normas ISO para la estructura de todo laboratorio forense que exige los elementos mínimos que permitan el desarrollo de la actividad forense con todos los procesos, procedimientos y herramientas que permitan la materialización de un informe pericial, de forma genérica los laboratorios deben tener las condiciones que indica la norma ISO 17025.

Alrededor de todo el mundo existen varios tipos de laboratorios dedicados al procedimiento forense digital, uno de los más reconocidos es el Regional Computer Forensics Labs (RCFL) el cual está en pleno funcionamiento en Estados Unidos (The FBI, 2011), todos deben cumplir con estándares que permitan contar con las herramientas y el ambiente adecuado para el tratamiento de la evidencia digital durante todo el proceso forense.

[10] *Instituto Nacional de Medicina Legal y Ciencias Forenses*, disponible en: http://www.medicinalegal.gov.co/, consultado 15 marzo 2011.

Tal y como se indicó arriba los laboratorios que manejan evidencia digital deben cumplir como mínimo las directrices que se establecen en el ISO/IEC 17025, acerca de los requisitos generales para la competencia de los laboratorios de ensayo y calibración (ICONTEC, 2005); dichas directrices explican cómo debe manejarse la evidencia digital, los métodos a utilizar y los instrumentos que interactúan con esta, pasando por la documentación asociada a los procedimientos.

Es necesario cumplir la norma ISO/IEC 17025, en cualquier laboratorio de evidencia forense, sin importar la naturaleza de la evidencia, sin embargo, dadas las condiciones especiales de la evidencia digital esta norma resulta obligatoria, mas no suficiente, a la hora de implementar un laboratorio en el cual se pueda certificar la conservación de la cadena de custodia y el correcto análisis y presentación de la evidencia.

Dada la carencia nacional e internacional en el tema se creó el American Society of Crime Laboratory Directors/Laboratory Accreditation Board, el cual ofrece acreditación a laboratorios de forense tanto digital como de las demás ramas forenses, sean del campo público o privado, alrededor de todo el mundo. Existen normas técnicas RCFL que se encuentran certificadas por esta entidad.

A nivel de investigación, promovidas por instituciones dedicadas a este campo del conocimiento, se han hecho una serie de esfuerzos a nivel técnico para establecer los parámetros a cumplir en dichos laboratorios, estos trabajos deben ser tenidos en cuenta a la hora de establecer las consideraciones que se deben cumplir en el montaje y el funcionamiento de estos laboratorios (Dodge y Cook, 2007).

Desde el ámbito institucional existe también una organización denominada European Network of Forensic Science Institutes (ENFSI), que se dedica a la certificación de laboratorios adscritos a la Unión Europea.

Es de anotar que existen tantas certificaciones y entidades dedicadas a esto que en el ámbito internacional y nacional se presentan confusiones, es por esto que se hace necesario, en un futuro inmediato, la normalización y estandarización de los laboratorios con el objetivo de unificar los criterios; y ojalá que dicha normalización fuese promovida bajo los lineamientos enmarcados desde la Convención de Budapest.

Sin embargo, haciendo un ejercicio de transversalidad de todas estas normas para el montaje y certificación de los laboratorios, es posible indicar cuatro bases fundamentales para el proceso de certificación, así:

a) Normalización de las instalaciones

b) Obtención de los medios materiales

c) Normalización de los procedimientos de trabajo

d) Formación certificada de analistas

En Colombia existen laboratorios del campo público y privado, como ya se indicó anteriormente, aunque es pertinente aclarar que en el campo público todos los laboratorios se encuentra certificados pues cumplen estándares internacionales y la norma ISO/IEC 17025, lo cual permite garantizar el trabajo forense digital realizado en laboratorio.

Desde el campo de la seguridad informática, que ha generado mayor desarrollo en el campo del conocimiento en comparación con la disciplina forense digital, existe otra norma requerida a cumplirse, denominada ISO/IEC TR 18044:2004: Gestión de Incidentes de Seguridad de la Información.

En el caso de laboratorios privados estos son promovidos por entidades, con o sin ánimo de lucro, que se dedican a prestar el servicio de prueba forense, y pueden invertir los recursos que les permitan tener su propio laboratorio, algunas son: KPMG, MATTICA, ADALID, ASOTO TECHNOLOGY; estas han implementado, inicialmente, ISO/IEC 17025 y los protocolos y herramientas forenses digitales certificados, tal y como fueron detallados anteriormente, con el fin de darle apoyo al Estado en casos especiales, como a las personas civiles al momento de contratar sus servicios, sin embargo, es muy posible que estas entidades que prestan sus servicios no posean laboratorios forenses digitales, pero los alquilan a otras entidades, siendo de especial importancia que el perito forense sí este vinculado a su institución.

k) Protocolos forenses digital

Se podría hablar de innumerables protocolos o estándares y procedimientos, como los desarrollados por el Instituto Scientific Working Group on Digital Evidence, organización que tiene una serie de publicaciones en las cuales definen procedimientos, mejores prácticas y estándares o protocolos para la obtención, manipulación y gestión de información forense e incidentes.

Aunque no existe un protocolo propiamente dado para Colombia, sí existen iniciativas gubernamentales, materializadas en el documento CONPES 3701 de Lineamientos de Política para Ciberseguridad y Ciberdefensa, donde se da cuenta, por parte del gobierno, de iniciativas que permiten vislumbrar el comienzo de una infraestructura tecnológica y organizacional a nivel nacional en términos de atención a incidentes; un ejemplo de esto es el Centro de Coordinación de Seguridad Informática en Colombia.

A continuación se especifica la lista de estándares más utilizados a nivel internacional y en Colombia, ya sean usados en el campo público como en el privado, sin embargo, el uso de uno de varios de estos no es por cumplimiento de una disposición normativa, es realmente a criterio individual del encargado en la labor investigativa del incidente informático, y su capacidad de utilización,

sin importar en muchos casos la experiencia en el análisis forense de la evidencia digital obtenida, ante tanta diversidad de protocolos, determinar, para una prueba válida y eficaz en juicio, la integralidad de la labor investigativa queda radicada exclusivamente en el perito forense, el cual dará cuenta de la correlación y pertinencia entre el perito forense debidamente certificado, el protocolo, el laboratorio y la herramienta forense aplicada:

1. NIST SP 800-61 - Computer Security Incident Handling Guide
2. NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
3. RFC 2350 - Expectations for Computer Security Incident Response
4. RFC 3227 - Guidelines for Evidence Collection and Archiving
5. ISO/IEC 17025:2005 - Requisitos generales para la competencia de laboratorios de ensayo y calibración
6. ISO/IEC TR 18044:2004 Gestión de Incidentes de Seguridad de la Información
7. Electronic Crime Scene Investigation: A Guider for First Responders, Second Edition
8. Digital Evidence in the Courtroom: A Guide for Law Enforcement Prosecutors
9. Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability Version 2.0
10. Incident Management Mission Diagnostic Method, version 1.0
11. Incident Management Capability Metrics Version 0.1
12. Creating a Computer Security Incident Response Team: A Process for Getting Started
13. First Responders Guide to Computer Forensics: Advanced Topics
14. Handbook for Computer Security Incident Response Teams (CSIRTs) version 2
15. CSIRT Services
16. A Common Language for Computer Security Incidents
17. Homeland Security - Legal Division Handbook
18. Best Practices For Seizing Electronic Evidence v. 3. A Pocket Guide for First Responders

Otros protocolos importantes de mencionar, acogidos por determinados Estados, se encuentran relacionados con los manuales que para Colombia son aplicables, sin embargo, es necesario aclarar que los protocolos, al ser en gran parte cadenas de custodia, se aplican con el fin de garantizar el cumplimiento de los principios procesales que enmarcan el estatuto procesal penal, implementado con la Ley 906 de 2004, sin embargo, se encuentran complementados con protocolos, o cadenas de custodia como se le conocen a nivel mundial, así:

• Computer Security Incident Handling Guide
Este documento contiene las recomendaciones del Instituto Nacional de Estándares y Tecnología norteamericano. Este es uno de los estándares más completos a nivel mundial acerca del manejo de incidentes y recolección de información en un incidente (Scarfone et al., 2008).

• RFC 3227: Guidelines for Evidence Collection and Archiving
Este Request For Comments (RFC) consiste en establecer los principios durante la recolección de evidencia, el procedimiento de recolección, la cadena de custodia y algunas referencias a herramientas (Brezinski & Killalea, 2002).

• Electronic Crime Scene Investigation: A Guide for First Responders
Es una guía del Departamento de Justicia norteamericano, y de la oficina de programas de justicia, en la que se define cuáles deberán ser los procedimientos para los equipos de respuesta a incidentes. Dentro de los elementos que trata están: dispositivos electrónicos, equipos y herramientas para la investigación, aseguramiento y evaluación de una escena, documentación de una escena, recolección de evidencia, empaquetado, transporte y almacenamiento, examen forense por categoría del crimen.

• Searching And Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations
Este documento del Departamento de Justicia norteamericano pretende ser usado por fiscales federales para propósitos de entrenamiento y ejecución. Comprende un conjunto de leyes de delitos informáticos, espionaje y otros crímenes relacionados con tecnología. Consiste en la búsqueda y aprovechamiento de la información en un computador con o sin una orden judicial. También trata los asuntos legales acerca de la vigilancia en redes de comunicaciones y el tratamiento de evidencia digital (Jarrett, Bailie, Hagen y Judish, 2002).

• RFC 2350: Expectations for Computer Security Incident Response
Este documento especifica las mejores prácticas actuales para la comunidad de Internet en cuanto a las expectativas frente a los equipos de respuesta a incidentes. Posiblemente no se definan todos los requisitos apropiados para cualquier tipo de equipo (Brownlee y Guttman, 1998).

• Prosecuting Computer Crimes
Este documento del Departamento de Justicia norteamericano pretende ser usado por fiscales federales para propósitos de entrenamiento y ejecución. Comprende un conjunto de leyes de delitos informáticos, espionaje y otros crímenes relacionados con tecnología. En los apéndices incluye las mejores prácticas para respuesta a incidentes, reporte de incidentes y recursos para crímenes en redes telemáticas (Jarrett, Bailie, Hagen y Eltringham, 2002).

• Computer Forensics: Digital Forensic Analysis Metholodogy
Este artículo del Departamento de Justicia norteamericano ofrece una metodología clara en cuanto al manejo de evidencia digital. Dicha metodología comprende los siguientes ítems: preparación/extracción, identificación y análisis (Carroll, Brannon y Song, 2008).

• Perfil sobre los delitos informáticos en el Ecuador (Pino, 2009).
Este documento es una guía para la VI Reunión del Grupo de Trabajo en Delito Cibernético de la REMJA, que se realizará el 21 y 22 de enero del 2010 en Washington D.C. En el contenido del documento se pueden encontrar los tipos de delitos informáticos existentes en la legislación ecuatoriana, el manual de manejo de evidencias digitales y entornos informáticos y los principios básicos en otros.

• Medios de pruebas electrónicos: estado de avance en la legislación argentina
Esta ponencia analiza las distintas normas procesales en lo referente al grado de aceptación que presentan respecto del uso de medios electrónicos en Argentina, tanto para la gestión diaria de la administración de justicia y funcionamiento interno de los tribunales, como para el diligenciamiento de notificaciones, así como también para el tratamiento de los medios de prueba digitales (Rivolta, 2007).

• HB 171-2003 Guidelines for the Management of IT Evidence
Este manual es el estándar australiano para el manejo de evidencia digital, establecido en el año 2003. Es un documento de referencia y en ningún momento se espera que el cumplimiento con estas recomendaciones sea suficiente para la admisibilidad de evidencia electrónica (Standards Australia International, 2003). Sólo es un enunciado de las mejores prácticas. Los temas principales que incluye son: principios para el manejo de evidencia de TI, ciclo de vida de la gestión de evidencia de TI.

• Manual de Manejo de Evidencias Digitales y Entornos Informáticos (Pino, 2009).
Este manual ecuatoriano define el procedimiento de operaciones estándar para la recolección de evidencia digital, cuáles son los principios básicos y principios de peritaje, qué aparatos electrónicos y herramientas se deben tener y cómo rastrear correo electrónico.

• Manual Único de Procedimientos para Cadena de Custodia
Este manual creado por la Fiscalía General de la Nación en Colombia establece los procedimientos para el manejo de evidencia general en un caso de investigación criminal. Sin embargo, no se especifica cuál es el manejo particular: si la evidencia digital o la electrónica.

• Manual Único de Policía Judicial
Este manual establece las funciones correspondientes a la Policía Judicial en Colombia, cuáles son los organismos adjuntos a esta y cuáles son los procedimientos que se deben seguir en un caso de investigación criminal. En este documento se considera únicamente la evidencia digital en el caso de navegación en Internet, dejando por fuera elementos críticos como los de comunicaciones y almacenamiento (Consejo Nacional de Policía Judicial).

Después de haber encontrado los estándares y procedimientos más utilizados, tanto a nivel nacional como internacional, es necesario analizar cuáles de estos procedimientos se adaptan adecuadamente al conjunto de principios de la ley colombiana para el tratamiento de evidencia digital.

Además de los existentes en artículos y revistas en los que se pueden obtener metodologías y procedimientos, como los establecidos en la página oficial del departamento de justicia de los Estados Unidos (Carroll et al., 2008).

I) Informe forense (Valdés Moreno, 2009)[11]

La prueba pericial es el medio de conocimiento probatorio con el que se da cuenta de la ciencia y disciplina, en los hechos acaecidos y tratados en un caso penal.

El informe forense consolida la labor desplegada en la obtención de una evidencia digital, por lo tanto se presentan las evidencias relacionadas con el caso, la cadena de custodia llevada a cabo, el análisis forense, las conclusiones del trabajo forense,[12] y de forma primordial, la justificación del protocolo[13] y herramientas empleadas, con el fin de certificar la viabilidad de estas en el trabajo forense.

El informe, una vez presentado en juicio, deberá ser ratificado y sustentando a través de la prueba testimonial, donde el perito tiene la oportunidad de defender y aclarar su informe a fin de ser aceptado como elemento material probatorio;[14] igualmente, es allí donde tiene la oportunidad de justificar su experiencia y profesionalidad en el campo de la ciencia o disciplina de la cual se deriva el informe pericial.

También se puede presentar que el informe no deba cumplir con la etapa de sustentación en juicio, toda vez que las empresas acostumbran a contratar informes forenses con el fin de tomar decisiones administrativas y estatutarias internas, ya que valoran más el buen nombre de la entidad y la confiabilidad que esta les genera a sus clientes internos y externos, permitiendo poner en una balanza el costo beneficio frente hacer una denuncia, sustentado con una evidencia digital, la cual, por sí sola, pocas veces logra vincular un sujeto con el incidente informático acaecido, el cual sí queda debidamente probado.

El perito debe tener la habilidad de hacerse entender con el informe pericial, es por ello que el lenguaje aplicado no debe ser utilizado abusando de los términos técnicos sino, por el contrario, es indispensable que tenga notas explicativas, al detalle, sobre los temas tratados en el informe; igualmente deberá utilizar cualquier tipo de soporte documental, sea del tipo listado en el Artículo 424 del Código de Procedimiento Penal, tal y como ya fue explicado en la Unidad 3, o cualquier otro anexo que permita acercarse a la certeza del juez para tener sustento al momento del fallo. Si el perito lo cree necesario podrá utilizar glosarios que le permitan dar un conocimiento más detallado a la persona a quien va dirigido el informe.

[11] Ver Anexos: Mapa 2; se incluye este mapa explicativo sobre la metodología aplicada por un perito forense, aplicable igualmente, desde la generalidad, a un forense digital en la obtención de una evidencia digital, respetando los protocolos internacionales.

[12] Estas deben estar motivadas con una explicación sobre las proposiciones o postulados o tesis que fundamentan la demostración científica o disciplinar del ámbito técnico o práctico concreto aplicado. Igualmente, indicando en qué casos deben aplicarse los postulados, proposiciones o tesis incluidas en el informe y el grado de validez que poseen estas, y el por qué sustentan el informe.

[13] Cadena de custodia: sistema documentado que se aplica a los EPM (Elementos Materiales Probatorios) y EF (Evidencia Física) por las personas responsables del manejo de los mismos, desde el momento en que se encuentran o que se aportan a la investigación hasta su disposición final, lo que permite no sólo garantizar su autenticidad sino que se permite demostrar que se han aplicado procedimientos estandarizados para asegurar las condiciones de identidad, integridad, preservación, seguridad, continuidad y registro (Fiscalía General de la Nación, 2004, p. 73).

[14] Elemento material probatorio: es cualquier objeto relacionado con la conducta punible que pueda servir para determinar la verdad en una actuación penal. Los elementos materiales probatorios en Colombia se asimilan a la evidencia física (Fiscalía General de la Nación, 2004, p. 83).

Es pertinente resaltar los detalles mínimos que un informe pericial debe contener:

- Identificación del perito, referencias del peritaje, fecha y hora en que se realizó la prueba y las diferentes etapas de desarrollo.
- Descripción minuciosa de los ítems o aspectos sujetos a examen con el detalle identificativo de cada uno.
- Identificación de fábrica, modelo, serie y demás.
- Identificación de la documentación de la cadena de custodia a la cual se sometieron los elementos objeto del examen pericial.
- Descripción detallada, o breve, a criterio del perito, siempre y cuando permita dar a entender el informe sobre las actividades y acciones desplegadas para la elaboración del examen pericial, igualmente, cómo fue realizada la búsqueda de información o recuperación de los archivos, entre otros, realizado en el examen forense.
- Indicar de forma detalla y genérica las evidencias encontradas en el examen.
- Resumen de las herramientas, utensilios, dispositivos (*hardware*), y soporte lógico (*software*) forenses aplicados.
- Finalmente, un relato sobre las evidencias encontradas y sus implicaciones.

Todo informe debe estar relatado con una línea argumental que permita evidenciar, de forma clara, precisa y concreta, la conectividad de los protocolos, herramientas y certificaciones aplicados en el trabajo forense, con el resultado obtenido.

La presentación del informe se determina según el protocolo forense utilizado, sin embargo, mínimamente debe contener, entre otros: portada, tabla de contenido, identificación de las partes (perito, solicitante, contraparte), intervinientes en el examen o trabajo pericial y actividades desplegadas por cada uno, antecedentes (ítem por medio del cual se explica cómo se encuentran los elementos materiales probatorios que serán sometidos a examen) y fuentes de consulta (estado del arte) que permiten dar soporte al trabajo pericial, alcance de la prueba pericial solicitada (detallando los aspectos involucrados relevantes para la realización del examen pericial, que son objeto de la solicitud o que por el examen debieron ser tenidas en cuenta, previo consentimiento de quien solicita el examen), fundamentos teóricos, métodos o procedimientos y tesis aplicadas (es aquí donde se detallan los fundamentos teóricos y procedimentales que permitieron obtener la prueba pericial), actuación de comprobación (datos y análisis para la obtención del resultado), resultados de las actuaciones (es aquí donde se realiza una descripción detallada de todo lo trabajado sin que el perito pueda omitir ninguna de las operaciones y trabajos realizados, ni podrá omitir la indicación de los principios científicos o técnicos en los que se basa el examen pericial, este es el cuerpo fundamental del informe, y es el que será valorado por el juez como parte fundamental de la prueba,

sin desconocer los demás ítems del informe), y conclusiones (es en este acápite donde el perito da cuenta de las conclusiones a las que ha llegado, previo análisis forense desplegado, igualmente es el ítem donde se evidencia la credibilidad del perito, la validez y eficacia del informe), finalmente, los anexos (son todos los documentos indicados en el informe como soporte de la investigación y análisis realizado, al igual que los documentos contentivos del protocolo aplicado que permitan validar lo expresado en cada uno de los acápites del informe).

En Colombia la función del perito forense en general se encuentra regulado en el Acápite de Pruebas, específicamente en la Prueba Pericial, Parte III, Prueba Pericial, Artículo 405 y subsiguientes.

Vale destacar un breve análisis de los siguientes artículos que refieren las condiciones del informe pericial, así:

> Artículo 413: *Presentación de informes.* Las partes podrán presentar informes de peritos de su confianza y solicitar que estos sean citados a interrogatorio en el juicio oral y público, acompañando certificación que acredite la idoneidad del perito. (Congreso de Colombia, 2004)

Este artículo fundamenta a cualquiera sobre las partes en donde debe soportar sus argumentos con una prueba pericial, sea esta obtenida por peritos del campo privado o del campo público, cada uno con las condiciones detalladas anteriormente.

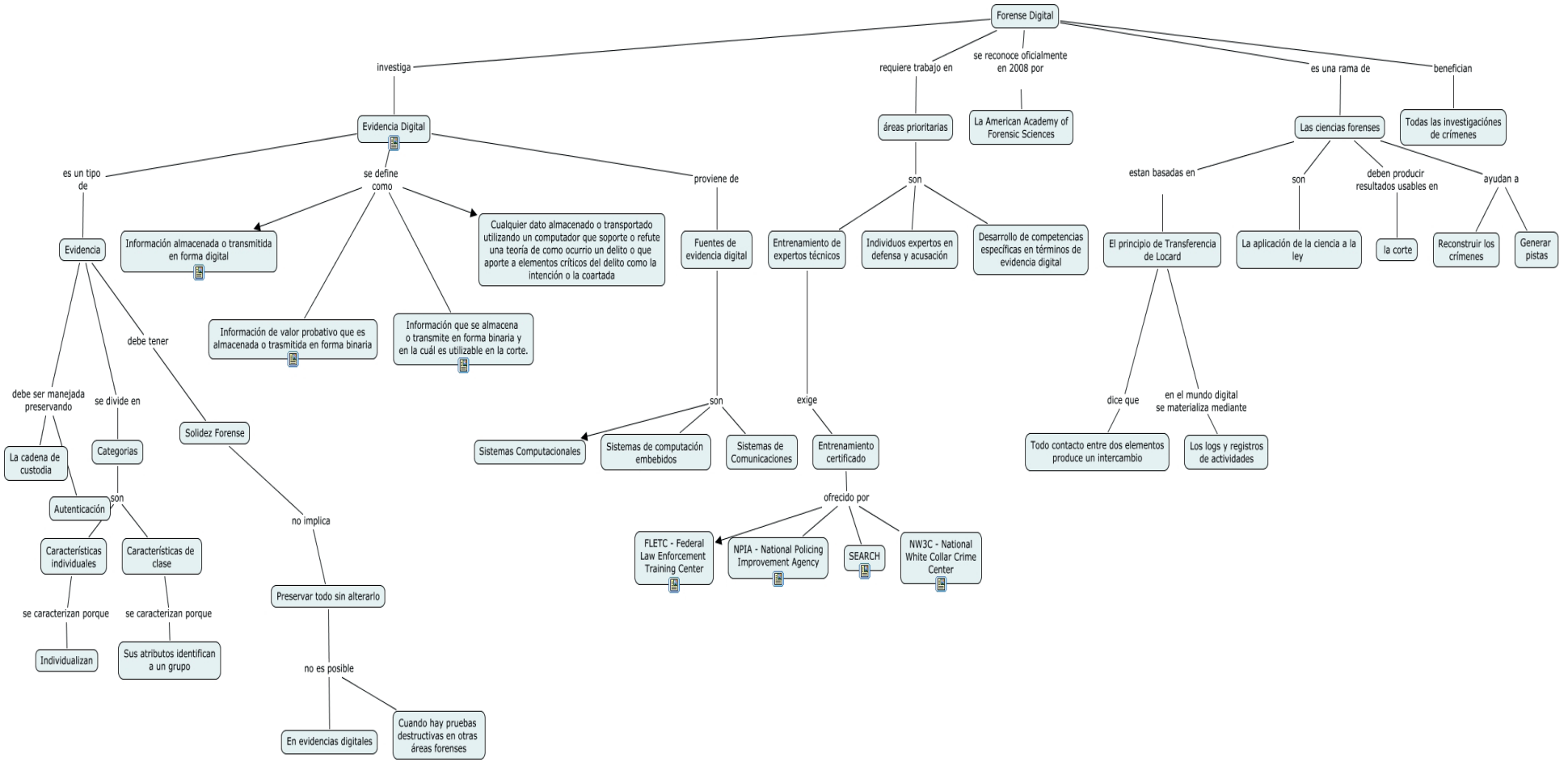
> Artículo 414: *Admisibilidad del informe y citación del perito.* Si el juez admite el informe presentado por la parte, en la audiencia preparatoria del juicio oral y público, inmediatamente ordenará citar al perito o peritos que lo suscriben, para que concurran a la audiencia con el fin de ser interrogados y contrainterrogados (Congreso de Colombia, 2004).

En esta norma podemos ver cómo el informe pericial es la herramienta objetiva que permite acercar al juez a la certeza, para poder fallar con la mayor seguridad de que la decisión tomada se funda en la verdad probatoria, toda vez que, es el interrogatorio el que permite contrastar lo escrito en el informe con la realidad de conocimiento científico y técnico desplegado por el perito, momento en el cual se puede comprobar la experiencia de este y la pertinencia del trabajo pericial desplegado.

> Artículo 415: *Base de la opinión pericial.* Toda declaración de perito deberá estar precedida de un informe resumido en donde se exprese la base de la opinión pedida por la parte que propuso la práctica de la prueba. Dicho informe deberá ser puesto en conocimiento de las demás partes al menos con cinco (5) días de anticipación a la celebración de la audiencia pública en donde se recepcionará la peritación, sin perjuicio de lo establecido en este código sobre el descubrimiento de la prueba. En ningún caso, el informe de que trata este artículo será admisible como evidencia, si el perito no declara oralmente en el juicio (Congreso de Colombia, 2004).

Finalmente, la norma ratifica que un informe pericial esta validado como medio probatorio en juicio en calidad de prueba que corresponde a informe forense digital siempre y cuando se sustente con el testimonio rendido por el perito, la ausencia de sustentación excluye la prueba de los medios probatorios.

El grupo de investigadores, por el sinnúmero de discusiones realizadas en cuanto al tema de forense digital concluyo un mapa mental donde se podría resumir la ciencia forense y su correlación con la disciplina forense digital, la correlación que existe con la extracción de la prueba denominada mundialmente evidencia digital, además las entidades estatales y privadas relevantes en cuanto a su campo de acción respecto de la actividad investigativa forense digital, y la viabilidad de existencia probatoria, en cuanto a la aplicación del principio de transferencia, la aplicabilidad de la norma interna vigente de cada Estado además de los tratados internacionales que rigen las relaciones trasnacionales, para finalmente obtener entre muchos otros referentes de conocimiento, el que la sociedad de la información o sociedad digital, reto al campo del derecho y la investigación, generando evolución en los lineamientos normativos y en los protocolos forenses, de allí que la disciplina forense digital o la informática forense permiten dar respuesta al ámbito de la evidencia digital sobre la ocurrencia de incidentes informáticos. De ésta gran conclusión se puede validar el mapa mental que a continuación se expone:



Mapa 3 – Disciplina Forense Digital – Autor Individual Juan G. Lalinde, investigador EAFIT.

HALLAZGOS

CAPÍTULO 5.

ANÁLISIS DE LA INFORMACIÓN Y DE LOS DATOS DE LA INVESTIGACIÓN EN DELITOS INFORMÁTICOS

Ana María Mesa Elneser

Jorge Eduardo Vásquez Santamaría

Diseño y Experiencia Metodológica

Modelo de investigación

Para el proyecto de investigación se adopta un diseño de investigación cuantitativo cualitativo, o lo que Hernández Sampieri, Baptista Lucio y Fernández Collado denominan "enfoque integrado multimodal o enfoque mixto" (Hernández, Collado y Baptista, 2006, p. 99), con dominación del diseño cuantitativo toda vez que los enfoques cualitativo y cuantitativo son considerados paradigmas de investigación científica, pues ambos emplean procesos cuidadosos, sistemáticos y empíricos en el esfuerzo por generar conocimiento.

La combinación de ambos paradigmas reúne la funcionalidad de las características metodológicas que orientan la ejecución de un proyecto de investigación determinado. En este caso la fusión de esos modelos se propone desde la posibilidad de adelantar la observación y la evaluación de los delitos informáticos y la informática forense como fenómenos socio jurídicos de relevancia en un país como Colombia; de establecer suposiciones o ideas como consecuencia de la observación y evaluación realizada sobre aquellos como objeto de estudio, de proponer y demostrar el grado en que las posturas y suposiciones tienen fundamento en el escenario jurídico, y de contrastarlas sobre la base de pruebas que resulten de la indagación. Finalmente, también permite proponer nuevas observaciones y evaluaciones para esclarecer, modificar y fundamentar las suposiciones o ideas, y generar otras. Además:

> Los enfoques mixtos parten de la base de que los procesos cuantitativo y cualitativo son únicamente "posibles elecciones u opciones" para enfrentar problemas de investigación, más que paradigmas o posiciones epistemológicas (Todd, Nerlich & McKeown, 2004). Como plantean Maxwell (1992) y Henwood (2004), un método o proceso no es válido o inválido por sí mismo; en ciertas ocasiones la aplicación de los métodos puede producir datos válidos y en otras inválidos. La validez no resulta ser una propiedad inherente de un método o proceso en particular, sino que atañe a los datos recolectados, los análisis efectuados, y las explicaciones y conclusiones alcanzadas por utilizar un método en un contexto específico y con un propósito particular (Hernández et al., 2006).

El carácter cualitativo resulta necesario y oportuno en la medida que desde el campo jurídico surge la problemática a indagar, lo que implica una valoración de los sujetos investigadores en el contexto del cual desprenden y delimitan una realidad compleja que postulan como problemática. No sería posible comenzar una investigación de componente social como la aquí trazada, de la nada, sin soporte alguno. Como señala Guillermo Briones en su obra *Metodología de la investigación cuantitativa en las ciencias sociales:*

> En el caso de un investigador con experiencia, su acercamiento a un cierto tema específico puede tener su origen en su formación teórica y metodológica y en los trabajos que ha realizado de modo tal que las nuevas investigaciones que realiza corresponden a una misma línea de indagación. Aun así, cuando tal investigador decide hacer un nuevo estudio, no solo se basa en sus investigaciones

> anteriores, sino que debe conocer los trabajos de otros investigadores, lo cual lo obliga a estar al día en la literatura pertinente, sea para comprobar resultados presentados en ella o para proponerse otros problemas (Briones, 2002, p. 18).

Desde dicho contexto, la problemática delimitada en la propuesta de investigación implicó un ejercicio de identificación y reconocimiento de un área especializada del conocimiento jurídico, una ponderación cualificada de aspectos problemáticos propios de la informática jurídica, y en ella de la informática forense.

En ese sentido, la investigación cualitativa le permite a los sujetos investigadores proponer un punto de partida teórico para el problema de investigación. En él, lo cualitativo aporta al trabajo desde la categorización como parámetro referencial que canaliza la búsqueda de soportes y elaboraciones teóricas y conceptuales sobre los componentes y tópicos de estudio del problema de investigación.

El paradigma de investigación cualitativo exige un trabajo disciplinado de los investigadores, la oportunidad de ser filtros selectivos de información encontrada a lo largo de la indagación, fuente de objetivación de conocimiento de posible naturaleza científica, y proponentes de dialécticas transformadoras de fenómenos sociales y jurídicos como el aquí propuesto.

En el caso del paradigma de investigación cuantitativa, se da carácter dominante en la medida que para la investigación se proyecta tener avances de naturaleza exploratoria, descriptiva y explicativa. Estos avances metodológicos fueron seleccionados para esta investigación con el fin de alcanzar la preponderancia del diseño cuantitativo en la medida que se cuenta con un problema de estudio delimitado y concreto en la informática forense que tiene relación con los delitos informáticos dispuestos en la Ley 1273 de 2009; el problema se delimita a una pregunta de investigación, y sobre ella, versan ciertas cuestiones específicas.

Método exploratorio

Desde la adopción del modelo cualitativo en la investigación, es necesario dar inicio por revisar lo que se ha investigado anteriormente, lo que implica examen de literatura sin que se excluya la posibilidad de cuantificar el soporte informativo relevante para el caso; la revisión de literatura posibilita la construcción del marco teórico de la investigación, y este fortalece la posibilidad de incluir datos objetivos, cerrados y estadísticos que interactúen con el fundamento teórico del que se pueden derivar algunas hipótesis.

Se adopta el estudio exploratorio por enfrentar un objeto de estudio o problema de investigación poco estudiado, no abordado en la universidad o incipientemente abordado en el medio. Este modelo se emplea cuando se examina un nuevo interés o cuando el objeto de estudio es relativamente nuevo (Babbie, 2000, p. 72). Los estudios exploratorios se hacen con el objetivo de satisfacer la

necesidad de investigar y ampliar el conocimiento, probar la viabilidad de un estudio más extenso, y desarrollar métodos que se aplicarán en un estudio subsiguiente.

Hernández Sampieri, Baptista Lucio y Fernández Collado (2006) describen el estudio exploratorio como aquel que se realiza cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no ha sido abordado anteriormente.

Método descriptivo

Este método se acoge puesto que el estudio descriptivo guarda la intención de describir fenómenos, contextos, situaciones y eventos, esto es, detallar cómo son y cómo se manifiestan (Hernández et al., 2006). Busca especificar las propiedades, características y perfiles de las personas, grupos, procesos, objetos u otros fenómenos que se sometan a análisis; busca describir la situación prevaleciente al momento de realizar el estudio. Con ella no se espera demostrar la influencia de una variable sobre otra, pues lo que se hace por el lector del informe de investigación es pintar una imagen (Salkind, 1999).

Método documental

La exploración y descripción de la información surgida en torno al objeto de estudio requiere de una plataforma teórica por medio de la cual se recolecte y sistematice la información que expone los constructos ya existentes, y facilite la descripción de las categorías objeto de análisis. Para ello se implementó el método documental, el cual se basa en fuentes de naturaleza documental, quiere decir, en diversos tipos de documentos como son los obtenidas a través de fuentes bibliográficas, hemerográficas o archivísticas; lo que se traduce en la consulta de libros, artículos científicos, ensayos de revistas y periódicos, y a su vez, las de corte jurídico formal, como la constitución, las leyes, los decretos y los actos administrativos.

En este último componente de la investigación documental es preciso destacar la orientación jurídica y socio jurídica que impregna la indagación. De un lado el proyecto se fundamenta en un enfoque jurídico, sustentado en varias fuentes formales del Derecho como recurso informativo, de donde se deriva el análisis de la unidad referente a la presentación de los delitos informáticos previstos en el ordenamiento jurídico colombiano.

Posteriormente, la corriente socio jurídica impregna la investigación, en donde se da lugar a la información que resulta de la interacción de los actores jurídicos previstos en la muestra poblacional con las figuras normativas propiamente dichas que disponen los delitos informáticos. De allí se extrae la información por medio de la consulta por el conocimiento, comprensión y reflexiones en torno a las normas objeto de estudio.

Instrumentos cualitativos

Desde su naturaleza cualificable de los fenómenos, valorable y descriptible de la realidad, abierta, dialógica, constructiva y recreativa, la investigación cualitativa propone una serie de instrumentos para la recolección de la información. El instrumento es la herramienta directa, más próxima entre el investigador y la fuente de información. Se convierte en el canal de acercamiento y contacto del interés indagable sobre la materia prima que reúne la información para el proyecto. Los instrumentos cualitativos acogidos para el proyecto fueron el fichado bibliográfico, la entrevista a profundidad, y la triangulación de la información.

El fichado o manejo de fichas bibliográficas en un instrumento de organización y sistematización de la información, que procura el adecuado y ordenado manejo de la información clasificada a partir de las categorías preestablecidas para el proyecto, o de aquellas que sean emergentes.

En el proyecto, la labor del fichado plasmó los resultados de toda la fase de rastreo bibliográfico e información, análisis documental, debates grupales sobre los constructos teóricos, permitiendo la recopilación del sustento secundario sobre las figuras de delito informático, informática forense, evidencia, prueba e indicio.

De otra parte se acogió la entrevista, la cual permite la comunicación interpersonal entre investigador y sujeto de estudio, con un propósito determinado que es obtener respuestas verbales a los interrogantes planeados sobre el problema propuesto. Las entrevistas resultan adecuadas, en la medida que se corresponden con el modelo cualitativo en la búsqueda de percepciones, opiniones, actitudes, experiencias y conocimientos.

Por medio de la información recolectada en las entrevistas se puede ahondar en la explicación del propósito del estudio y especificar la información que se necesita para despejar el problema, permitiendo aclarar la pregunta para asegurar la respuesta adecuada. Además, permite mayores posibilidades de expresión permitiendo una comprensión amplia de los temas abordados. El profesor Carlos Andrés Aristizábal (2008) en su guía “Teoría y Metodología de la investigación”, afirma frente a la entrevista:

> Es uno de los instrumentos más flexibles e importantes, dentro de la investigación cualitativa, es una técnica que permite, sobre la marcha ir corrigiendo o previniendo ciertos errores, además que asegura la validez de las respuestas, mediante aclaraciones, replanteamiento de las preguntas, etc. Con la entrevista se puede acceder a las percepciones, las actitudes y las opiniones, que no pueden inferirse de la observación, pero que con la entrevista puede recolectarse.
>
> La entrevista es una conversación entre dos personas por lo menos, en la cual uno es el entrevistador y otro u otros son los entrevistados; estas personas dialogan con arreglo a ciertos esquemas o pautas acerca de un problema o cuestión determinada, teniendo un propósito profesional, la búsqueda de los sentidos y significados del entrevistando frente a lo que se le pregunta (…).

> La entrevista debe convertirse para el entrevistador en el espacio para acceder a la vivencia y experiencia del otro con quien dialoga, lo que no solo permite el acceso e interacción con un nuevo espacio de conocimiento, sino que le permite acceder a nuevas relaciones sociales que son reconstruidas por el entrevistado en el momento de la entrevista. En este sentido la entrevista presupone, la existencia de personas y la posibilidad de interacción verbal dentro de un proceso de acción recíproca. Como técnica de recopilación va desde la interrogación estandarizada hasta la conversación libre; aun cuando en ambos casos se recurre a una guía que puede ser un formulario o un esquema de cuestiones que han de orientar la conversación.

La entrevista realizada fue a profundidad, lo que destaca la intención de aproximación a las ideas y conocimientos por parte del investigador, acudiendo a la posibilidad de acceder a datos precisos, lo que exige preguntas muy elaboradas que pueden ser orientadas en su ejecución sin sugerir respuestas al entrevistado.

Finalmente, la triangulación de información es, como explica Mayumi Okuda Benavides y Carlos Gómez Restrepo (2005, p. 119), un ejercicio permanente que dará lugar al surgimiento de afirmaciones pero a la vez de nuevas interpretaciones que nutrirán el trabajo y posibilitarán la recreación de los encuentros y la orientación para la construcción conceptual.

Descripción de las entrevistas a profundidad[1]

En materia de aplicación de instrumentos de consulta, fue necesario, teniendo en cuenta un eje temático tan específico y especializado, entrevistar a personas involucradas con el campo de la informática forense y el derecho informático, a fin de develar el grado de conocimiento que se posee por parte de actores en el marco de la Ciencia Forense y la Ciencia del Derecho.

Sólo se obtuvo autorización para revelar la identidad de cuatro de las personas entrevistadas: un experto forense, dos jueces y un abogado con experiencia como ingeniero de sistemas; las demás personas, entre las cuales se encuentran expertos forenses, hackers éticos, abogados y fiscales, dejaron clara la necesidad de preservar su identidad, en términos de confidencialidad, teniendo en cuenta temas de seguridad profesional y personal de cada una de ellas, aunque es de aclarar que se recibió autorización expresa y verbal para la utilización de la información facilitada por estas. Por esta razón se procede en primer término a hacer un análisis introductorio a los resultados obtenidos, indicando de forma holística el panorama investigado, luego se procederá a hacer un análisis del resultado sobre cada entrevistado, bajo reserva confidencial.

Para el análisis de las diferentes entrevistas se extraerán apartes obtenidos de los entrevistados y posteriormente se dará una breve postura como conclusión a lo obtenido.

a) Jueces

[1] Ver Unidad 8: Anexos formato de entrevistas a profundidad: abogados - jueces y expertos forenses.

Jurista y operador judicial Alexander Díaz, juez penal de Rovira Tolima, quien fue entrevistado de forma electrónica. Se toman apartes de su entrevista (García, 2011):

Frente al primer objetivo específico indicó:

> Convenio sobre Cibercriminalidad de Budapest o Convención sobre Delitos Informáticos, siendo a la postre el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia. Este acuerdo fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión N.° 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004. En abril de 2001 el Consejo Europeo publicó el proyecto destinado a armonizar las legislaciones en los Estados miembros (47 miembros y 8 observadores al día de la fecha) y abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU. en noviembre de 2001. Actualmente países como Argentina (que ha basado su Ley de Delitos Informáticos en este convenio) y Ecuador están analizando adherirse. Si se analiza con cuidado mi propuesta (la ley de delitos informáticos), la que se tomó como base legislativa, se tuvo en cuenta lo sugerido por el Convenio, esto es la seguridad de la información y los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos, resaltando que ese esfuerzo se materializó cuando nos dieron la razón los Congresistas al elevar como uno de los pocos países, sino el único, en proteger como BIEN JURÍDICO TUTELADO La Información y el Dato, especialmente también el de penalizar, como homenaje al mismo título, la VIOLACIÓN DE DATOS PERSONALES, también resultando de los pocos países que penalizamos (con prisión) puesto que esta violación en otras latitudes es una falta administrativa y se sanciona pecuniariamente como ocurre en Argentina, Chile y España, con sus respectivas Agencias de Protección de Datos Personales. Debo aclarar que en la Ley 1273 de 2009, se incluyeron unos tipos que no son exactamente informáticos, porque los legisladores y aún hoy, abogados y especialistas judiciales, creen que el delito informático vulnera el BIEN JURÍDICO TUTELADO DEL PATRIMONIO ECONÓMICO porque se encuentra a continuación de ese Título VII o porque éste finalmente se encuentra vinculado con una conducta que afecta este bien. Debemos recordar que el BIEN JURÍDICO TUTELADO o protegido en el Título VII BIS del Código Penal Colombiano es LA INFORMACIÓN Y EL DATO. Se puede revisar y comparar mi proyecto original, el que sirvió de fundamento para la Ley de marras, con la norma promulgada y observamos que los últimos tipos publicados son en blanco o subordinados, pues están condicionados a la consumación de otros y más exactamente patrimoniales, diferentes a los ocho sistemáticos tipos anteriores. Lamentablemente algún sector de la Academia considera que el tipo penal clásico se puede informatizar simplemente agregándole el término de “informático” como lo han hecho otras legislaciones del mundo o simplemente un bis, literal o numeral, pues se cree que la conducta es informática porque se realiza a través de medios tecnológicos, olvidando que el delito informático se puede consumar en soporte papel simplemente porque lo que se vulnera es la información y/o el dato. Otro detalle que tenemos que resaltar sobre el epígrafe del artículo 269 G, lo habíamos redactado originalmente como PHISHING como se le conoce internacionalmente, argüíamos que se debería conservar el nombre en ese idioma pues así se han castellanizado otros términos como el Leasing y así lo han entendido para referirse al arrendamiento financiero, pero no sirvieron nuestros esfuerzos, finalmente el artículo 269G quedó como: **SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.**

Frente a estas afirmaciones es pertinente traer a colación lo expresado en la Unidad 3 del presente texto, igualmente, se encuentra la posibilidad de reafirmar que la ley de delitos informáticos en Colombia, aunque llegó de forma tardía al Estatuto Sustancial Penal, e introdujo un bien jurídico nunca antes tutelado como la información y el dato, sí requiere, en algunos casos, modificación, para darle mayor relevancia en el campo penal internacional, entre otros aspectos, siendo importante que en dicho capítulo se incluyan castellanismos propios de las conductas y figuras informáticas, conocidas por los ciudadanos, en mayor medida que los conceptos tradicionales utilizados para indicar un tipo de delito, una herramienta utilizada o la cualificación de un delincuente.

Plantea el operador judicial:

> Me parece que se refiere al CONPES 3701 denominado **LINEAMIENTOS DE POLÍTICA PARA CIBERDEFENSA Y CIBERSEGURIDAD.** El desarrollo legislativo actual en tratándose de **DELITOS INFORMÁTICOS** no requiere grandes cambios legislativos, tal vez considero que el cambio sería en ubicar puntualmente los tipos patrimoniales en el título correspondiente y establecerlos como circunstancias de agravación, los que se encuentran en el Título VII BIS. Es más considero que deberíamos esperar un tiempo razonable para ver la respuesta de la efectividad o no de los tipos propuestos y aplicados, pues así con base a ese estudio podríamos sugerir las modificaciones que se deben tener en cuenta. Ahora bien sobre si se necesita un cambio en Colombia frente al recurso físico y humano dedicado a las unidades de investigación de delitos informáticos en las distintas entidades del Estado y las entidades privadas, considero que sí y pronto, puesto la experiencia nos enseña cómo se están realizando graves errores en la tipificación de los delitos informáticos, conjugan conductas en verbos que no corresponden y concursan tipos cuando no se puede, como vg. Concursar la **INTERCEPTACIÓN DE DATOS INFORMÁTICOS** (Clonación) con **VIOLACIÓN DE DATOS PERSONALES** (Identidad Robada), cuando no se puede concursar tipos del mismo título en conductas desplegadas en unos mismos hechos (García, 2011).

Lo indicado por el operador judicial reafirma lo expresado en la Unidad 6 del presente texto, donde se plantean una variedad de artículos del estatuto procesal penal, el cual no ha sido evolucionado en mayor medida y dificulta en muchos casos la judicialización de delitos informáticos, en muchos casos trasladados al campo de los delitos tradicionales, o como también se puede indicar, pasar la conducta delictual sobre el bien jurídico, denominado información o dato, al campo del bien jurídico patrimonio, lo cual descontextualiza las verdaderas conductas cibernéticas delictuales.

Frente al objetivo 4 opina el operador judicial:

> Siempre le he dicho a mis discípulos que frente a una escena de un delito informático, debemos establecer las condiciones especiales de aislamiento en tratándose de allanamientos o recintos que se tenga como centro de trabajo criminal (cuartos, estudios, oficinas, escritorios, mesas) se debe establecer el control de acceso de energía de los equipos enchufados o desenchufados (PC LAPTOPS). Al encontrarse conectados fantástico para realizar la extracción de la evidencia digital (información o datos volátiles) colgada temporalmente en la memoria RAM, la extracción de los metadatos (datos de los datos) y logrado todo esto el estampado de la huella hash, que le va a per-

> mitir al primer respondiente judicial, si los que están extrayendo no son funcionarios de la Policía Judicial, que la evidencia extraída está incólume desde su extracción a la fijación y será la misma para cuando en copia espejo nos permita hacer análisis en el laboratorio forense. Igual ocurrirá con el Majordomo de la Red, cuando detecte o establezca en el reporte una intrusión, procederá en idénticas condiciones arriba anotadas, para entregarla evidencia al primer respondiente de Policía Judicial a quien se le debe entregar, con todas las solemnidades que exigen los protocolos (García, 2011).

Lo cual permite darle soporte a la Unidad 7 en muchos de sus apartes, donde se indica que Colombia, a pesar de tener personal especializado, tanto en el campo público como privado, tiene deficiencias en la extracción de evidencias digitales y el manejo o tratamiento ante un incidente informático, tanto por el administrador del sistema como por el personal dedicado al desarrollo estructural de este; y que por lo tanto requieren mejor capacitación en protocolos o cadenas de custodia que permitan minimizar el riesgo de invalidación de los elementos materiales probatorios, toda vez que la volatilidad de los datos y la fácil alteración de estos por un mal procedimiento invalidan la prueba posterior, como pasa en errores tan simples cometidos por la policía judicial o los funcionarios del CTI, cuando en la escena se descubren dispositivos electrónicos encendidos y estos son apagados para su embalaje, sin aplicar técnicas forenses digitales, generándose la primera afectación de alteración de la huella o código hash, elemento tecnológico que permite certificar la no alteración del sistema en el momento de la captura.

Frente al objetivo 5 opina el operador judicial:

> Si existen protocolos como el diseñado y desarrollado por el Ing. John Jairo Echeverry Aristizábal, ex Director Nacional de la Unidad de Delitos Informáticos de la Fiscalía General de la Nación en Colombia, hoy es consultor de OPDAT programa de la Embajada de los Estados Unidos en Colombia; protocolo que me parece acertado, académico y le creo, porque respeta todos los parámetros que los estándares internacionales establece en los suyos. Este permite ser aplicado, en el tratamiento de un incidente, a prueba de errores del experto forense y se evita la afectación al EMP presentado en juicio para obtener la prueba digital del argumento fundamentado por ésta. No obstante no se descarta, tampoco yo lo haría, en aplicar los protocolos internacionales como el de la INTERPOL, claro está sin mezclarle el interés político que tenga la nación en donde se va a aplicar, porque así sea ilegal la extracción de la evidencia digital ésta va a certificar la legalidad de la evidencia que es ilegal por congraciarse con el gobierno de turno (García, 2011).

Una vez más es permisible indicar que el conocimiento de unos cuantos sobre protocolos, herramientas, técnicas y laboratorios en el campo forense digital, no valida la evolución de la norma sustancial en Colombia y mucho menos la procesal penal; si se comparan estos mismos elementos acogidos por Colombia o desarrollados en Colombia para otras conductas delictuales, como el homicidio y el hurto, con gran desarrollo doctrinal y jurisprudencial, son de relevancia y conocimiento no sólo de los cuerpos de investigación judicial del Estado sino también del ámbito privado, no así en el caso de delitos informáticos, materializando una manta de confidencialidad inoficiosa para la

seguridad jurídica que el ordenamiento jurídico colombiano debe brindar a sus ciudadanos, y agrandando la brecha facilitadora para los ciberdelincuentes, que abusan en la comisión de conductas tipificadas en la Ley 1273 de 2009, toda vez que es de gran facilidad lograr una sentencia absolutoria, fundamentada, en muchos casos, por la ignorancia en el tratamiento tanto de la imputación como del campo probatorio.

Ahora analizaremos la entrevista realizada a la jueza Gloria Luz Restrepo Mejía, Juzgado Tercero Penal del Circuito de Medellín (Mejía, 2012):

> Comenzando con lo de las evidencias digitales nosotros en el momento actual estamos tramitando un juicio, del cual no vamos a contar los pormenores, aunque es público, para los efectos que nos ocupan valga destacar que se pretendía hacer valer como prueba una información que se había obtenido vía Internet, los pantallazos se pretendían introducir como prueba dentro de la actuación, sin embargo el despacho considero que esos pantallazos, es información que se había obtenido, no estaba debidamente acreditadas su autenticación (…) aquí una de las preguntas habla precisamente en cuanto a la evidencia digital se refiere para obtener su validación y elevarse a categoría de prueba digital en delito debe contar con un perito forense informático al respecto debe manifestar que en algunos eventos debe, puede contarse con un perito forense informático, pero en algunos otros eso se puede obviar con la firma digital hay metodologías o métodos de autenticación señalados des la misma ley en cuanto a la evidencia digital para hacerla valer dentro del proceso penal como prueba, para que sea autentica y que tenga eficacia aprobatoria, en ese caso en particular el simple pantallazo, la simple información obtenida sin tener la claridad de quien era el autor de esa información, no sería posible que ingresase válidamente al proceso y por eso el despacho no decretó la práctica de esas pruebas (…) podía haberse obviado lo de la prueba digital o de los métodos de autenticación con un perito forense informático, pero la parte en el nuevo sistema penal acusatorio es la que tiene que pedir la prueba e indicar como la tiene que hacer valer y en consecuencia, la defensa en este caso no pidió ningún perito forense informático por lo que, mal haría el despacho en entrar a suplir esa inconsistencia e indicarle que podía autenticarlo con un perito forense informático, en consecuencia la prueba no se admitió, sin embargo pues llama la atención por lo novedoso de la evidencia digital y que se pretendiese hacer valer como tal dentro de un proceso penal (…) advirtiendo que no se autentico debidamente la evidencia digital, no se extrajo como dice la ley con los requisitos formales y materiales para elevarse a la categoría de prueba digital en juicio la cual no deja de ser un documento (…) estos documentos tienen que ser auténticos conforme al artículo 424 del código de procedimiento penal (…) existen métodos de la autenticación de la prueba digital uno de ellos es precisamente la firma digital, en consecuencia, si se puede acreditar la firma digital del documento entonces no habría problema se puede detectar la práctica de esta prueba o si no con un perito forense informático, pero realmente nuestros abogados no manejan muy bien la temática y en general para todos los operadores jurídicos, toda vez que es novedoso para nosotros esta cuestión de la evidencia digital, su práctica dentro del proceso penal como se eleva a la categoría de delito (Mejía, 2012).

Tal y como lo indica la funcionaria, la evidencia digital requiere una especialidad de protocolos y herramientas que permitan la autenticidad del documento y la vinculación con el autor, siendo el requisito indispensable para validar la prueba y permitir su inclusión en un proceso penal.

Para la operadora judicial entrevistada uno de los aspectos a destacar en Colombia en gran medida es el desconocimiento, tanto de operadores judiciales como de abogados, defensores públicos y demás intervinientes en el proceso, sobre el tratamiento e investigación de los delitos informáticos, por lo tanto, la deficiencia en los procesos y la judicialización efectiva que tiene como consecuencia la impunidad, tiene un factor determinante y es la falta de capacitación.

En los procesos que se llevan a cabo ante juez control de garantías, son marcadas las exigencias que el funcionario debe tener en cuenta al momento de valorar la prueba pericial dada por un perito forense digital, aunque éstas no estén expresamente consagradas en la ley, aun así, son necesarias por la especificidad de la evidencia digital como medio cognitivo del incidente informático sometido a investigación judicial y que de ello se vale el derecho en conexidad con la informática forense, para delimitarlas y hacerlas valer en juicio.

Como evidencia de la tesis antes descrita sobre la ausencia normativa en el Código Procesal Penal de las características o elementos, de los cuales deben darse cuenta en la prueba pericial derivada de la obtención de una evidencia digital, es la existencia de valoración judicial con apoyo a otros ámbitos científicos y disciplinares para identificarlos y valorarlos, motivo por el cual en la Unidad 6, se desarrolla una propuesta preliminar de reforma a las normas procesales del Estatuto Procesal Penal que, en principio, deben ser ajustadas para la inclusión de un medio cognitivo como lo es la evidencia digital y en consecuencia, el cumplimiento de las condiciones normativas que desarrolla los medios probatorios correlacionados a esta tipología de medio cognitivo, con el único objetivo de brindar mayor seguridad jurídica en los procesos donde se encuentre involucrada una evidencia digital, que por su naturaleza debe ser obtenida por un perito forense digital.

Se extrajo, de la misma entrevista, un aparte donde se indica que la realidad y validez de las evidencias digitales se dan, con fundamento a la libertad probatoria, en muchos casos donde no se cuenta con un perito forense, pero sí con otros elementos materiales probatorios que permiten certificar la existencia de los hechos y acercar al juez a la verdad procesal, así:

> Pues la fiscalía trajo toda esa información obtenida de la entidad crediticia para poderla obtener válidamente como se trata de información que se considera privilegiada inicialmente debió acudir al juez de control de cuentas de garantías para obtener el permiso, la autorización de acceder a este tipo de información y obtenerla, una vez el juez de control de garantías les dio la autorización pidieron al banco que les informase cuales fueron las transacciones efectuadas desde esta cuenta a donde había ido a parar el dinero las cuentas receptoras y si era posible la dirección IP, o sea, si se lograba determinar desde que sitios se habían hecho las transacciones, a nivel del banco se hizo una investigación por el grupo de seguridad, ellos lograron detectar las transacciones fraudulentas y algunas direcciones IP, en varias ciudades de Colombia toda esa información se plasmo en un informe al cual asedio la fiscalía y una vez se obtuvo se volvió ante el juez de control de garantías a legalizar esta información y a verificar obviamente que no había extra limitación y que no se habían violado garantías fundamentales. Todo esto para qué?, para poder ingresar al juicio válidamente esta información todos estos delitos informáticos en muchos de los casos implica ac-

ceder a información privilegiada , entonces para poder elevarse a la categoría de delito toda esa información hay unos pasos previos que es acudir ante el juez de control y garantías para obtener toda esa información, ingresar a bases de datos si no se hace este procedimiento corre el riesgo de que la prueba sea excluida por violación de garantías fundamentales que es la sanción principal y así mismo la prueba que se derive sea prueba ilegalmente obtenida (…) una vez la fiscalía acudió ante el juez de control de garantías y legalizo todo el procedimiento, se seguro que puede acudir a la etapa del juicio, la etapa en la audiencia preparatoria ir como prueba toda esa información (…) en este caso en concreto, todos eso informes del banco ingresaron como prueba a la actuación pero, prueba digital propiamente no hubo, aquí no vino un perito forense informático para explicar que fue lo que paso, sino que simplemente se explicaron las transacciones fraudulentas y se tuvo que haber duplicado, plagiado la información privilegiada de las hermanitas, pero con solo esos escritos de la información de seguridad del banco, el despacho considero estructurada la materialidad de la infracción sobretodo, aquí en Colombia es un sistema de libertad probatoria (…) sin desconocer que lo ideal es que se cuente con un perito forense informático, recuerdo que algunos de los defensores se sustentaban que no se hubiese podido determinar la dirección IP, si embargo el despacho considero que lo importante era que de las cuentas había salido el dinero que todo la diferencia lógica o razonable que se imponía es que realmente habían plagiado el certificado digital y habían obtenido las claves de las hermanitas (…) ello se acreditó con que no tenían nada que ver con esta sustracción de sus dineros, entonces por la vía de la valoración probatoria el despacho logro reconstruir la materialidad de la infracción a pesar de que no se contó con un perito forense informático y lograr determinar a si la ocurrencia del hurto informático y la responsabilidad de todas las personas que recibieron el dinero en sus respectivas cuentas, las cuales no dieron una explicación debida frente a esas transacciones (…) entonces con un perito forense informático propiamente no se contó, fueron otros elementos materiales probatorios que le permitieron al despacho obtener un conocimiento cierto y seguro sobre ese delito de hurto informático, y en resumidas cuentas en Colombia, lo reiteramos, ante esa libertad probatoria, se puede acceder a la verdad por diferentes medios de conocimiento, sin embargo, es ideal o hubiese sido ideal en el caso en concreto, contar con un perito forense informático, esa es nuestra experiencia y finalmente el fallo fue condenatorio (…) el mismo fue apelado en el tribunal superior de Medellín frente a los reparos que se hacían enguanto a la dirección IP o a la acreditación en si del delito informático que se pensaba que tenía que ser por un perito forense informático, el tribunal, avalo la posición del despacho respecto a que existe libertad probatoria y se podía obtener de conocimiento con todos los elementos materiales probatorios aportados válidamente por la fiscalía porque ya había acudido ante el juez control de garantías y toda esa información fue válidamente obtenida desde el sistema informático del banco, en concordancia con los testimonios de la víctima y de las personas objeto de las transacciones realizadas en el hurto (Mejía, 2012).

Partiendo de la postura que expone la operadora judicial, es el informe pericial elaborado por un experto forense digital el que permite materializar el medio cognitivo de los hechos categorizado como mera evidencia, que una vez valorado por el juez control de garantías y adquiera su categoría de prueba, ésta se considera de mayor certeza y credibilidad en la demostración de un incidente informático, aunque se aclara que no debe ser un medio de prueba aislado, o la única prueba que deba tomarse, para ello se debe acompañar de otras pruebas como son el testimonio, interrogatorio de parte, documental, entre otros.

En un juicio el informe pericial se considera una prueba objetiva que permite indicar la ocurrencia de un incidente informático, sin embargo, ésta misma prueba responde de forma limitante ante el ámbito o espacio de tratamiento de la evidencia en relación a las limitaciones por imposibilidad judicial de apertura legal de archivos, *logs* o ficheros, (como deseen catalogarse toda vez que se han entendido como sinónimos), limitación que se fundamenta en la defensa de los derechos constitucionales a la intimidad y la información consagrados, en la Constitución Política de 1991 artículo 15 y 20 respectivamente, impidiendo generar una trazabilidad completa entre el punto emisor, trasmisor y receptor de la operación maliciosa o identificar un eventual almacenamiento indebido de malware.

El impedimento antes descrito en cuanto a la obtención de la evidencia digital, minimiza la posibilidad de indicar, únicamente desde la prueba pericial de un incidente informático, una autoría irrefutable del sujeto activo de la conducta; es por ello que los operadores judiciales deben dar validez a la información que se obtenga de testimonios e interrogatorios en el juicio, y deben valorar de forma integral todos los medios de prueba presentados, tengan o no soporte de un informe pericial forense digital, pues sólo así es posible reducir la impunidad sustentada, en muchas sentencias, con fallos absolutorios por falta de prueba forense digital.

Es también necesario resaltar que la libertad probatoria genera, para el derecho procesal penal, la inclusión de condicionamientos con los que se deben contar para que estas pruebas novedosas e innovadoras garanticen los principios probatorios y la protección de derechos constitucionales como la intimidad, la información y el debido proceso, principalmente, tal y como se plantea en la Unidad 6, al presentar la evolución que deben tener algunos artículos del Código Procesal Penal Colombiano.

b) Abogados

En cuanto a la obtención de información por expertos abogados se conto con varios entrevistados, sin embargo el doctor Hernán Darío Elejalde, quien es profesional en derecho e ingeniería de sistemas, fue el único abogado consultado que permitió dar publicidad de los resultados de la entrevista, teniendo en cuenta que la mayoría de ellos no se permite revelar su debilidad cognitiva en temas tan contemporáneos como es la investigación de delitos informáticos aduciendo entre otros aspectos la pérdida de credibilidad profesional, aunque fueron asequibles a dar la entrevista en el anonimato apelando a la relevancia del tema investigado. En consecuencia se procede a presentar el análisis de la entrevista en la presente unidad además de la validar las posturas con datos obtenidos de forma privada, y adicionalmente se complementará con los datos de entrevistas anónimas en la unidad 7 de conclusiones y recomendaciones que se fundan en datos obtenidos de forma confidencial.

Indica el abogado Hernán Darío Elejalde en su entrevista frente al primer objetivo los siguientes apartes:

> Considero que para la época actual si están bien tipificados, pero que el legislador por lo cambiante de la informática debe estar muy pendiente para tipificar nuevas conductas que son muy viables aparezcan en el tiempo y con los avances tan acelerados de la informática. Considero que si hay aspectos técnicos que pueden ser difíciles para un jurista, pero estos se deben apoyar en peritos expertos a la hora de tomar una decisión y que las pruebas recolectadas deben ser lo suficientemente claras para poder procesar una persona. Igual cuando empiece aparecer jurisprudencia al respecto y que muchos doctrinantes sigan opinando, se tendrá más claridad en lo que quiso decir el legislador a la hora de escribir la norma. Considero como lo dije en la primera pregunta que el legislador debe estar atento a las diferentes manifestaciones de delitos informáticos que se vayan presentando para irlas tipificando, pero que la Ley 1273 de 2009, está acorde a lo que pasa actualmente. Igualmente considero que falta capacitar más desde las universidades a las personas y estudiantes en el manejo técnico de las herramientas que día a día aparecen para evitar delitos informáticos, así como para detectarlos. De igual forma las universidades se deben comprometer en traer tecnología internacional que detectan los delitos informáticos para capacitar a los estudiantes en las mismas (López, 2011).

Desde otra postura doctrinal, al abogado, formado en las ciencias informáticas y del derecho, le es clara la consagración de los tipos penales, reconociendo que la informática en contraposición al Derecho es dinámica y evolutiva de forma imposible de medir, es por ello que su afirmación de la constante evolución del ordenamiento jurídico en aras de abarcar las formas delictuales desarrolladas en el mundo cibernético se convierte, más que una necesidad, en una realidad constante, dinámica, que fundamenta el trabajo de las personas dedicadas a la seguridad informática y a los expertos forenses digitales en correlación con la ciberdelincuencia.

Frente al objetivo 2:

> Lo primero es que en la informática, así como en cualquier tipo penal se debe conservar la cadena de custodia, siendo en esta más difícil ya que la prueba se debe manipular directamente. Lo más importante es demostrar que la prueba no fue alterada ni manipulada, aspecto que se puede evidenciar con el hardware y software que se tiene hoy en día. De igual manera la Ley 527 de 1999 ayuda en lo probatorio frente a los mensajes de datos que tienen o no firma electrónica, donde si se comprueba que desde la salida y llegada de un dato este no fue manipulado, tiene validez (…) la evidencia digital si se puede equiparar a un documento, siempre y cuando cumpla con dos características esenciales la integridad y la autenticidad que se garantizan con el manejo de la firma digital, que no es más que el manejo de un par de claves: una pública y una privada, que combinándolas de forma adecuada garantizan estas dos características. En algunos casos como los cheques y las escrituras públicas, la ley no acepta el documento electrónico (López, 2011).

Esta postura evidencia el reiterado conocimiento de los abogados frente a los diferentes medios probatorios en materia de delitos informáticos, donde, sin desconocer la competencia de los abogados y mucho menos del entrevistado, la completitud de las pruebas pertinentes en un proceso penal, en materia de delitos informáticos, no es de todos los abogados, mucho menos de los que

no poseen conocimiento técnico en el campo informático, pues muchas veces se desconoce que el tipo de prueba reina es la documental, previendo la lista de medios probatorios relacionados en el Artículo 424 del Estatuto Procesal Penal, el cual sustenta la realidad, que de forma reiterada, se ha evidenciado en las diferentes unidades del presente texto; la mayor amenaza en el manejo de los delitos informáticos, respecto del campo probatorio, es la falta de capacitación y conocimiento respecto a las implicaciones probatorias que se poseen, frente a los medios probatorios tradicionales y su aplicación en el campo del ciberdelito.

Frente al objetivo 3:

> Considero que no se requiere mucha experticia en este aspecto si el documento trae una firma electrónica, el problema si estaría si la prueba no viene con esta firma, ya que se tendría que evidenciar de donde salió el dato, donde llegó y que no se haya modificado. La firma electrónica garantiza esto (…) en algunos casos si se requeriría de la experticia de otro profesional, ya que la informática tiene muchos programas, bases de datos, sistemas operativos y el mismo hardware donde hay expertos para cada tema (López, 2011).

Cabe resaltar que hasta el momento, de forma reiterativa, todos los entrevistados han destacado la importancia de la firma digital o electrónica en materia de evidencias digitales, ya que sólo en el mundo digital se puede vincular el autor a un documento a través de una firma; en consecuencia, en Colombia, tal y como lo plantea la Ley 527 de 1999 y su Decreto Reglamentario 1747 de 2000, existe validez de la firma digital o electrónica como instrumento legal vinculante, sin embargo, no siempre las evidencias digitales cuentan con el cumplimiento de este requisito, por lo cual, toma importancia indicar que no sería sólo la evidencia digital el único medio de conocimiento en un proceso, pues es necesario que el caso se encuentre fundamentado en varios medios probatorios como los testimonios, interrogatorios, inspecciones judiciales y demás, que permitan denotar la existencia fáctica de las circunstancias que se alegan en el caso penal, con la finalidad de llevar al juez de conocimiento a la verdad procesal.

Frente al objetivo 4:

> Frente a esta pregunta es poco lo que conozco. Pero como lo he dicho en toda la entrevista lo importante para la valoración de la prueba sea por parte del juez de control de garantías o del mismo ente acusador, lo importante es demostrar que la prueba no fue modificada ni alterada, lo que se logra con la firma digital o con programas que extraen la información de los equipos así estos hayan sido formateados (…) tampoco conozco mucho al respecto desde lo práctico, pero reconozco que la mejor forma de evitar su alteración es a través de la firma digital (López, 2011).

El desconocimiento de los protocolos forenses digitales, su aplicación y validación en un caso penal de delitos informáticos, por los abogados contractuales, no puede considerarse reprochable pues no conocen de la temática por parte de los fiscales, jueces y demás terceros intervinientes en representación del Estado como lo son los defensores públicos; de ello queda evidencia en

las encuestas aplicadas en la investigación realizada en el proyecto, este desconocimiento reiterado plantea dos visiones, una direccionada al campo de la capacitación, donde se reafirma que sólo son competentes las personas que por sus propios recursos se logran capacitar o si se encuentran adscritos a las unidades de delitos informáticos de la fiscalía y la policía, en contraposición, que Colombia se encuentra clasificado como el quinto país donde se cometen delitos informáticos, siendo esta correlación fundamento notorio para afirmar que existe una gran deficiencia en materia de capacitación sobre el tratamiento de los ciberdelitos, tanto en el campo investigativo como en juicio; otra visión es la inseguridad jurídica que se genera en un caso penal, en cuanto a la forma en que se desarrolla un caso penal donde se involucren delitos informáticos y la necesidad de evidencia digital como medio de prueba, siendo al momento de aportación y presentación de la prueba ante el juez no es clara los elementos de forma que debe respetarse para la presentación, sustentación del informe pericial, para que posteriormente, al momento de valoración judicial, se logre el convencimiento del juez en la ocurrencia del incidente informático y la relación autoral que el sindicado tenga.

c) Expertos forenses

Se cuenta también con una sola entrevista pública a expertos forenses, teniendo en cuenta que en este campo sí que es evidente el grado de confidencialidad en la información que se puede obtener, por esta razón se eligió a una de las personas más reconocidas en el medio de la informática forense, el Ingeniero de Sistemas Manuel Alberto Santander (Santander, 2012), con formación a nivel de Maestría en Administración de la Universidad EAFIT y Master of Science in Information Security Engineering (MSISE)- SANS Technology Institute, actualmente es Coordinador de Seguridad de la Información en EPM:

Frente al objetivo 1:

> Sí hay interceptación de comunicaciones en cuanto a los contenidos, el acceso a claves para la suplantación, acceso abusivo del sistema informático. Hay integralidad para sancionar penalmente con estos delitos y no sé si cuatro años son suficientes ya que la legislación puso este tope para que estos delitos no fueran excarcelables (…) básicamente que los delitos son de dos clases informático que es la violación de la información consignada en las computadora y que el medio informático sea un vehículo para cometer algún tipo de delito, los tradicionales involucran otros bienes que se consideran agravantes dentro de los delitos consagrados en la ley (…) no por que cambiaron los tipos penales, la sanción, pero el código de procedimiento penal quedo igual, y por consiguiente no quedo regulado, sigue siendo de total interpretación del juez que este conociendo un caso. Creo que debería modificarse el código para que estos delitos quedaran consagrados y tomar en cuenta los diferentes tipos de evidencia informática, porque en la actualidad se debe tener un soporte físico de una evidencia informática (…) yo dejaría así los tipos penales (Santander, 2012).

Los tipos penales consagrados en la Ley 1273 de 2009, tal y como se evidencia en la totalidad del texto, tienen sustento y validez en tanto su creación fue dada desde la Convención de Budapest; recuérdese la postura expresada en esta unidad por el autor y proponente de la ley y su aplicación en

el entorno colombiano que no ha dado notorio desarrollo jurisprudencial y doctrinal que permita, de forma categórica, afirmar que estos tipos penales son insuficientes o susceptibles de ser modificados para aumentar su efectividad.

Por lo anterior, existe una postura reiterada, y en igual sentido opina el entrevistado, de que el estatuto procesal penal, el cual permite la aplicación del estatuto penal sustancial de forma sistemática y armónica, debe ser objeto de evolución en aspectos probatorios.

Frente al objetivo 2:

> No tiene, desconoce la existencia de la prueba de tráfico de datos, de medios de almacenamiento, no dice cómo proceder y le da discrecionalidad al juez y al fiscal para que lo admita o no lo admita como delito. No, porque como se menciono anteriormente se deja a la discrecionalidad de los jueces y fiscales la admisión de dichas pruebas (…) no hablo de mensajes de datos sino de medios de almacenamiento ya que el anterior es diferente y no se presenta almacenamiento. Porque el mensaje de datos es una abstracción distinta de comunicación entre dos entes (…) no porque no consagra. El manual de la cadena de custodia de la fiscalía, no consagra cuales son las operaciones que se deben realizar para obtener una imagen, en qué términos, las posibles excepciones que se deben tener en cuenta cuando hay un problema de hardware, cuando el medio de almacenamiento es excesivamente grande y no se pueden sacar evidencias parciales (…) la verdad es única pero las realidades son distintas, se diría que la verdad hay que encontrarla, y se encuentran porciones de esa verdad. Depende cien por ciento del conocimiento (Santander, 2012).

Frente a los medios de prueba es necesario destacar que por el especial conocimiento del entrevistado este tiene una postura frente al aspecto probatorio cuando indica que tal y como se encuentra el desarrollo normativo en el campo procesal penal, el criterio de validez o no de una evidencia digital queda a criterio de la valoración probatoria que haga el juez control de garantías y posteriormente el de conocimiento. Adicionalmente, reconoce la falta de desarrollo en materia de cadena de custodia, denotando la deficiencia en la regulación de la técnica y protocolos para la recuperación de la evidencia digital, es por ello que, entre otros aspectos, la evolución del sistema procesal penal es urgente.

Frente al objetivo 3: “El consagrado en la norma NIST SP800-61, es un estándar que se utiliza a nivel Interpol” (Santander, 2012).

En materia de protocolos forenses digitales es reiterada la aplicación de protocolo formulado por el Instituto NIST, entre los cuales encontramos el protocolo denominado NIST SP800-061 y el NIST SP800-086, ambos responden a la necesidad que la evidencia digital sea obtenida respetando las características de: autenticidad, confiabilidad, integridad, originalidad y no repudio, con el objetivo de poder certificar la no alteración de la evidencia que por su naturaleza es volátil y susceptible de ser alterada, muchas veces de forma involuntaria. Es por ello que Colombia debería reglamentar, apelando a que es un ordenamiento de la ley escrita, la idea de acoger un protocolo estándar o promover el desarrollo de un protocolo con adecuación al ordenamiento jurídico colombiano.

Frente al objetivo 4:

> El consagrado en la norma NIST SP800-61, es un estándar que se utiliza a nivel Interpol (…) básicamente se manejan dos cosas: primero cuando uno no está investigando se podría escribir sobre el medio de almacenamiento y se podría caer gran parte de la información ya que usted misma la sobre escribe y segundo como usted adquiera esa evidencia, porque se puede adquirir con el equipo apagado o con el equipo prendido, y dependiendo de las circunstancia si se adquiere con el equipo prendido eso involucra una seria de implicaciones que a la hora de el análisis podrían llegar a pesar. Ya que es muy difícil probar que uno no interrumpe los procesos físicos de una máquina (Santander, 2012).

De forma reiterada, y se expresa en el desarrollo de la Unidad 3, el protocolo y las técnicas forenses en concordancia con los principios para la recolección de la información para la evidencia digital, requieren en muchos casos de especialidad en su aplicación, experiencia del sujeto encargado de la prueba, y finalmente, el cumplimiento de características a la evidencia digital, con el fin de que las etapas de obtención, preservación, almacenamiento, análisis y presentación en juicio puedan darle al experto forense un elemento material probatorio objeto de análisis forense con el cumplimiento de garantías constitucionales, y legales; en consecuencia, la posibilidad de dar sustento con su informe como prueba pericial, superando entre otros trámites procesales la prueba testimonial, donde sea el mismo perito quien sustente la obtención de la prueba, valide y certifique su experiencia, protocolos, principios y técnicas aplicadas, y que ante el interrogatorio de la contraparte procesal no se invalide esta, dejando como consecuencia, en muchos casos, al juez, con la sola posibilidad de dictar una sentencia absolutoria o desestimar un juicio por falta de pruebas o de elementos materiales probatorios válidos.

Frente al objetivo 5:

> El código de procedimiento penal no establece el protocolo en juicio. Lo único que existe es lo que tiene establecido la fiscalía porque el protocolo de la policía no es oficial, ya que esto se vuelve un tema subjetivo y se dirige a la discrecionalidad de los jueces (…) los forenses tienen protocolos internacionales autorizados (Santander, 2012).

Finalmente, en el análisis sobre la postura del entrevistado lo indicado en materia de aplicación de protocolos ratifica gran parte de los postulados desarrollados en las diferentes unidades temáticas, dejando como conclusión dos aspectos, el primero, Colombia no ha acogido un protocolo y herramienta forense digital estándar o en su defecto no lo ha desarrollado para la investigación y obtención de evidencias digitales, a pesar de la notoria necesidad y urgencia, para brindar mayor seguridad jurídica en materia de pruebas periciales; el segundo es la capacitación con apoyo de las Instituciones de Educación Superior, la evolución del Instituto de Medicina Legal y Ciencias Forenses frente a la promoción y conocimiento de la disciplina forense digital en Colombia, con los aspectos que esta misma involucra, entre otros, certificar protocolos aplicados, certificar laboratorios y certificar, si es posible, la experiencia y profesionalidad de peritos.

A continuación se incluyen los aspectos obtenidos bajo reserva de confidencialidad, por parte de funcionarios públicos y entes privados que involucran jueces de control de garantías, fiscales de las unidades de apoyo, investigadores de las unidades de delitos informáticos (fiscalía y policía), abogados y defensores públicos, al igual que expertos forenses digitales del campo privado; vale la pena destacar que son estos sujetos los de mayor competencia en el conocimiento, la profesionalidad y la experiencia para el campo explorado de la disciplina forense digital.

Para mayor claridad al lector este aparte se estructura con la indicación de posturas breves dadas por personas cuyas identidades están bajo confidencialidad; solamente se hará mención de la información que pertenece al dominio público.

1. En Colombia existe desarrollo a nivel académico, investigativo y doctrinal; un "análisis" de forma separada de la temática de delitos informático, y la temática de la informática forense, existiendo una gran deficiencia frente a la interrelación de ambas, siendo de gran pertinencia, pues sólo así se logra dar sustento a un conjunto macro tanto de delitos como la parte forense y la parte forense desde la temática de laboratorios, y protocolos.

2. Una de las grandes falencias en juicio es que no todos los jueces tienen conocimiento del área informática, hasta ahora se están empapando de esto, muchas veces evaden procesos de esta naturaleza porque no saben cómo cumplir con un tratamiento adecuado en el juicio.

3. La mayoría de funcionarios expertos en forense digital, y que se encuentran asignados en las unidades de delitos informáticos, son personas de origen bogotano, ya que hace cinco años se realizó un concurso con trescientos servidores que se presentaron a una convocatoria pública realizada por Internet y que dejó en evidencia que la gran mayoría eran originarias de la capital; la institución decidió distribuirlos por todo el país, y por tal motivo, en todas las unidades de delitos existentes se verán funcionarios de muchas regiones,

4. Las certificaciones que poseen los funcionarios no son siempre las más relevantes como las del NIST y SANS, pero internamente el trabajo de los expertos forenses se valida desde la competencia en solución de casos, a nivel de experiencia, sin embargo, los jefes de las unidades de delitos informáticos sí son obligatoriamente certificados a nivel internacional. Es de aclarar que todo el personal que se encuentre involucrado en una unidad de delitos informáticos debe tener certificación en el uso de herramientas y protocolos forenses, en consecuencia, pueden ser peritos forenses en juicio, sean tanto del campo público como privado, siendo los primeros de forma obligatoria y los segundos en las condiciones contractuales.

5. En una unidad de tratamiento de delitos informáticos pueden existir varios peritos y cada uno con un rol distinto, por ejemplo, en unidades de delitos informáticos del campo público se cuenta con dos perfiles o roles, el perfil de investigador que trabaja en campo y el perfil de perito que trabaja en el laboratorio, teniendo en cuenta que la investigación se inicia y se termina con la misma investigación, desde cero, desde la denuncia; o como gerentes de investigación que realizan recolección de evidencia digital necesaria o requerida, al igual que recolección de información, acompañado de entrevistas, allanamientos, seguimientos, encubiertos y demás actos que impliquen la investigación

de casos urgentes, para que se deban seguir unos protocolos, y la cadena de custodia donde se presenta la etapa del embalaje, se entrega al almacén o se pone a disposición del fiscal para que ellos tomen la decisión si la mandan para el laboratorio para el análisis forense digital o se requiere completar la evidencia con autorización del juez control de garantías, finalmente se debe elaborar el informe y la evidencia digital se conserva en el almacén.

6. En el campo público, si la investigación comenzó en el CTI la termina el CTI, si la inicia SIJIN termina la SIJIN, sin embargo, la norma procesal penal permite que en un acto urgente haya iniciado por la SIJIN, pero el fiscal de investigación puede asignar como policía judicial al CTI para que continúe la investigación y quede como caso del CTI, es allí donde será la unidad de delitos informáticos del CTI la encargada.

7. Cuando en los casos a procesar se encuentran implicados servidores de algunas de las entidades (CTI y SIJIN) entonces la investigación la hace la otra entidad.

8. Cuando son casos de connotación nacional se trabaja en cooperación entre la fiscalía y la policía judicial, se trabaja como una sola unidad, donde pueden participar miembros de toda la policía judicial e inclusive a nivel de trabajo en laboratorios, apelando al interés general, sobre el particular.

9. En los últimos cinco años la ciberdelincuencia ha generado un incremento en el comportamiento del crimen electrónico en materia de robo de propiedad intelectual, focalizando al tema corporativo y el tema de ataques y robos a través de Internet, el crecimiento ha sido exponencial y se espera que sea mayor en los próximos años. En el último informe del FBI se habla de un crecimiento bastante grande en el tema de creación de Malware, tanto como herramienta de ataque y como creación de herramientas de acceso; el fraude se ha ido reduciendo durante los últimos años.

10. Son empresas del campo privado utilizadas como fachadas para la comisión de delitos electrónicos como lavado de activos y hurto informático.

11. Los ex agentes de entidades gubernamentales son precisamente los promotores del espionaje corporativo; y usan la misma tecnología del gobierno, en materia de asuntos tan delicados como las herramientas tecnológicas aplicadas, especialmente las de infecciones tan conocidas como los Troyanos, de muy alto nivel, desarrollados precisamente para utilizar protocolos alternos de afectación, ofuscación, entre otras, incluyendo técnicas muy avanzadas de acceso a la máquina a través de las redes de procesadores y otros programas a través del hardware.

12. La ciberguerra, en comparación con el cibercrimen, el cual está motivado por el lucro económico, está motivada por preceptos políticos, con la finalidad de atacar a otro país; es por ello que ahora el cibercrimen y la ciberguerra están cogidos de la mano.

13. La evidencia digital en Colombia se empezó a trabajar con el caso del ataque al campamento de Raúl Reyes, en la actualidad, el negocio de la evidencia forense tiene un gran incremento en el mercado corporativo, con la intervención de investigaciones que se llevan a cabo con entidades privadas, donde se evidencia que entre las nuevas técnicas se da el rompimiento de claves, ya no de manera reactiva si no proactiva, e incluso nuevas técnicas para sacar información por la web a través de la basura corporativa.

14. La Academia Nacional de Ciencias Forenses Americana se dividió en dos ramas: a. una como violencia digital para el tema de cómputo y b. multimedia en el análisis de video y audio que puedan ser digitalizadas.

15. En Colombia Certicámara S.A. es quien maneja los registros digitales y estampados cronológicos del sistema, registro muy utilizado por compañías que les ponen una huella hash matemática a los archivos, para identificar si alguien les hizo algún cambio.

16. La norma técnica 11-1725, ISO, dada para el laboratorio forense, es de obligatorio cumplimiento, incluyendo los de tratamiento de evidencia digital.

17. Sobre el tema de la información en la nube no se trata únicamente de elementos económicos o elementos tecnológicos, además del agravante en cuanto a la inmadurez en el componente jurídico, entonces a la medida que estamos en un mundo Interrelacionado, en un mundo globalizado, hoy ya no es la aplicación de normas nacionales sino internacionales, determinando que nuestras organizaciones adopten una serie de estándares que permitan tener presencia y preservación al derecho a la intimidad y el derecho a la información.

18. En las organizaciones no solamente las cámaras de vigilancia controlan la vida privada, muchas controlan la vida pública que puede ser filmada; por esta razón se ha creado la afirmación de que “la privacidad ha muerto”, se genera con fundamento al mal uso de la información personal obtenida por medios cámaras e incluso Malware (keylogger o spyware), donde los datos de grabación muchas veces son obtenidos y usados para beneficio propio o de un tercero sin tener fundamento o autorización legal para hacerlo, convirtiéndose en una prueba fílmica ilegal o susceptible de ser anulable.

19. En materia de manipulación y administración de información, las normas que regulan cuando se hacen análisis forenses de cumplimiento, con el objetivo de que las organizaciones cumplan con estándares de certificación ISO 27001 a 27002, los cuales no establecen políticas específicas del tratamiento de la información. Adicionalmente, teniendo en cuenta el Artículo 15 y el Artículo 20 de la Constitución Política de 1991, que trata el derecho a la intimidad y de la protección de datos frente al derecho a la información, las organizaciones rara vez se oponen a un juicio de proporcionalidad frente a la situación de vulneración de estos dos derechos, teniendo en cuenta que el alcance de la Ley 1266 de 2008 frente a la nueva ley de delitos informáticos va más allá.

20. En Colombia el panorama se complicó por la expedición de la Ley 1273 de 2009, la cual introduce al ordenamiento jurídico el delito informático, se materializa cuando hay violación de datos personales como tipificar una conducta cuando se sustrae, vende, manipula, intercambia, compra, intercepta, comercializa cualquier tipo de información sin autorización de la persona o el simple acceso abusivo a un sistema de información; o algo más básico como una cuenta de correo electrónico. En Colombia, si bien existen unas normas legales de reciente creación, se puede decir que el desarrollo jurisprudencial, desde el año 1991, no tiene nada que envidiarle a Europa pues su alcance normativo ha hecho frente a estos derechos fundamentales y sirve, además, para enriquecer otros procesos.

Como análisis concluyente a modo de triangulación de posturas se presenta una tabla comparativa categorizada por variables temáticas, y permiten identificar las posiciones de cada uno de los actores: juez, experto forense, abogado (contractual y defensor público) permitiendo concretar el comportamiento de la interrelación científica, el Derecho, la Informática y Forense. A continuación se presenta el ejercicio de análisis a modo de trazabilidad:

Concepto	JUEZ	EXPERTO FORENSE	ABOGADO (contractual y defensor público)
Tipos Penales E Interpretación	Generalmente es un sujeto procesal que creen suficiente la existencia de los tipos penales informáticos para investigar cualquier tipo de conducta delictiva, sea cual fuere la modalidad de ataque, sin embargo, se manifiesta que aún es un ámbito con poco desarrollo doctrinal y jurisprudencial que permitan una mejor aplicabilidad de los tipos penales, ello dificulta en algunos casos su judicialización.	El grupo de tipos penales por ahora son suficientes para individualizar y judicializar cualquier tipo de conducta penal, pero cabe resaltar que el experto forense, en la tarea investigativa del incidente es quien valida una modalidad delictiva que se pueda adecuar. Por otro lado, lo preocupante es el rango mínimo de pena por 4 años se debiera ser repensado toda vez que, un delincuente informático puede ser altamente dañino.	De acuerdo a la época actual si están bien tipificados, pero el legislador, como respuesta a la dinámica comportamental de la sociedad y los criminales, deben estar pendientes para tipificar nuevas conductas que aparezcan en el tiempo y con los avances tan acelerados de la informática
Evidencia Digital	Es una figura del derecho sustancial procesal que responde al cumplimiento de requisitos formales y materiales para su existencia y valor probatorio dentro del proceso penal como prueba documental, uno de los requisitos que se debe lograr acreditar es la integridad y autenticidad del documento, que de acuerdo a los artículos 430 y 431 del código de procedimiento penal se excluyen como medio de prueba los documentos (evidencia digital obtenida en un proceso de investigación forense) que no individualicen el autor, su ausencia lo convierte en documento anónimo, el juez debe NO admitirlo como prueba documental, a pesar de la existencia de libertad probatoria, la evidencia digital si tiene que darse cumplimiento a los requisitos de ley y preservar derechos y garantías fundamentales como son la intimidad y la información, por lo tanto el documento que se quiere hacer valer como prueba dentro de juicio oral entonces se puede acceder a la información que consagra, recapitulando otros medios probatorios que admite el código, sin embargo, cuando se quiere hacer valer como medio probatorio particular una evidencia digital tiene que darse cumplimiento estricto a los requisitos señalados en la ley para que se pueda elevar a la categoría de delito, la conducta investigada, siendo prevalente la integridad y autenticidad de ese documento.	En el ámbito colombiano solo cambio los tipos penales, la sanción, pero el código de procedimiento penal se encuentra sin haberse modificado, y por consiguiente no quedo regulado, sigue siendo de total interpretación del juez que este conociendo un caso, y los diferentes tipos de evidencia informática en la actualidad se debe tener un soporte físico de una evidencia informática, lo cual podría entenderse como una forma material que descontextualiza la evidencia digital desde su origen digital.	la evidencia digital si se puede equiparar a un documento, siempre y cuando cumpla con dos características esenciales la integridad y la autenticidad que se garantizan con el manejo de la firma digital, que no es más que el manejo de un par de claves: una pública y una privada, que combinándolas de forma adecuada garantizan estas dos características. En algunos casos como los cheques y las escrituras públicas, la ley no acepta el documento electrónico. Consideran que en principio no se requiere mucha experticia en la extracción de la evidencia, siempre y cuando el documento posea una firma electrónica, que permita vincular al autor con la prueba obtenida, para evidenciar de donde salió el dato, donde llegó y que no se haya modificado. La firma electrónica garantiza esto.

Protocolo forense	El protocolo forense, sea ése nacional o internacional debe aplicarse respondiendo a lineamientos legales y no políticos como ocurre en operaciones de inteligecia y contrainteligencia, donde los tratados internacionales firmados para cooperación en la lucha contra el terrorismo y el delito no se respeten en una operación de Gobierno podría invalidar las pruebas por mas protocolo forense certificado que se haya aplicado. "En Colombia es evidente que no existen abundantemente abogados con especialización en nuevas tecnologías y menos en informática forense, como tampoco todos los ingenieros tienen especializaciones en Ciencias Penales, Constitucionales o en Derecho Procesal o son abogados a la vez, permitiéndonos colegir que la mayoría de las veces el aporte colectivo e integral de estos dos profesionales preferiblemente deberían estar presentes ante un caso de **DELITOS INFORMÁTICOS**" (se extrae de la entrevista por ser un concepto concurrente en los jueces consultados). Adicionalmente en materia de extracción y fijación de la evidencia digital, se requiere no solo el conocimiento de la técnica que así lo permite son la competencia cognitiva para valorar el hallazgo e identificar el incidente, y que respete las Garantías Constitucionales y Legales.	El código de procedimiento penal no lo regula de forma expresa un protocolo determinado, es por ello que desde la prueba pericial se debe validar la existencia como medio probatorio. En el ámbito de los expertos forenses, no es solo el conocimiento académico lo que genera la competencia en el manejo de un protocolo forense determinado, lo hace también la experiencia en solución de casos específicos.	Frente a los protocolos forenses se parte de la base que es la minoría de abogados lo que se encuentran cercanos a este elemento. Lo que se conoce o reconoce de ella es que, para fines de la valoración de la prueba por parte del juez de control de garantías o del mismo ente acusador, lo importante es demostrar que la prueba no fue modificada ni alterada, lo que se logra con la firma digital o con programas que extraen la información de los equipos así estos hayan sido formateados.
Incidente informático	En el momento de realizar valoración probatoria se debe proceder haciendo una revisión de evidencia digital, verificando el tratamiento forense aplicado, el cumplimiento de la cadena de custodia frente a los elementos probatorios presentados y que ha realizado el forense (no necesariamente tiene que ser policía judicial, como muchos creen) la revisión debe abarcar detalladamente: la captura o extracción y fijación, la toma de los datos volátiles, de los metadatos, y el estampado de la huella hash, que todos estos aspectos logren dar cuenta de la transparencia, integridad y autenticidad de su obtención, podrá ser objetivo de declaración judicial como prueba legal. Igualmente, como postura originara del juez Alexander Diaz, es obligatorio, antes de realizar la examinación de la prueba, realizar un control de legalidad y Constitucionalidad, que responde a "la solicitud de legalidad previa de acceso a los ficheros con datos personales ante el Juez de Control de Garantías Constitucionales", para lograr garantizar el derecho fundamental que tienen todos los ciudadanos, el de HÁBEAS DATA.	El incidente informático debe tratarse a modo investigativo con protocolos que sean avalados y certificados, esto con la finalidad de aportación en juicio, uno de los mejores protocolos a aplicarse es el consagrado en la norma NIST SP800-61, es un estándar que se utiliza a nivel Interpol.	En algunos casos si se requeriría de la experticia de otro profesional, ya que la informática tiene muchos programas, bases de datos, sistemas operativos y el mismo hardware donde hay expertos para cada tema.

Instrumentos cuantitativos[2]

La preponderancia del modelo de investigación cuantitativo sobresale en la implementación de instrumentos y estrategias de análisis y recolección de información de este corte. El instrumento empleado fue la encuesta estructurada, la cual se define como un método de obtención de datos mediante consulta individual, en la que el encuestado proporciona información de forma voluntaria y consciente, como respuesta a una serie de preguntas planteadas en el cuestionario (Jiménez Marques, 2004).

La encuesta materializa un procedimiento sistemático de recolección de datos facilitados por los encuestados, recoge información sobre uno o varios temas, permitiendo que la información obtenida corresponda a una muestra de la población investigada. Las encuestas permiten obtener información sobre características puntuales del objeto de estudio que se investiga, pueden ser socioeconómicas, opiniones, actitudes y motivaciones del público objetivo.

La encuesta puede ser diseñada específicamente para el estudio que se va a realizar, denominándose *ad hoc* o estándar, esto es, encuestas cuyo diseño ha sido previamente establecido y el tipo de información es uniforme para todos los suscriptores, caso que será adoptado en la investigación.

La encuesta cerrada fue el instrumento implementado a la mayoría de la muestra poblacional seleccionada en la investigación, y como tal, se estructuró por preguntas estrictamente cerradas mediante las cuales se proporcionaba la posibilidad de respuesta sin dejar margen de ampliación o justificación para el indagado.

Descripción de las encuestas cerradas

A continuación se detalla la muestra poblacional seleccionada para la aplicación de los instrumentos de consulta cerrada y la elaboración de las encuestas aplicadas como la fase de trabajo de campo de corte cuantitativa empleada en la investigación.

Población y muestra

La población se refiere a la globalidad de individuos que tienen ciertas características similares o sobre los cuales se desea hacer inferencia del conocimiento indagado. La recolección de información por medio de la aplicación de instrumentos de consulta toma como base la población y la muestra señaladas; para la investigación la población está integrada por informantes claves del escenario informático forense.

[2] Ver Unidad 8. Anexos: formato de encuestas: fiscales; abogados y defensores público; jueces

Algunos investigadores distinguen las diferentes modalidades de población en dos grupos: población blanco u objeto, y población accesible. La población blanco u objeto es aquella que el investigador desea estudiar, acerca de la cual el investigador desea hacer la generalización y que es de difícil acceso. La población accesible es aquella que reúne los criterios de inclusión, debe ser representativa de la población, está limitada a una institución, comunidad o región (Hernández et al., 2006), descripción que se acopla a la población seleccionada en el presente proyecto de investigación por tratarse de un tema de naturaleza pública, de seguridad y de innovación en el cual, desde los delitos informáticos, como categorías preestablecidas de investigación, se abordan las dinámicas tendientes a establecer la evidencia digital requerida para dar soporte probatorio a la comisión de delitos informáticos proferidos mediante la Ley 1273 de 2009 en Colombia.

Por ello, la población delimitada para la investigación reúne profesionales involucrados con la informática forense en Colombia, estos son, fiscales, jueces, abogados y defensores públicos. Todos ellos fueron trabajados como población accesible a partir de la cual se constituyeron muestras poblacionales específicas a partir de los trámites y contactos adelantados durante el trabajo de campo para facilitar su consulta. La muestra poblacional accesible con la cual se trabajaron las encuestas cerradas se circunscribe a los municipios que integran el Área Metropolitana del Valle de Aburrá y Envigado.

Fiscales: señala la Constitución Política en su Artículo 250, modificado por el Artículo 2 del Acto Legislativo 3 de 2002:

> La Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas que indiquen la posible existencia del mismo. No podrá, en consecuencia, suspender, interrumpir, ni renunciar a la persecución penal, salvo en los casos que establezca la ley para la aplicación del principio de oportunidad regulado dentro del marco de la política criminal del Estado, el cual estará sometido al control de legalidad por parte del juez que ejerza las funciones de control de garantías. Se exceptúan los delitos cometidos por Miembros de la Fuerza Pública en servicio activo y en relación con el mismo.

Por ser los fiscales los funcionarios que tienen la tarea de entregar a la justicia a los que violan las leyes del país, investigar las conductas que se adviertan como delictivas y acusar, ante los jueces de conocimiento, a los posibles responsables presentando los elementos probatorios que soportan las investigaciones; su intervención se hace necesaria para el conocimiento y comprensión de los delitos informáticos y establece la evidencia digital requerida para dar soporte probatorio.

Jueces: dice el Artículo 19 de la Ley 906 de 2004: “Nadie podrá ser juzgado por juez o tribunal ad hoc o especial, instituido con posterioridad a la comisión de un delito por fuera de la estructura judicial ordinaria”, por lo que la comisión de las conductas punibles tipificadas en la Ley 1273 de 2009 cuentan con una autoridad encargada de recibir la investigación adelantada por los funciona-

rios de la Fiscalía General de la Nación como los contraargumentos expuestos por la defensa. Esto es, la autoridad competente en Colombia para resolver y valorar en Derecho la realización de las conductas tipificadas como delitos informáticos es el juez, y él, se encarga del direccionamiento del proceso que determina la existencia de la comisión.

Abogados: como profesionales del Derecho, los abogados elegidos del universo poblacional existente son aquellos que tienen énfasis o especialidad en el área penal o probatoria. De esa manera se asegura una fuente de información esencial que trabaja de forma directa con las autoridades oficiales en los procesos que pueden involucrar la comisión de las conductas descritas como delitos informáticos, y a su vez, contribuir al esfuerzo por establecer la evidencia digital requerida para dar soporte probatorio.

Defensores públicos: similar justificación encuentran los defensores públicos, abogados de oficio al servicio del Estado para asumir la defensa de aquellos casos que no cuenten con abogado que represente al investigador en el proceso, y se garantice así el debido proceso, la defensa técnica y el ejercicio de contradicción.

Aplicación y Resultados de las Encuestas Cerradas

Las encuestas aplicadas a los distintos perfiles tomados como muestras poblacionales para la investigación, parten de un derrotero o modelo común que sólo sufre variaciones en casos puntuales por motivos justificados, esto es, cambio o adición de preguntas a las que se reiteran en todos los instrumentos debido a la especialidad de la actividad que desarrolla cada operador en particular.

Las encuestas fueron elaboradas en común partiendo de un encabezado introductorio con datos generales de la investigación, con el propósito de informar y contextualizar a los distintos encuestados. Posteriormente cada instrumento registró algunas preguntas de referencia personal para facilitar el reconocimiento y categoría de la muestra indagada. En todos los casos se preguntó por el sexo del consultado, pero se reservó la identidad para facilitar mayor confianza y seguridad al momento de diligenciar el instrumento.

En el caso de los abogados se preguntó por su título profesional, título de posgrado en caso de haberlo cursado o estarlo cursando, actividad laboral que desempeña y municipio donde ejerce. En el caso de los jueces se preguntó el número del juzgado y el municipio, datos que se mantuvieron en el caso de los fiscales.

Seguidamente todas las encuestas fueron elaboradas a partir de los objetivos específicos como derroteros temáticos que sustentaban las preguntas realizadas. Ello quiere decir que cada encuesta contó con cinco grupos de preguntas que se corresponden con el número de objetivos trazados para la investigación. Como se mencionó, todas las preguntas fueron cerradas en dos modalidades:

pregunta de afirmación o negación del supuesto, donde el consultado se limitaba a responder sí o no frente a un postulado planteado como interrogante; y pregunta de valoración, donde de acuerdo a una escala de correspondencia previamente propuesta en el instrumento, el consultado manifestaba el grado de aceptación que tenía frente al supuesto presentado.

Desde el objetivo específico, consistente en la presentación del grupo de tipos penales informáticos existentes en la Ley 1273 de 2009 y la legislación complementaria, la encuesta propuso una serie de interrogantes frente al reconocimiento, divulgación, suficiencia, redacción e interpretación de los denominados delitos informáticos. Las preguntas se incrementan en número para la muestra poblacional de jueces debido a la especial relación que tienen o pueden tener frente a esos tipos penales, por lo cual se les preguntó si han conocido procesos sobre el tema o han proferido imputación de un tipo penal de esa naturaleza.

En lo referente al objetivo tendiente a listar los medios probatorios existentes a partir de la Ley 906 de 2004, que son generalmente aceptados en Colombia, y evidenciar cuáles son o se pueden presentar como evidencia digital o física en relación con un tipo penal informático, las preguntas dirigidas a los abogados se enfocaron en la pertinencia de los medios probatorios de los delitos informáticos, la claridad de la caracterización de la prueba para los delitos en mención, la falta de individualización de la evidencia digital en la ley colombiana, y distintos aspectos frente al uso de protocolos para la obtención de la evidencia digital y la recolección del material probatorio.

Con menos preguntas se abordó este objetivo en el caso de fiscales y jueces penales, siendo más concretas y directas las preguntas sobre la pertinencia de los medios probatorios destinados a los delitos informáticos, la claridad en la caracterización de la prueba, y el uso de los medio probatorios dispuestos en la ley colombiana como soporte de evidencia y prueba en materia de delitos informáticos.

Sobre el objetivo tendiente a identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia, las encuestas tuvieron un número de interrogantes similares para todas las muestras poblacionales consultadas, siendo preguntas principalmente enfocadas al conocimiento de las técnicas por parte de cada uno de los operadores jurídicos.

Finalmente, de naturaleza valorativa son los interrogantes formulados a los abogados en torno al objetivo dirigido a analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal, y de índole cerrado los propuestos a fiscales y jueces, con quienes se mantuvo la indagación en torno al conocimiento que deben tener de estos aspectos de la materia.

Con el fin de triangular la información de las tres muestras poblacionales, se equipararon preguntas de cada objetivo específico, y se insertaron las estadísticas porcentuales obtenidas de forma individual al momento de elaboración de las gráficas con el fin de hacer un análisis de las diferentes posturas frente a un mismo objetivo específico, destacando para el análisis de datos, las preguntas

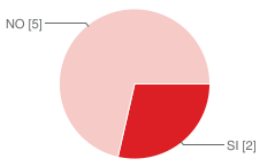
más adecuadas, además se correlacionaron las preguntas elaboradas en los tres tipos de encuestas cerradas teniendo en cuenta su función frente a un proceso penal y en consecuencia se realizó transversalidad de las mismas, con el objetivo de realizar un análisis del dato porcentual que estas arrojaron.

Se aclara que para hacer la triangulación se elegirán las preguntas más relevantes agrupadas por cada objetivo específico dado en la investigación inicial, que permita dibujar los hallazgos de la investigación y se insertarán los gráficos que dan cuenta de ello, posteriormente se incluirá un análisis sobre lo indagado.

Frente al primer objetivo específico: "Presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria".

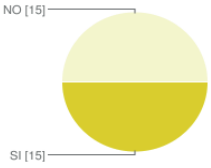
1. La pregunta "¿Reconoce usted el conjunto de tipos penales informáticos vigentes en la legislación colombiana?", número 1 de fiscales fue relacionada con la 1 de jueces y 1 de abogados, donde el resultado obtenido es:

a. Fiscales



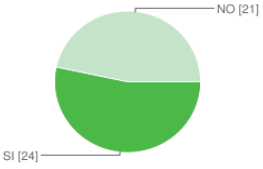
SI	2	29%
NO	5	71%

b. Jueces



SI	15	50%
NO	15	50%

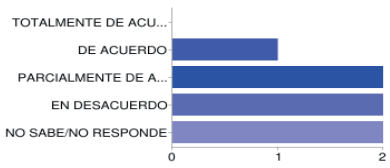
c. Abogados y defensores públicos



SI	24	53%
NO	21	47%

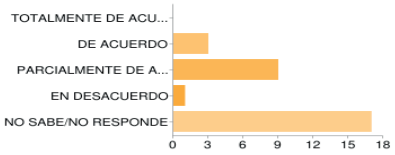
2. La pregunta ¿Cree usted que los tipos penales consagrados en la ley colombiana son suficientes para procesar las diferentes conductas que se desarrollan en el campo tecnológico? número 3 de fiscales fue relacionada con la 5 de jueces y la 1 de abogados, donde el resultado obtenido es:

a. Fiscales



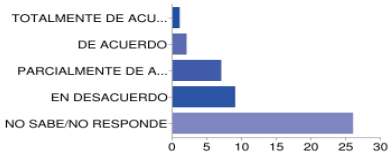
TOTALMENTE DE ACUERDO	0	0%
DE ACUERDO	1	14%
PARCIALMENTE DE ACUERDO	2	29%
EN DESACUERDO	2	29%
NO SABE/NO RESPONDE	2	29%

b.Jueces



TOTALMENTE DE ACUERDO	0	0%
DE ACUERDO	3	10%
PARCIALMENTE DE ACUERDO	9	30%
EN DESACUERDO	1	3%
NO SABE/NO RESPONDE	17	57%

c. Abogados y defensores públicos



TOTALMENTE DE ACUERDO	1	2%
DE ACUERDO	2	4%
PARCIALMENTE DE ACUERDO	7	16%
EN DESACUERDO	9	20%
NO SABE/NO RESPONDE	26	58%

Triangulación de resultados frente al objetivo # 1

Las posturas que identifican las poblaciones encuestadas permiten ser individualizadas y analizadas directamente con el cargo y profesión que desempeñan en tres categorías: jueces, fiscales y abogados (contractual o defensor público).

Los resultados arrojados generan una alerta para el Estado Colombiano, toda vez que la falencia más grande que puede evidenciarse en un operador judicial o investigador es la falta de capacitación, actualización y profesionalización, lo cual se hace evidente con resultados significativos en fiscales y jueces ante el desconocimiento de los delitos informáticos, e incluso la ausencia de hermenéutica jurídica aplicable a la interpretación sobre el alcance y aplicabilidad de los tipos penales, como se muestra en la gráfica, toda vez que estas categorías poblacionales debieran de haber arrojado un resultado del 100% en el conocimiento de la ley y el 100% sobre su ámbito y pertinencia de aplicabilidad con el objetivo de judicializar las conductas delictuales dadas en el ámbito digital.

Una postura concreta que direccione la solución a la situación es que el Gobierno fortalezca la materialización de políticas públicas direccionadas a subsanar las falencias en capacitación y formación a sus funcionarios públicos, siendo los fiscales lo más necesitados en capacitación que les permita acercarse al grupo de delitos informáticos, su tratamiento, comprobación, con el fin de fundamentar una imputación objetiva para la judicialización del sindicado, en consecuencia, al ser los jueces el ente encargado para fallar, denota una leve diferencia en cuanto al conocimiento que se posee sobre este grupo de delitos respondiendo solo un 50% positivo, que para la calidad de fallador, se reitera el estado ideal sería un 100%.

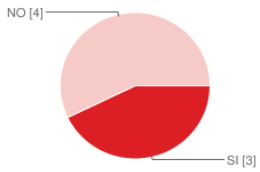
Finalmente, los abogados y defensores públicos siempre deben procurar su formación, de forma personal, pues su cargo u oficio no depende de la voluntad política del Estado para su proceso de formación académico y profesional, por el contrario nace de su voluntad propia, dedicarse a conocer los tipos penales que se constituyen en el ordenamiento jurídico colombiano, e impulsar, desde el ejercicio de su profesión, el desarrollo jurisprudencial y doctrinal, para el perfeccionamiento, sea de la aplicación del tipo penal o de la estructura como fuere concebido por el legislador.

En materia de delitos informáticos han hecho tránsito una infinidad de críticas a la estructura de los tipos penales, a su vez, es ello fundamento justificante para la ausencia de apropiación sobre el tipo penal y su aplicación en la judicialización de un caso, sin embargo, es notable cómo el desconocimiento conceptual de una ciencia como la informática pone en entredicho no sólo al operador judicial sino también a la defensa y la fiscalía, en el tratamiento y prueba de una conducta delictual involucrada con el campo informático, situación que permite dar más fuerza a las posturas innovadoras del campo jurídico, donde es notoria la necesidad de que se reconozca una jurisdicción especial para el campo informático, ya que son muchos los vacíos normativos, en consecuencia, es grande el desconocimiento y la falencia en interpretación jurídica de los aspectos legales que rodean el derecho informático, y es mucho más notorio en el campo de los delitos.

Frente al segundo objetivo específico: "Listar los medios probatorios existentes a partir de la Ley 906 de 2004, que son generalmente aceptados en Colombia, y evidenciar cuales son o se pueden presentar como evidencia digital y física en relación con un tipo penal informático".

1. La pregunta ¿Comparte usted que la caracterización de la prueba para la defensa en juicio en materia de delitos informáticos es clara? número 1 de fiscales se relaciona con la pregunta 1 de jueces y la 1 de abogados, donde el resultado obtenido es:

a. Fiscales

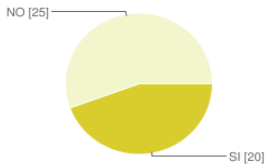


SI	3	43%
NO	4	57%

b. Jueces

SI	9	30%
NO	21	70%

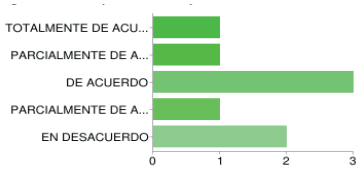
c. Abogados y defensores públicos



SI	20	44%
NO	25	56%

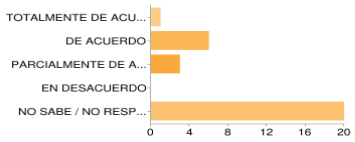
2. La pregunta ¿Estima valido que los medios probatorios existentes en la ley 906 de 2004 pueden ser usados como EVIDENCIA digital o física en un proceso por delito informático? número 2 de fiscales se relaciona con la 3 de jueces y la 2 de abogados, donde el resultado obtenido es:

a. Fiscales



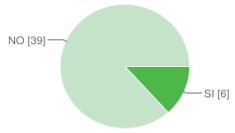
TOTALMENTE DE ACUERDO	1	14%
PARCIALMENTE DE ACUERDO	1	14%
DE ACUERDO	3	43%
PARCIALMENTE DE ACUERDO	1	14%
EN DESACUERDO	2	29%

b. Jueces



TOTALMENTE DE ACUERDO	1	3%
DE ACUERDO	6	20%
PARCIALMENTE DE ACUERDO	3	10%
EN DESACUERDO	0	0%
NO SABE / NO RESPONDE	20	67%

c. Abogados y defensores públicos



SI	6	13%
NO	39	87%

Triangulación de resultados frente al objetivo # 2

Igualmente la triangulación de posturas se identifican por poblaciones encuestadas individualizadas y analizadas por el cargo y profesión, correspondientes a tres categorías: jueces, fiscales y abogados (contractual o defensor público).

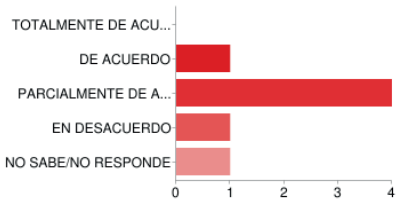
En el campo probatorio se reflejan posturas opuestas, una es la que se evidencia del fiscal y abogado, y la otra parte es el juez, en el primer grupo poblacional es un hecho notorio respecto de indicadores de 43% y 44% respectivamente que tiene mayor acercamiento a la prueba digital, a su caracterización, su obtención y presentación en juicio, no así lo denota el juez 30%, a pesar de que es éste quien está llamado a dirigir el curso del proceso y fallar.

Por otro lado son los resultados significativos en materia de medios probatorios aceptados por el Ordenamiento Procesal Penal, aplicables con la finalidad de presentar los hechos acaecidos en un caso específico que involucra un incidente informático o la investigación de un delito informático, aquí el comportamiento es diferente donde los fiscales son los que en un porcentaje de 43% manifiestan que cualquier medio probatorio es válido para probar un delito informático no solo la evidencia digital, en contraposición se encuentran los abogados y jueces donde los resultados son 87% y 67% respectivamente no son aplicables o desconocen su pertinencia para la investigación de un delito informático la utilización de medios probatorios tradicionales.

Frente al tercer objetivo específico: "Identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia".

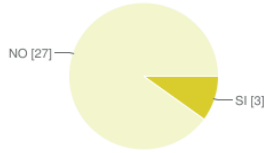
1. La pregunta ¿Conoce usted los protocolos forenses que deben aplicarse en Colombia para la investigación de un delitos informático? número 1 de fiscales se relaciona con la 2 de jueces y la 3 de abogados, donde el resultado obtenido es:

a. Fiscales

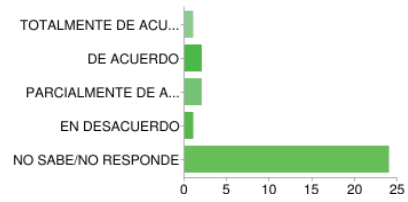


TOTALMENTE DE ACUERDO	0	0%
DE ACUERDO	1	14%
PARCIALMENTE DE ACUERDO	4	57%
EN DESACUERDO	1	14%
NO SABE/NO RESPONDE	1	14%

b. Jueces

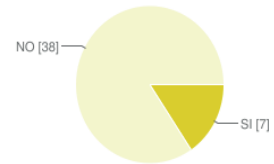


SI	3	10%
NO	27	90%



TOTALMENTE DE ACUERDO	1	3%
DE ACUERDO	2	7%
PARCIALMENTE DE ACUERDO	2	7%
EN DESACUERDO	1	3%
NO SABE/NO RESPONDE	24	80%

c. Abogados y defensores públicos



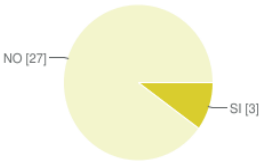
SI	7	16%
NO	38	84%

2. La pregunta ¿Conoce las calidades, capacidades, formación profesional y la certificación que debe poseer el experto forense informático para la obtención e informe como perito en pruebas electrónicas? número 2 de fiscales se relaciona con la 1 de jueces y la 1 de abogados, donde el resultado obtenido es:

a. Fiscales

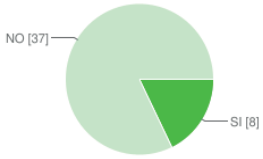
SI	0	0%
NO	7	100%

b. Jueces



SI	3	10%
NO	27	90%

c. Abogados y defensores públicos



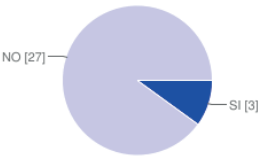
SI	8	18%
NO	37	82%

3. La pregunta ¿Conoce que protocolos de análisis que debe seguir el investigador de forma, para cada tipo penal que informático que se investiga? número 3 de fiscales se relaciona con la 3 de jueces y 2 de abogados, donde el resultado obtenido es:

a. Fiscales

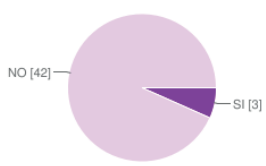
SI	0	0%
NO	7	100%

b. Jueces



SI	3	10%
NO	27	90%

c. Abogados y defensores públicos



SI	3	7%
NO	42	93%

Triangulación de resultados frente al objetivo # 3

Igualmente la triangulación de posturas se identifican por poblaciones encuestadas individualizadas y analizadas por el cargo y profesión, correspondientes a tres categorías: jueces, fiscales y abogados (contractual o defensor público).

Los resultados obtenidos frente a este objetivo no son distantes de los obtenidos frente al objetivo 1 y 2, en cuanto a que el desconocimiento de la interrelación disciplinar entre el derecho informático y la informática forense es la consecuencia nefasta del escenario problematizante en Colombia respecto al conocimiento, tratamiento y judicialización de conductas delictuales informáticas.

Es claro que los encuestados responden positivamente a la ciencia del Derecho desde el ámbito sustancial y procesal, siempre y cuando no se involucren conductas delictuales tipificadas como delito informático, porque desde ese contexto la competencia profesional ya no es suficiente, y emerge un grado significativo de ausencia en el tratamiento de delito informático desde la adecuación típica de una conducta específica y los medios probatorios que se requieren, por la parte interesada, que se practiquen para demostrar la inocencia o culpabilidad de un sindicado.

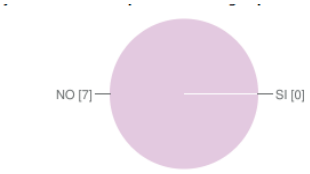
Para el campo de las pruebas en delitos informáticos se requiere el conocimiento de las herramientas de ataque y su forma de utilización, la intencionalidad y cualificación del sujeto activo de la conducta, y con el fin de determinar la pertinencia de un medio de prueba, respecto de un hecho cometido.

Por lo anterior, y en correlación con los resultados estadísticos que arrojaron las encuestas, sí se conocen los medios tradicionales de prueba; la falencia se encuentra precisamente en su aplicación al mundo informático, y a su vez la interpretación y análisis forense que debe tener este tipo de prueba, como se estructuró en la Unidad 6 del presente texto, y como se desprende de las entrevistas a profundidad realizadas a abogados y expertos forenses informáticos, el estatuto procesal penal requiere una rápida modificación en su regulación, direccionada, entre muchos otros aspectos, a evolucionar la forma de probar la conducta penal acaecida como incidente informático y su vinculación autoral con un sujeto determinado.

Frente al cuarto objetivo específico: "Verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis post mortem de un incidente en Colombia":

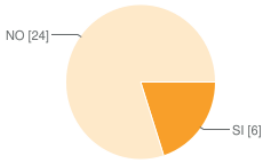
1. La pregunta ¿Conoce el protocolo de cadena de custodia para el análisis de dispositivos de almacenamiento digital con fines forenses? número 1 de fiscales se relaciona con la 1 de jueces y 1 de abogados, donde el resultado obtenido es:

a. Fiscales



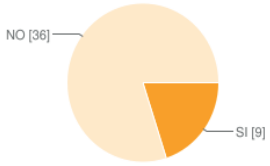
SI	0	0%
NO	7	100%

b. Jueces



SI	6	20%
NO	24	80%

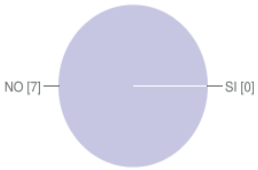
c. Abogados y defensores públicos



SI	9	20%
NO	36	80%

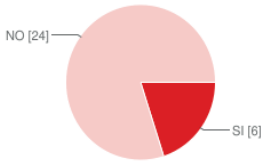
2. La pregunta ¿Usted sabe cuáles requisitos formales y materiales verificar del EMP en el tratamiento de laboratorio forense, con el fin de garantizar que la evidencia digital sea aceptada como prueba electrónica que soporte los hechos que se alegan? número 3 de fiscales se relaciona con la 1 de jueces y la 3 de abogados no tiene correlación con otra pregunta de los otros dos tipos poblacionales, por lo cual se inserta el resultado pero su análisis es independiente, donde el resultado obtenido es:

a. Fiscales



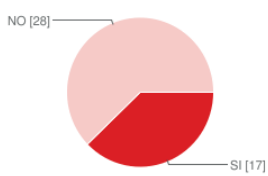
SI	0	0%
NO	7	100%

b. Jueces



SI	6	20%
NO	24	80%

c. Abogados y defensores públicos



SI	17	38%
NO	28	62%

Triangulación de resultados frente al objetivo # 4

Igualmente la triangulación de posturas se identifican por poblaciones encuestadas individualizadas y analizadas por el cargo y profesión, correspondientes a tres categorías: jueces, fiscales y abogados (contractual o defensor público).

Una coyuntura más relevante en cuanto a la transversalidad entre el derecho, la informática y el campo forense, es el tema de los protocolos forenses y las herramientas para la implementación y aplicación de estos protocolos.

Los resultados obtenidos en las encuestas no distan de la realidad que se recolectó con el rastreo documental de la investigación y mucho menos con la notoria falencia en Colombia de un protocolo y herramientas forenses digitales para el tratamiento de evidencia, toda vez que, cuando el ordenamiento jurídico colombiano nada dice sobre herramientas forenses propias o protocolos forenses digitales propios, sería impensable que los actores en un caso penal tuviesen competencia en el conocimiento de los mismos.

Ahora bien, no se está afirmando que en Colombia no existan protocolos y herramientas forenses aplicables, sólo que no son propias del Estado, no son de desarrollo nacional, sin embargo, tanto en el campo público a través de las unidades de delitos informáticos, como en el privado a través de las compañías que prestan el servicio de peritaje forense, son usuarias de protocolos creados por la INTERPOL, SANS y NIST debidamente certificados, entre otros que ya fueron identificados en el capítulo 4, y de herramientas forenses (software y hardware) certificados, como es la tan reconocida herramienta ENCASE, la cual para su obtención de licenciamiento es costoso y de difícil acceso a todo público, toda vez que una licencia puede costar desde US 15.000 a 30.000, dependiendo del usuario de la licencia, y del uso y goce que se le dará.

Lo expresado en el anterior párrafo hace surgir la necesidad de iniciativas investigativas con herramientas forenses digitales *open source* que son en algunos casos de distribución ilegales, es por ello que no se permiten evidencias digitales obtenidas con este tipo de herramientas en el campo público, ya que no cuentan con licenciamiento y pago avalado por parte del Estado.

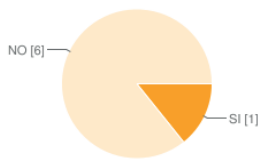
Al analizar los resultados de las preguntas, la tendencia mayoritaria en las respuestas de las poblaciones encuestadas es tajante al evidenciar el alto y casi absoluto desconocimiento de los protocolos forenses digitales en cuanto a sus elementos formales y materiales que validen su aplicación en el procesamiento de un caso penal, quedando en manos del perito forense la validación de toda la labor investigativa, generando ausencia de fundamentos para ejercer el derecho de oposición a la prueba puesto que, el desconocimiento de la prueba y la técnica de obtención no permite indicar los errores, fallas, manipulaciones, irregularidades, entre otros hechos que comporte la prueba y sirvan de argumento al momento de ejercer el derecho de contradicción probatoria, podría traerse a colación la tesis jurídica que indica “el desconocimiento de la ley no sirve de excusa”, pero en el caso que nos ocupa ni siquiera el ordenamiento procesal penal se ha permitido avanzar y regular aspectos relevantes como los protocolos forenses digitales, por ello, es válido afirmar que en materia probatoria queda evidenciada la inseguridad jurídica que en consecuencia genera el desconocimiento de la prueba en sí misma.

Cabe anotarse igualmente que se desconoce la pertinencia o no de una herramienta forense digital determinada, nuevamente quedando en cabeza del perito forense la responsabilidad de demostrarla, y evidencia la certificación en el tratamiento de casos penales, por último, y no menos importante, el desconocimiento de cómo se certifica la experiencia o profesionalidad de un perito forense digital, toda vez que el principio de libertad probatoria está cargando de una gran responsabilidad, certeza y validez de la prueba pericial en el criterio de un sujeto, convalidado en la incapacidad, muchas veces, de controvertir el testimonio que esté presente en juicio.

Frente al quinto objetivo específico: “Analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal”.

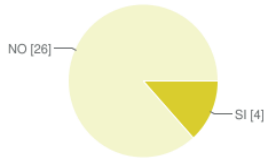
1. La pregunta ¿conoce el procedimiento que aplica la unidad de investigación criminal de la policía para la recepción, análisis de elementos materiales prueba y finaliza con entrega del informe de investigador de laboratorio y elementos materiales de prueba? número 1 de fiscales se relaciona con la 1 de jueces y la 1 de abogados, donde el resultado obtenido es:

a. Fiscales



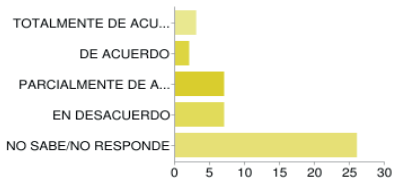
SI	1	14%
NO	6	86%

b. Jueces



SI	4	13%
NO	26	87%

c. Abogados y defensores públicos (este resultado es analizado de forma individual en la conclusión)



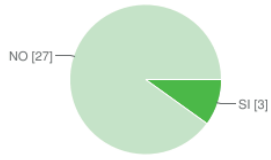
TOTALMENTE DE ACUERDO	3	7%
DE ACUERDO	2	4%
PARCIALMENTE DE ACUERDP	7	16%
EN DESACUERDO	7	16%
NO SABE/NO RESPONDE	26	58%

2. La pregunta Si su respuesta anterior fue afirmativa, responda: ¿este procedimiento permite la aplicación de protocolos impertinentes en el tratamiento del EMP en el laboratorio forense informático? número 2 de fiscales se relaciona con la 2 de jueces y la 2 de abogados, donde el resultado obtenido es:

a. Fiscales

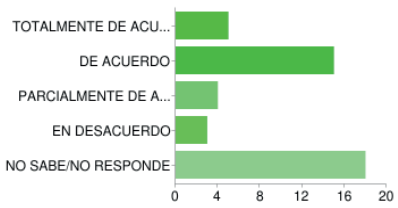
SI	0	0%
NO	7	100%

b. Jueces



SI	3	10%
NO	27	90%

c. Abogados y defensores públicos



TOTALMENTE DE ACUERDO	5	11%
DE ACUERDO	15	33%
PARCIALMENTE DE ACUERDP	4	9%
EN DESACUERDO	3	7%
NO SABE/NO RESPONDE	18	40%

Triangulación de resultados frente al objetivo # 5

Igualmente la triangulación de posturas se identifican por poblaciones encuestadas individualizadas y analizadas por el cargo y profesión, correspondientes a tres categorías: jueces, fiscales y abogados (contractual o defensor público).

Finalmente, un indicador de alerta a la situación general y preocupante en nuestro entorno nacional se evidencia con las cifras obtenidas indicando que entre el 87% y 88% se desconocen las técnicas, procesos, procedimientos y demás trabajo investigativo se realiza en la investigación penal para la obtención de una evidencia digital, resultado significativamente grave, por la calidad profesional y laboral que poseen los encuestados, por ello el desconocimiento de los protocolos aplicados por las unidades de investigación en delitos informáticos, por parte de los operadores judiciales y de cualquier actor dentro de un proceso penal, plantea un panorama más complejo aún, ya que el no conocer una técnica forense digital para la obtención de una evidencia digital, dificulta su defensa y contradicción, según la parte que la aporte.

Lo anterior es una situación fundante de inseguridad jurídica en materia de pruebas, toda vez que, el conocimiento de la técnica en el trabajo de investigación para la obtención de la evidencia digital, aplicada en un proceso de delitos informáticos, significa que los casos penales donde se encuentre involucrada este medio probatorio, la existencia de la prueba que fundamenta lo hechos, ven su futuro de verificación de validez y eficacia, solo se enmarca a la capacidad de valoración del juez sobre la evidencia digital, en correlación con otros medios cognitivos probatorios, en caso de que existan. El estado ideal de la validez y eficacia de una evidencia digital debería ser que ésta en sí misma fuera suficiente para podría demostrar la ocurrencia de un incidente informático, pero difícilmente ésta puede lograr vincular a un sujeto con la comisión del hecho, y menos cuando la universalidad de la evidencia digital queda en manos del forense, su extracción, validación, aportación en juicio y defensa.

Podría pensarse que en muchos casos penales las partes del proceso y los actores involucrados en él actúan desde el sentido común y la lógica jurídica, más que desde el campo de la realidad y evidencia científica, para participar de forma directa o indirecta en un juicio penal.

De la anterior afirmación sólo basta ver los resultados frente a las preguntas, y la tendencia negativa frente al desconocimiento de los protocolos, en contraposición con la tendencia, en mayor implicación, cuando se cuestiona frente a los resultados de una mala aplicación de un protocolo, en cuyo caso los efectos de invalidación por exclusión o anulación de una prueba a causa de la mala aplicación de un protocolo forense, debe alegarse por la parte interesada, aunque es pertinente dejar un cuestionamiento que abre el camino para la indagación ¿cómo podría alegar la invalidación sin tener competencia profesional y académica para demostrar la ocurrencia de circunstancias fácticas para demostrar la nulidad o exclusión de la prueba?

La conclusión más transversal de todas es que en Colombia la cantidad de personas que son competentes en materia de delitos informáticos, tanto en su investigación y juzgamiento, no se correlacionan con el volumen de delitos informáticos que a diario ocurren en nuestro país; existe entonces una necesidad manifiesta de la evolución del estatuto procesal penal, direccionado entre otros objetivos a obligar la competencia y la especialidad de la ciencia informática y la disciplina forense digital, tanto para los jueces, abogados, defensores públicos, fiscales, sin dejar de lado a los auxiliares de la justicia en calidad de investigadores forenses y peritos en juicio.

Finalmente, las recomendaciones, conclusiones y sugerencias de artículos que permitan la evolución del estatuto procesal penal dados en las Unidades 6 y 7 del presente texto, no distan mucho de estos resultados, se pensaría más en una reafirmación de las consecuencias sobre el tratamiento de un campo innovador, en materia de comportamiento delincuencial, que reta al derecho penal colombiano, tanto en el campo sustancial como en el procesal.

HALLAZGOS

CAPÍTULO 6.

CONSIDERACIONES FRENTE AL DERECHO PROCESAL PENAL CON MIRAS A LA EVOLUCIÓN LEGAL FRENTE A LA INFORMÁTICA FORENSE

Ana María Mesa Elneser

La Convención de Cibercimen dada en Budapest, plantea su campo de aplicación en el ámbito sustancial y procesal, el resultado de las entrevistas y encuestas, instrumentos aplicados en la fase de análisis en la ejecución del proyecto de investigación, permiten afirmar que existen bases Constitucionales de acuerdo al artículo 29 consagratorio del derecho fundamental al debido proceso en el cual, frente a la prueba regula “Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso.”, y legales (estás se desarrollarán en este capítulo de forma más detallada) que fundamentan la necesidad de evolución normativa en el Estatuto Procesal Penal, teniendo en cuenta que su estructura, muchas veces criticada y demandada, en materia de delitos informáticos, resulta no ser suficiente, y en muchos casos, su interpretación y aplicación resulta contradictoria o violatoria de derechos sustanciales procesales, aunque en otros casos sí permite protegerlos.

En la presente unidad se plantearán temáticas, cada una acompañada de un breve análisis conceptual, con el objetivo de que las mismas sean tomadas a consideración como evolución normativa, teniendo en cuenta parámetros jurídicos derivados del desarrollo investigativo del proyecto, previa valoración de la comunidad científica y legislativa, para ser acogidas como parte integrante del proyecto de ley modificatorio al código procesal penal, Ley 906 de 2004.

Temáticas a tratar: evidencia digital, elemento material probatorio, protocolo(s) y herramienta(s) forense(s) digital(es), profesionalidad y cualificación de experiencia del perito forense y el Instituto Colombiano de Medicina Legal y Ciencias Forenses.

En el título II del Estatuto Procesal Penal se regulan los medios cognoscitivos en la indagación e investigación, denominando el capítulo único como “elementos materiales probatorios, evidencia física e información”; desde la titulación pareciera ser que son identificaciones con objetivos diferentes, sin embargo, desde la interpretación jurídica se tiene la postura que: “Elemento material probatorio: es cualquier objeto relacionado con la conducta punible que pueda servir para determinar la verdad en una actuación penal. Los elementos materiales probatorios en Colombia, se asimilan a la evidencia física” (Consejo Nacional de Policía Judicial), generando de forma tácita una vacío legal al momento de darle aplicación al término de *evidencia digital,* forma denominativa, a nivel internacional y nacional, por las ciencias forenses digitales o computación forense, al material obtenido en el tratamiento de un incidente informático, situación que implica un aparente vacío normativo bajo la premisa de que la evidencia digital posee entre sus características la inmaterialidad de la evidencia, lo cual, contrastado frente al término elemento material probatorio y EF -evidencia física, en correlación con la ED– evidencia digital, se entendería excluida como medio cognoscitivo, es por ello que se sugiere, a modo de reforma de la norma procesal penal, el texto insertado en cursiva:

TÍTULO II

MEDIOS COGNOSCITIVOS EN LA INDAGACIÓN E INVESTIGACIÓN

CAPÍTULO ÚNICO

Elementos materiales probatorios, evidencia física y *digital* e información

Artículo 275: *Elementos materiales probatorios, y evidencia física y digital.* Para efectos de este código se entiende por elementos materiales probatorios y evidencia física y *digital,* los siguientes:

f) Los elementos materiales obtenidos mediante grabación, filmación, fotografía, recuperación de datos, video o cualquier otro medio avanzado, utilizados como cámaras de vigilancia, en recinto cerrado o en espacio público;

h) Los demás elementos materiales, *en formato digital o físico,* similares a los anteriores y que son descubiertos, recogidos y custodiados por el Fiscal General o por el fiscal directamente o por conducto de servidores de policía judicial o de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente, *por los organismos internacionales oficiales en ciencias y disciplinas forenses.*

Parágrafo. Entiéndase para los términos del presente código, cuando se trate de evidencia, será física o digital.

TÍTULO IV

PARTES E INTERVINIENTES

CAPÍTULO I

Fiscalía General de la Nación

Artículo 114. *Atribuciones.* La Fiscalía General de la Nación, para el cumplimiento de sus funciones constitucionales y legales, tiene las siguientes atribuciones:

4. Asegurar los elementos materiales probatorios y evidencia física y *digital,* garantizando su cadena de custodia mientras se ejerce su contradicción.

LIBRO II

TÉCNICAS DE INDAGACIÓN E INVESTIGACIÓN

DE LA PRUEBA Y SISTEMA PROBATORIO

TÍTULO I

LA INDAGACIÓN Y LA INVESTIGACIÓN

CAPÍTULO I

Órganos de indagación e investigación

Artículo 205: *Actividad de policía judicial en la indagación e investigación.* Los servidores públicos que, en ejercicio de sus funciones de policía judicial, reciban denuncias, querellas o informes de otra clase, de los cuales se infiera la posible comisión de un delito, realizarán de inmediato todos los actos urgentes, tales como inspección en el lugar del hecho, inspección de cadáver, entrevistas e interrogatorios, *autorización para apertura de log o ficheros o archivos, que contengan datos informáticos.* Además, identificarán, recogerán, embalarán técnicamente los elementos materiales probatorios, y evidencia física y *digital* y registrarán por escrito, grabación magnetofónica o fonóptica las entrevistas e interrogatorios y se someterán a cadena de custodia.

Cuando deba practicarse examen médico-legal a la víctima, en lo posible, la acompañará al centro médico respectivo. Si se trata de un cadáver, este será trasladado a la respectiva dependencia del Instituto Nacional de Medicina Legal y Ciencias Forenses o, en su defecto, a un centro médico oficial para que se realice la necropsia médico-legal. *Si se trata de un incidente informático, deberá procederse ante las unidades de delitos informáticos con laboratorio forense digital y protocolo forense digital que permita el tratamiento de la evidencia.*

Sobre esos actos urgentes y sus resultados la policía judicial deberá presentar, dentro de las treinta y seis (36) horas siguientes, un informe ejecutivo al fiscal competente para que asuma la dirección, coordinación y control de la investigación.

En cualquier caso, las autoridades de policía judicial harán un reporte de iniciación de su actividad para que la Fiscalía General de la Nación asuma inmediatamente esa dirección, coordinación y control.

Artículo 209: *Informe de investigador de campo.* El informe del investigador de campo tendrá las siguientes características:

c) Relación clara y precisa de los elementos materiales probatorios y evidencia física y *digital* descubiertos, así como de su recolección, embalaje y sometimiento a cadena de custodia, *además del protocolo y la técnica aplicada en el caso de evidencias digitales;*

Artículo 210: *Informe de investigador de laboratorio.* El informe del investigador de laboratorio tendrá las siguientes características:

La descripción clara y precisa del elemento material probatorio y evidencia física y digital examinados;

La descripción clara y precisa de los procedimientos técnicos empleados en la realización del examen y, además, informe sobre el grado de aceptación de dichos procedimientos por la comunidad técnico-científica; demás, *cuando se trate de evidencia digital, deberá contener la indicación de la(s) certificaciones y reconocimientos que posee el protocolo o procedimiento aplicado para el tratamiento forense;*

Relación de los instrumentos empleados e información sobre su estado de mantenimiento al momento del examen; *cuando se trate de evidencia digital, deberá contener la indicación de utensilios, dispositivos y soportes lógicos aplicados;*

Explicación del principio o principios técnicos y científicos aplicados e informe sobre el grado de aceptación por la comunidad científica;

Descripción clara y precisa de los procedimientos de su actividad técnico- científica; *cuando se trate de evidencia digital indicar los fundamentos teóricos, métodos, o procedimientos aplicados;*

Interpretación de esos resultados; *cuando se trate de evidencia digital, indicar los principios científicos y técnicos aplicados para el análisis forense digital.*

CAPÍTULO IV

Métodos de identificación

Artículo 251: *Métodos.* Para la identificación de personas se podrán utilizar los diferentes métodos que el estado de la ciencia aporte, y que la criminalística establezca en sus manuales, tales como las características morfológicas de las huellas digitales, la carta dental y el perfil genético presente en el ADN, *y cuando se trate de incidentes informáticos, la apertura de log o ficheros o archivos, que contengan datos informáticos,* los cuales deberán cumplir con los requisitos del Artículo 420 de este código respecto de la prueba pericial.

Igualmente coadyuvarán en esta finalidad otros exámenes de sangre o de semen; análisis de composición de cabellos, vellos y pelos; caracterización de voz; comparación sistemática de escritura manual con los grafismos cuestionados en un documento, o características de redacción y estilo utilizado en el mismo; por el patrón de conducta delincuencial registrado en archivos de policía judicial; o por el conjunto de huellas dejadas al caminar o correr, teniendo en cuenta la línea direccional, de los pasos y de cada pisada. *Igual categoría tendrá la apertura de log o ficheros o archivos, que contengan datos informáticos y se encuentren almacenados en los servidores de las entidades prestadoras de servicio de internet o ISP.*

CAPÍTULO V

Cadena de custodia

Artículo 254: *Aplicación.* Con el fin de demostrar la autenticidad de los elementos materiales probatorios, y evidencia física *y digital,* la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos. *Cuando se trate de dispositivos, se deberán copiar los bits que éste contenga de manera que permita crear una copia exacta con hardware y soporte lógico forense digital, para ser admisible como evidencia digital.*

La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física y digital, y finaliza por orden de autoridad competente.

Parágrafo 1. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos.

Parágrafo 2. *Instituto de medicina legal y ciencias forenses, deberá promover la reglamentación, que permita establecer los protocolos forenses para tratamiento de evidencia digital e indicar la forma en que debe certificarse el protocolo, la experiencia y profesionalidad del perito forense, al igual que las herramientas forenses válidas en la implementación del protocolo.*

Artículo 257: *Inicio de la cadena de custodia.* El servidor público que, en actuación de indagación o investigación policial, hubiere embalado y rotulado el elemento material probatorio y evidencia física y digital, lo custodiará.

Artículo 263: *Examen previo al recibo.* Toda persona que deba recibir un elemento material probatorio y evidencia física, antes de hacerlo, revisará el recipiente que lo contiene y dejará constancia del estado en que se encuentre. *Cuando se trate de dispositivos de almacenamiento digital, la cadena de custodia deberá cumplirse con los requisitos mínimos de preservación de autenticidad, confiabilidad, integridad y originalidad, requeridos por el protocolo forense a aplicarse en laboratorio de tratamiento forense digital.*

Artículo 264: *Identificación.* Toda persona que aparezca como embalador y rotulador, o que entrega o recibe el contenedor de elemento material probatorio y evidencia física, deberá identificarse con su nombre completo y apellidos, el número de su cédula su ciudadanía y el cargo que desempeña. Así constará en el formato de cadena de custodia. *Cuando se trate de evidencia digital, que será obtenida de dispositivos encendidos, con el fin de preservar la autenticidad, deberá realizarse una documentación con acta, fotografías o grabación de video, que permita dar soporte al embalaje de dispositivos hallados en funcionamiento.*

CAPÍTULO III

Práctica de la prueba

Parte III

Prueba pericial

Artículo 408: *Quiénes pueden ser peritos.* Podrán ser peritos, los siguientes:

1. Las personas con título legalmente reconocido en la respectiva ciencia, técnica o arte.

2. En circunstancias diferentes, podrán ser nombradas las personas de reconocido entendimiento en la respectiva ciencia, técnica, arte, oficio o afición aunque se carezca de título.

A los efectos de la cualificación podrán utilizarse todos los medios de prueba admisibles, incluido el propio testimonio del declarante que se presenta como perito.

Parágrafo. Cuando se trate de prueba forense digital, deberá tenerse en cuenta que la certificación del numeral primero debe provenir de una entidad nacional o internacional con la facultad legal para ello; para la certificación del numeral segundo deberá entenderse como fundamento para la cualificación de experiencia y especial conocimiento, el manejo de casos forenses digitales llevados a cabo y compararse con estándares internacionales para certificación de profesionales especializados en la materia.

Finalmente, este capítulo pretende presentar la estructura que la norma, del Estatuto Procesal Penal, requiere evolucionar para la inclusión directa de la disciplina forense digital con validez, eficacia y pertinencia en la investigación de delitos informáticos y delitos tradicionales que involucren herramientas tecnológicas informáticas en su ejecución, toda vez que la justificación de la investigación tuvo como eje temático, entre otros, el desconocimiento notorio (causa que afecta la judicialización de delincuentes en Colombia, afirmación realizada con fundamento al desarrollo investigativo del proyecto y confirmados en el documento CONPES 3701, la Convención Cibercrimen de Budapest y demás referencias del presente texto), por los operadores judiciales y los sujetos procesales involucrados en un caso penal por causa de su cargo como son los fiscales, abogados contractuales, defensores públicos, ministerio público, auxiliares de la justicia y demás, o por ser partes directas del proceso como son la víctima y el victimario.

CONCLUSIONES Y RECOMENDACIONES

El desarrollo del proyecto de investigación permitió materializar la interrelación entre la Ciencia Informática, las Ciencias Forenses y la Ciencia del Derecho, de ello quedaron varios aspectos concluyentes respecto del campo situacional colombiano. En igual sentido, se han planteado algunas recomendaciones que permiten materializar aspectos legales innovadores para el Ordenamiento Penal vigente, tanto en el campo sustancial y procesal.

Para esta unidad se deberán tener en cuenta, como parte integrante, las diferentes posturas tratadas en todos las unidades, en calidad de análisis, posturas, afirmaciones que permiten darle aplicabilidad a los resultados obtenidos en el desarrollo investigativo.

Estas recomendaciones y conclusiones serán materia de divulgación en los diferentes eventos y artículos que se presenten durante el año 2012 y subsiguientes, con la participación de diferentes autores con sus ponencias en eventos de divulgación académica.

Es por ello que se plantea a continuación un sinnúmero de temáticas que permiten indicar de forma breve los aspectos concluyentes y las recomendaciones, así:

1. En el rastreo bibliográfico, en las encuestas y entrevistas, quedó evidenciado el desconocimiento en el contexto colombiano sobre la existencia de protocolos forenses digitales, menos el tipo de protocolo y casi imperceptible, la existencia de una certificación institucional. Ello evidencia el desconocimiento en el campo científico sobre la cooperación que presentan las ciencias forenses, informática y el derecho, en contraposición sobre el nivel de criminalidad que hay en Colombia, donde, como lo indica el documento CONPES 3701, nos encontrábamos para mediados del año 2011 en el quinto puesto, es por ello que urge en Colombia que el Instituto Colombiano de Medicina Legal y Ciencias Forenses se apersone sobre el campo forense digital, no sólo con expertos en el área sino con la certificación de protocolos pertinentes para la aplicación en la recolección de evidencia digital, sean estos de entidades internacionales y eventualmente, cuando ello ocurra, de entidades del orden nacional.

2. Es importante para Colombia la indicación, desde el Estado, del protocolo base válido para los procedimientos forenses digitales en Colombia, en consecuencia, y en la misma perspectiva, es necesario crear procedimientos de validación de herramientas forenses digitales para el tratamiento forense digital de la evidencia, permitiendo, entre otras herramientas, las denominadas *open source* o de código abierto, toda vez que las herramientas oficiales tienen un costo muy alto y las pocas entidades privadas que poseen estas prestan sus servicios a costos inaccesibles para cualquier persona, e incluso, entidades empresariales con recursos económicos se abstienen de requerir el servicio y prefieren direccionar estos recursos a políticas de privacidad de la información. Sin embargo, el protocolo forense digital acogido por Colombia, o en desarrollo propio, debe ser público y su elaboración puede basarse en otros protocolos aceptados a nivel mundial y manuales de mejores prácticas.

3. Los protocolos forenses digitales aplicados por el Estado colombiano, a través de las unidades de delitos informáticos o tecnológicos existentes en la fiscalía y la policía, respectivamente, son protocolos no sometidos a reserva o exclusividad en el contexto internacional, igualmente en el ámbito nacional e incluso para cualquier ciudadano; a pesar de ello no es de divulgación o publicidad por estas unidades los protocolos que aplican, en muchos casos por temor a ser más vulnerables ante los atacantes informáticos, generándose

como efecto nocivo un problema bastante complejo, el cual se materializa en el desconocimiento frente a la caracterización de la prueba forense digital y el ejercicio al derecho de contradicción probatoria, impidiendo a la contraparte de la aportante del medio probatorio alegar circunstancias que la invaliden sobre aspectos como la metodología, técnicas y los protocolos aplicados, con el argumento y demostración de impertinencia investigativa.

En consecuencia de lo anterior es poco probable ejercer el derecho de contradicción frente a una prueba, cuando de ella no se conocen los elementos formales y materiales que permiten obtenerla, menos podría, a falta de materialización en el mundo fáctico, alegar invalidación de la misma, ello debería de entenderse como una violación directa al principio de contradicción probatoria, así su obtención, como se realiza actualmente, responde al ejercicio del principio de libertad probatoria, ambos principios existentes en el estatuto procesal penal.

A pesar de que existen entidades certificadoras a nivel internacional, debe crearse una política de investigación forense, en Colombia, que permita definir exactamente qué tipos de dispositivos, procedimientos, mecanismos, protocolos y manejo de documentación deben garantizarse dentro de un laboratorio forense digital, permitiendo que posea las características de autenticidad, integridad, originalidad, confiabilidad y no repudio.

4. Definir cuáles son los roles y habilidades del forense digital a desempeñar dentro de un proceso de investigación forense digital. En igual perspectiva, debe implementarse, para la investigación de cualquier tipo delictual, la recolección de información en dispositivos electrónicos, y será el estatuto procesal penal en cooperación con los lineamientos del Instituto Colombiano de Medicina Legal y Ciencias Forenses, la entidad que delimite los roles y habilidades del forense aplicables para todos los casos sobre un crimen, no necesariamente informático.

5. El origen formal de la cadena de custodia en Colombia es a partir de la Ley 906 de 2004, y una total incoherencia o incluso inexistencia en la Ley 600 de 2000 y anteriores regulaciones, pues en estos estatutos anteriores no se tenía claro el quehacer en el lugar de los hechos, los policías con funciones judiciales que operan en la captura, registro o allanamiento, hoy el estatuto los denomina como primer respondiente, es decir, quien conoce los hechos por asistir de primeros a escena.

Con los estatutos anteriores se carecía de lineamientos sobre el acordonamiento de área, restricción en el acceso a las personas por contaminación de la escena del crimen y los EMP o EF, la utilización de animales o cosas, o el cómo dar aviso de inmediato a quien ejerza las funciones de policía judicial, para el caso en concreto, y que se iniciaran las labores de reconocimiento de escena, recolección, embalaje y etiquetamiento de EMP y EF, e inicio la cadena de custodia. Para la época inicial sobre la implementación de la norma actual vigente, ley 906 de 2004, no se hablaba de formatos únicos que permitieran evidenciar estos aspectos, ni del recibido en los laboratorios con un rigorismo que permitiera establecer más tarde la inalterabilidad del elemento material probatorio y evidencia física. Como se tiene contemplado en el derecho anglosajón, se tiene homologado en la Ley 906 de 2004 en materia de cadena de custodia, importancia y repercusiones dentro del proceso

penal, aunque, Colombia en América latina fue uno de los últimos en acogerse al sistema acusatorio, la oralidad y sus consecuencias prácticas, todo ello que la Constitución de 1991 ya ordenaba un cambio en las políticas legislativas penales, solo surtiéndose hasta 2004.[1]

Sin embargo, se debe destacar que atendiendo el aspecto procesal desarrollando la parte general y especial, y principalmente el aspecto probatorio y los principios que se venían desarrollando desde finales de los años setenta, con primordial atención a la recolección de esas futuras pruebas, en concordancia con la exigencia de especialidad por parte del funcionario, la imparcialidad y la garantía de inalterabilidad: in dubio pro reo y debido proceso.

En la actualidad, y de forma notoria para el campo forense digital, se adquiere gran relevancia en materia probatoria, del cumplimiento de los principios probatorios que garanticen la autenticidad, integridad, confiabilidad, originalidad y no repudio, toda vez que, al no existir en muchas ocasiones la forma demostrativa de la alteración y fabricación (con fines ilícitos) de la prueba, su autenticidad se hace mayormente difícil para defender, y es por ello que esta disciplina forense exige especialidad y conocimiento en su ejecución al forense que actúa como perito.

6. Los Cafés Internet son sitios dedicados a prestar el servicio de conectividad a Internet a cualquier usuario por un precio específico, de gran interés para los ciberdelincuentes ya que los *log* o registros contenidos en archivos del computador se encuentran llenos de información y de datos informáticos atractivos para ellos pero a los cuales no se accede, salvo autorización expresa del juez control de garantías. Cabe resaltar que son estos operadores judiciales los principales propulsores y defensores sobre la tesis de defensa constitucional de derechos como la preservación de la intimidad del usuario que está por encima del derecho a obtener la prueba sobre la comisión de un delito, pues el primero es un derecho de rango constitucional y el otro derecho es de rango legal, toda vez que, para obtener la plena prueba de la ocurrencia de un incidente informático y la extracción de la evidencia digital, se hace imprescindible acceder a los equipos computacionales, específicamente los logs o archivos que contengan estos, los cuales contienen información tanto del propietario del equipo como de terceras personas, y ante una apertura de éstos, en principio se entiende para el juez constitucional violación de derechos fundamentales.

Sin embargo, urge en el ordenamiento jurídico colombiano una innovación en esta materia donde se amplíe el concepto restrictivo en materia de log o archivos o ficheros del servidor, sin que se considere violación a la intimidad de la persona usuaria, que en muchos casos resulta ser sospechosa, lo cual podría solucionarse o minimizar el riesgo de la “violación a la intimidad”; es importante reglamentar los sitios dedicados a este servicio, no sólo en los términos de la Ley 1336 de 2009 (julio 21 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”, sino que debe ampliarse a que todos los sitios cuenten, entre otras cosas, con circuito cerrado de televisión, monitoreo selectivo de usuarios sospechosos con acceso a páginas web con o sin contenido sospechoso con la conectividad directa a un cuerpo especial de policía judicial, sea por denuncia inmediata del

[1] Condición de ética autoral: conclusión realizada principalmente por el grupo de investigadores de la IES IDEAS, entre el coinvestigador Rodrigo Osorio y el semillero de estudiantes; la intervención realizada al informe de conclusiones es hecha, de forma exclusiva, por la investigadora principal Ana Maria Mesa Elneser, por la IES FUNLAM, con la finalidad dar inclusión y coherencia temática en el texto.

administrador del sitio a través de una plataforma de comunicación entre el sitio y el cuerpo de policía judicial, o de oficio por el mismo monitoreo que pueda hacer el servicio policial directamente.

7. En materia de delitos informáticos cobra gran relevancia que se retome la discusión sobre Responsabilidad de las Personas Jurídicas, ya que, aunque este tipo de persona es una ficción jurídica de la ley, es la que le da existencia a entidades inmateriales que operan a través de personas físicas y que, finalmente, son las que materialmente cometen la conducta delictiva, sin embargo, la figura a través de la que se esconden es precisamente la persona jurídica.

Existe en la Convención de Budapest (2001) el Artículo 14 donde se indica para los Estados la posibilidad de incluir en su ordenamiento interno la responsabilidad penal de las personas jurídicas, y realizando un análisis desde el contexto colombiano no sería ilegal acoger esta medida, ya que:

> Las personas físicas que comenten el delito actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en: a. un poder de representación de la persona jurídica; b. una autorización para tomar decisiones en nombre de la persona jurídica; c. una autorización para ejercer control en el seno de la persona jurídica. 2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica. 3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado. 4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción (Consejo de Europa, 2001).

Lo anterior fundamenta y da credibilidad a una afirmación consensuada como resultado de la investigación, sobre la igualdad entre la persona física y jurídica, en materia de responsabilidad, toda vez que, si en las otras jurisdicciones como son: civil, administrativo, laboral, comercial y entre otras ramas, la persona jurídica sí es responsable, es prohibitivo de forma directa en el área temática penal la responsabilidad de la persona jurídica, bajo argumentos como el que indica que la falta de permisibilidad en este tipo de responsabilidades, se debe a la ausencia de capacidad de raciocinio y de actuación de la persona jurídica, toda vez que su existencia es una ficción legal, mas su operatividad es por intermedio de la persona natural, la cual claramente soporta la imputación de cargos frente a los hechos.

Sin embargo, el fraude electrónico, a modo de ejemplo, es de mayor ocurrencia buscando engañar a la víctima a través de una persona jurídica, generando nivel de credibilidad debido a la existencia de la entidad, organización o compañía empresarial, de allí que sea el *phishing* uno de los instrumentos de ataque más usados por los ciberdelincuentes, o en materia de tipos penales, conductas como la suplantación de sitios web o la obstaculización ilegítima o la transferencia no consentida de activos, son de gran ocurrencia en nuestro país.

8. Se extrae una parte de la entrevista realizada al juez Alexander Díaz, como una postura que recoge y valida gran parte de las conclusiones y recomendaciones dadas en el texto, así:

> Hemos logrado ponernos a tono en la parte sustantiva con la expedición de la Ley 1273 de 2009, pero no en la parte procesal. Con la ambivalencia ante un sistema acusatorio puro o ecléctico, el ente investigador y su policía judicial no han podido establecer fehacientemente cuándo se debe contar con la anuencia previa del Juez de Control de Garantías y cuándo no, en tratándose de la evidencia digital y especialmente en el manejo de datos sensibles., a los que no se le quieren dar privilegios constitucionales que les corresponde. Observo que es por falta de cultura informática.

9. En materia de herramientas forenses digitales se ha resaltado la importancia de la aplicación de *softwares* con licencia, como lo tiene ENCASE, sin embargo, es de especial importancia ver cómo el operador judicial Alexander Díaz indica:

> No importa la categoría de software si se trata de uno con licencia u otro de OP o GNU, lo que importa es que su desarrollador permite su uso para fines oficiales o particulares. Sumado a esto, se debe considerar el buen uso de sus herramientas, pensemos si se le dieron buen uso al hardware y al software con los que hicieron interceptaciones de llamadas o comunicaciones en la Suprema Corte de Colombia, un ente oficial de inteligencia, lo cual implica que no todos los jueces control de garantías tienen el mismo criterio, toda vez que la mayoría de jueces para darle credibilidad a una prueba pericial, solo se accede a ello cuando se han aplicado técnicas, protocolos y herramientas forenses digitales certificadas y licenciadas, dejando de lado, otras herramientas forenses digitales como las open source, que permiten la extracción de la evidencia digital preservando los criterios valorativos de la prueba, pero el desconocimiento del juzgador, sin más miramientos las invalida.

10. El Estado a través del ministerio de educación nacional MEN debería generar una política pública que exija actualización curricular de todos los programas de formación en derecho y carreras afines con la inclusión de contenidos temáticos que permitan la formación en las disciplinas de: Derecho Informático, Informática Jurídica e Informática Forense.

11. Los criterios de valoración que debe tener en cuenta un juez de la República de Colombia al momento de fallar no pueden limitarse frente a tecnicismos y dejar por fuera la acreditado un hecho delictivo, es por ello que existe libertad probatoria y cando no se cuenta con la posibilidad de acreditar la titularidad de una dirección IP, mal haría el juzgador en no valorar las demás pruebas presentadas, menos cuando existe una notoria certeza de la comisión de un delito, es por ello que respecto a los hechos delictuales y violación de garantías fundamentales en materia de apertura de archivo o log o ficheros, se deben integrar todo los medios cognoscitivos para obtener la información que sustente la verdad procesal.

Si bien es cierto, la información contenida en estos registros es información privilegiada y el acceso a ella se equipara al acceso a una base de datos, situación que se encuentra regulada por la ley 1266 de 2008 y ley 1581 de 2012, exigiendo del funcionario judicial investigativo o fiscal respondiente , previo a la audiencia preparatoria, acudir ante el juez de control de garantías para obtener la autorización en procura a la obtención de información contenida en dichos registros, toda vez que se equipara como una búsqueda selectiva en una base de datos para garantizar que no se vayan a

vulnerar derechos de terceras personas, es el mismo juez quien otorga un término para recuperar la información, una vez recuperada, es el mismo juez de control de garantías, el que valida o no la actuación y la información recopilada siempre y cuando por el experto forense digital, realizando un examen de verificación de un tratamiento de la prueba sin vulnerar garantías fundamentales, igualmente se cumple dicha verificación con la prueba aportada así sea, por una persona no perito forense informático certificado, es posible probar la comisión del delito informático, toda vez que se puede acceder a esa información por otras vías diferentes a la informática, más que desde la experticia del forense, es con la obtención de los logs que certifican las transacciones electrónicas realizadas y las IP comprometidas..

Los elementos materiales probatorios aportados en un juicio penal se encuentran en gran medida soportados por normas del derecho sustancial, que permiten darle cabida o elevar a la categoría de delito una conducta delictual, independientemente de la forma como se haya obtenido la prueba; de todas maneras existen unos requisitos formales y materiales para hacer valer las evidencias digitales dentro del proceso penal como prueba documental, siendo uno de los requisitos el que se logre acreditar la autenticidad del documento, en los artículos 430 a 432 del Código de Procedimiento Penal, se indica que si al practicarse la prueba documental en la audiencia de juicio oral definitivamente no se logra determinar la autoría ese documento se considera anónimo y el juez debe admitirlo como prueba documental.

Si bien existe libertad probatoria, como sucede con una evidencia digital, esta tiene que darse en cumplimiento a los requisitos formales y materiales de ley, también tiene que evidenciar que tiene una relación con las garantías fundamentales, siendo relevante conocer la procedencia del documento que se quiere hacer valer como prueba dentro de la audiencia de juicio oral, sin embargo, cuando se quiere hacer valer como medio probatorio particular una evidencia digital, tiene que darse cumplimiento estricto a los requisitos señalados en la ley para que se pueda elevar a la categoría de prueba de una conducta delictual, siendo la principal la autenticidad de ese documento, toda vez que su valor probatorio se da por el análisis.

REFERENCIAS

CAPÍTULO 1.

Referencias

- Normativa

Colombia. Constitución Política de 1991.

Colombia. Congreso de la República. Ley 599 de 2000

Colombia. Congreso de la República. Ley 906 de 2004

Colombia. Congreso de la República. Ley 1273 de 2009

Colombia. Congreso de la República. Ley 1288 de 2009

Colombia. Departamento Nacional de Planeación. Documento CONPES 3701 de 2011

- Doctrinal

Barbie, E. (2000). *Fundamentos de la investigación social.* México: Thomson.

Cano, J. J. (Junio, 2006). Introducción a la Informática Forense, Una disciplina técnico-legal. Sistemas (96), 64-73.

Castro Ospina, S. J., (2010), *Delitos Informáticos: La Información como Bien Jurídico y los Delitos Informáticos en el Nuevo Código Penal Colombiano. Sitio web:* www.delitosinformáticos.com, disponible en: http://delitosinformaticos.gov.co/?q=rss.xml, consulta: julio 21 de 2010.

Encuesta fiscales, instrumentos de consulta elaborado por el grupo de investigadores del proyecto interinstitucional. Sitio web: Google Docs disponible en: https://docs.google.com/spreadsheet/viewform?formkey=dGVBSFA3NUFROWs5amtsMjhqM1hUWXc6MQ

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2007) *Metodología de Investigación.* (4 ed.) México: McGraw-Hill.

Informática jurídica, instrumentos de consulta elaborados por el grupo de investigadores del proyecto interinstitucional. Sitio web: Google Docs disponible en: http://tics.org.ar/index.php?option=-com_content&view=article&id=96:computaciorense-ansis-de-cadres-virtuales&catid=22:auditory-peritaje-informco&Itemid=40

Salkind J. Neil. (1999). *Métodos de Investigación.* México: Prentice-Hall.

CAPÍTULO 2.

Referencias

• Normativa

Colombia. Departamento Nacional de Planeación. Documento CONPES 3701 de 2011

• Doctrinal

Téllez Valdez, J. (1996). *Derecho Informático* (2 Ed.). México: McGraw -Hill.

Cibergrafía

CCIT, Recuperado de: http://www.ixp.net.co/contenido/

Ciberdelincuencia.com. Recuperado de: http://ciberdelincuencia.org/fuentes/prensa.php

Consejo de Europa (2001). *Convenio sobre la ciberdelincuencia.* Budapest: Council of Europe. Recuperado de: http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CB8Q-FjAA&url=http%3A%2F%2Fwww.coe.int%2Ft%2Fdghl%2Fstandardsetting%2Ft-cy%2FETS_185_spanish.PDF&ei=oDJaUPniBoi-9QS0poDwDQ&usg=AFQjCNH89PD_ieJFvv8VRRsdeXkslWK8rA

Instituto Nacional de Estándares y Tecnología. Recuperado de: http://www.nist.gov/index.html

INTERPOL. Recuperado de: http://www.interpol.int/es

SANS. Recuperado de: http://www.sans.org/top-cyber-security-risks/ y http://www.sans.org/

White House. Recuperado de: http://www.whitehouse.gov/espanol

CAPÍTULO 3.

Referencias

Babbie, E. (2000). *Fundamentos de la investigación social*. México: Thomson.

Balanta, H. (2009). *Aproximación legal a los delitos informáticos: una visión de derecho comparado.* En II Congreso Internacional de Criminología y Derecho Penal. Cali.

Bequai, A. (1996). "Computer Related Crimes". *Comisión de las comunidades Europeas. Delitos relativos a las computadoras.* Bruselas: Council of Europe.

Briones, G. (2002). *Metodología de la investigación cuantitativa en las ciencias sociales,* Bogotá: ICFES.

Conde Ortiz, C. (2006). *La protección de datos personales, un derecho autónomo con base en los conceptos de intimidad y privacidad*. Cádiz: Universidad de Cádiz.

De Pablos Heredero, C., López Hermoso, J. J., Romano Romero, S. M., Medina Salgado, S, Montero Navarro A. & Nájera Sánchez, J. J. (2006). *Dirección y gestión de los sistemas de información en la empresa, una visión integradora.* Madrid: Universidad Rey Juan Carlos

Durán Climent, C. (1999). *La prueba penal.* Valencia: Tirant Lo Blanch.

Firtman, S. J. (2005). *Seguridad informática.* Buenos Aires: MP Ediciones.

Hernández, R. (2006). *Metodología de la investigación.* México: MacGraw Hill.

Jiménez Marques, E. (2004). *Análisis de la investigación cuantitativa, métodos clásicos.* Zaragoza.

Landeira Prado, R. A., Cortizo Rodríguez, V. R., & Sánchez Valle, I. (2006). *Derecho de las nuevas tecnologías.* Madrid: Editorial Reus.

Salkind J. N. (1997). *Métodos de Investigación.* México: Prentice Hall.

Sánchez Bravo, A. (1998). *La protección del derecho a la libertad informática en la unión europea.* Sevilla: Universidad de Sevilla.

Santos Pascual, E. & López Vidriero Tejedor, I. (2005). *Protección de datos personales, manual práctico para empresas.* Madrid: FC Editores.

Télles Valdez, J. (1996). *Derecho informático.* México: Mc Graw Hill.

Vásquez Santamaría, J. E. (2009). *Derecho e interés público: aproximaciones y relación.* Medellín: Fundación Universitaria Luis Amigó.

Marica, A. (2012). El sistema de tratamiento de la información en EUROPOL. Barcelona: Institut de Ciències Polítiques i Socials (ICPS). Recuperado. http://ddd.uab.cat/pub/worpap/2012/hdl_2072_204891/icpswp309.pdf.

Cibergrafía

Acurio del Pino, S. (2011). Delitos informáticos: Generalidades. En Organización de Estados Americanos. Recuperado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arcesio Bolaños, F. y Martínez, J. E. (2004). Consideraciones legales de la seguridad informátic. En Acis. Recuperado de: www.acis.org.co/memorias/JornadasSeguridad/IVJNSI/aspectos%20legales%20de%20la%20seguridad.rtf

Biblioteca del Congreso Nacional de Chile (2004). Delitos informáticos en la legislación de España, Francia, Alemania e Italia. Santiago de Chile: BCN. Recuperado de: http://www.bcn.cl/carpeta_temas/temas_portada.2005-10-20.2791530909/pdf/informe_BCN_delitos_informaticos.pdf35

Cano Martínez, J. J. (Septiembre, 2001). Credenciales para investigadores forenses en informática. Certificaciones y entrenamiento. *Revista Electrónica de Derecho Informático* (38). Recuperado de: http://www.alfa-redi.org/node/9590

Díaz García, A. (7 de enero de 2010). Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos. *En Derecho, telecomunicaciones y tecnología.* disponible en: http://alejandrodelgadomoreno.com/2010/01/aniversario-de-la-ley-de-delitos.html

Díaz García, A. (7 de noviembre de 2010). La información como bien protegido en el delito de transferencia no consentida de activos. Artículo 269J. Código Penal Colombiano. En *Slideshare. Recuperado de:* http://www.slideshare.net/Alediaganet/la-informacin-como-activo-protegido-penalmente-en-colombia

Equipo de Redacción. (31 de octubre de 2011). Más de 400 millones de intentos de acceso malicioso fueron bloqueados por el blindaje al sitio Web de la Registraduría. *Sincelejo Herald.* Recuperado de: http://sincelejoherald.com/issue/noviembre-1-de-2011/article/mas-de-400-millones-de-intentos-de-acceso-malicioso-fueron-bloqueados-por-el-blindaje-al-sitio-web-de-la-registraduria

Fernández, C. A. (17 de noviembre de 2002). Prueba pericial. Delitos y tecnología de la información. Características y valoración en el proceso penal argentino. *Delitos informáticos.com.* Recuperado de: http://www.delitosinformaticos.com/delitos/prueba.shtml

García Espinal, Y. (26 de marzo de 2009). Delitos informáticos en Colombia. En *Scribd.* Recuperado de: http://es.scribd.com/doc/13643827/Delitos-informaticos-en-Colombia

García Noguera, N. (15 de julio de 2002). Delitos Informáticos en el Código Penal Español. *En Delitos informáticos.com.* Recuperado de: http://www.delitosinformaticos.com/delitos/codigopenal.shtml

García Noguera, N. (23 de abril de 2001). Delito de estafa informática (Artículo 248.2 C.P. Español). *En Delitos informáticos.com.* Recuperado de: http://www.delitosinformaticos.com/estafas/delito.shtml

Instituto de Educación Secundaria Tiempos Modernos. Sistemas electrónicos. En *Tiempos modernos.* Recuperado de: http://www.iestiemposmodernos.com/depart/dtec/Recursos/siselec4.pdf

La F.M. (31 de octubre de 2011). El registrador Carlos A. Sánchez dijo que fueron bloqueados más de 400 millones de intentos de hackeos. Recuperado de: http://www.lafm.com.co/audios/audios/31-10-11/el-registrador-carlos-s-nchez-dijo-que-fueron-bloqueados-m-s-de-400-millones

Meneses, C. A. (30 de septiembre de 2002). Delitos Informáticos y nuevas formas de resolución del conflicto penal chileno. En *Delitos informáticos.com.* Recuperado de: http://www.delitosinformaticos.com/delitos/penalchileno.shtml

Radio Nacional de Colombia. (31 de octubre de 2011). Registraduría bloqueó más de 400 millones de intentos de acceso de tráfico malicioso. Recuperado de: http://www.radionacionaldecolombia.gov.co/index.php?option=com_topcontent&view=article&id=22639:registraduria-bloqueo-mas-de-de-400-millones-de-intentos-de-acceso-de-trafico-malicioso&catid=1:noticias

Real Academia Española (2001). *Diccionario de la lengua española* (22 ed.) Recuperado de: http://www.rae.es

Semana.com. (31 de octubre de 2011). A la Registraduría le funcionó su blindaje 'antihackers'. *Semana.com.* Recuperado de: http://www.semana.com/nacion/registraduria-funciono-su-blindaje-anti-hackers/166756-3.aspx

Legislación

Ley 599 de 2000 por medio de la cual se expide el Código Penal de Colombia.

Ley 906 de 2004 por medio de la cual se expide el Código de Procedimiento Penal.

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 1288 de 2009 por medio del cual se expiden normas para fortalecer el marco legal 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.

Jurisprudencia

Corte Constitucional de Colombia, 2007. Sentencia C – 336, M.P.: Jaime Córdoba Triviño.

Corte Constitucional de Colombia, 2009. Sentencia C – 025, M.P.: Rodrigo Escobar Gil.

Corte Constitucional de Colombia, 2010. Sentencia C – 334, M.P.: Juan Carlos Henao Pérez.

Corte Constitucional de Colombia, 2009. Sentencia C – 131, M.P.: Nilson Pinilla Pinilla.

CAPÍTULO 4.

Referencias

- Normativa

Colombia. Congreso de la República. Ley 906 de 2004.

Consejo Nacional de Policía Judicial (s.d.) *Manual único de Policía Judicial.* Bogotá: Consejo Nacional de Policía Judicial.

Fiscalía General de la Nación (2004). *Manual de procedimientos para cadena de custodia.* Bogotá: Fiscalía General de la Nación.

Pino, S. A. (2009). *Manual de manejo de evidencias digitales y entornos informáticos.* Ecuador: Fiscalía General del Estado.

Pino, S. A. (2009). *Perfil sobre los delitos informáticos en el Ecuador. Ecuador:* Fiscalía General del Estado.

Rivolta, M. (2007). Medios de prueba electrónicos: estado de avance en la legislación argentina". En panel Gobierno electrónico: experiencias en el poder legislativo y el poder judicial, *Cuarto Congreso Argentino de Administración Pública.* Congreso efectuado en Buenos Aires.

Standards Australia International, HB 171 (2003). *Handbook Guidelines for the management of IT evidence.* Sydney: Standards Australia International.

U.S. Department of Justice (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*. Washington: Departemnt of Justice.

Cibergrafía

Bonilla, J. E. (2009). Computación forense. En *Slideshare.* Recuperado de http://www.slideshare.net/joseber/computacin-forense

Brezinski, D. & Killalea, T. (2002). Guidelines for Evidence Collection and Archiving. En The Internet Engineering Task Force (IETF). Recuperado de http://www.ietf.org/rfc/rfc3227.txt

Brownlee, N. & Guttman, E. (1998). *Expectations for Computer Security Incident Response.* Recuperado de http://www.ietf.org/rfc/rfc2350.txt

Carroll, O., Brannon, S., & Song, T. (enero, 2008). Computer Forensics: Digital Forensic Analysis Methodology. *Computer Forensics 56*(1). Recuperado de http://www.justice.gov/usao/eousa/foia_reading_room/usab5601.pdf

Dodge, R. & Cook, D. (2007). Out of the Box Forensics Labs. *En 40th Annual Hawaii International Conference on System Sciences (HICSS'07).* Recuperado de http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2007.1

ICONTEC. (2005). Norma técnica NTC-ISO/IEC colombiana 17025. En I*CONTEC.* Recuperado de http://www.itp.gob.pe/normatividad/demos/doc/Normas%20Internacionales/Union%20Europea/ISO/ISO17025LaboratorioEnsayo.pdf

Jarrett, M., Bailie, M., Hagen, E. & Eltringham, S. (2002). *Prosecuting Computer Crimes. Computer Crime and Intellectual Property Section Criminal Division.* Recuperado de: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

Jarrett, M., Bailie, M., Hagen, E. & Judish, N. (2002). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Recuperado de http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

Kent, K., Chevalier, S., Grance, T. & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. En *Computer Security Division.* Recuperado de http://goo.gl/yMTD1

Locard, E. (2010). *Manual de Técnica Policíaca*. Valladolid: Maxtor. Recuperado de http://books.google.com.co/books?id=kjIs1nquYEYC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Scarfone, K., Grance, T., & Masone K. (2008). Computer Security Incident Handling Guide. En *National Institute of Standards and Technology.* Recuperada de http://www.s3dev.com/clientuploads/pdfs/ComputerSecurityIncidentHandlingGuide.pdf

The FBI (2011). Digital Forensics. En *The FBI.* Recuperado de http://www.fbi.gov/news/stories/2011/may/forensics_053111

Tuohey J. (2004). Government Uses Color Laser Printer Technology to Track Documents En *PC World.* Recuperado de http://www.pcworld.com/article/118664/article.html

Valdés Moreno, C. E. (2009), Medicina legal y ciencias forenses. En *Scribd.* Recuperado de: http://es.scribd.com/doc/73435726/Medicina-Legal-y-Ciencias-Forenses

CAPÍTULO 5.

Referencias

Aristizábal, C. A. (2008). *Guía Teoría y Metodología de la Investigación.* Medellín: Fundación Universitaria Luis Amigó.

Babbie, E. (2000). *Fundamentos de la investigación social.* México: Thomson.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2007) *Metodología de Investigación.* (4 ed.) México: McGraw-Hill.

Jiménez Marques, E. (2004). *Análisis de la investigación cuantitativa, métodos clásicos.* Zaragoza: Fondo Editorial UNAULA. Recuperado http://unaula.edu.co/sites/default/files/ACERCAMIENTO%20A%20MODALIDADES%20DE.pdf. 22 marzo 2011.

Okuda Benavides, M. & Gómez-Restrepo, C. (enero-marzo, 2005). Métodos en investigación cualitativa: triangulación. *Revista Colombiana de Psiquiatría 34*(1).

Salkind, N. (1999) *Métodos de investigación.* México: Prentice-Hall.

Cibergrafía

Briones, G. (2002). *Metodología de la investigación cuantitativa en las ciencias sociales.* Bogotá: Arfo Editores e impresores. Recuperado de http://biblioteca.ucn.edu.co/repositorio/Maestria/SemInvestg2/documentos/Doc12%20-20Metodologia%20de%20la%20investigacion%20cuantitativa%20en%20CS.pdf

CAPÍTULO 6.

Referencias

- Doctrinal

Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Recuperado de: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf. 15 abril 2013.

Convención Cibercrimen dada en Budapest 2001

Colombia. Departamento Nacional de Planeación. Documento CONPES 3701 de 2011

Consejo Nacional de Policía Judicial (s.f.) *Manual único de Policía Judicial.* Bogotá: Consejo Nacional de Policía Judicial.

Ley 599 de 2000 por medio de la cual se expide el Código Penal de Colombia.

Ley 906 de 2004 por medio de la cual se expide el Código de Procedimiento Penal.

Cibergrafía

Consejo de Europa (2001). *Convenio sobre la ciberdelincuencia.* Budapest: Council of Europe. Recuperado de http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.coe.int%2Ft%2Fdghl%2Fstandardsetting%2Ft-cy%2FETS_185_spanish.PDF&ei=oDJaUPniBoi-9QS0poDwDQ&usg=AFQjCNH89PD_ieJFvv8VRRsdeXkslWK8rA

CONCLUSIONES Y RECOMENDACIONES.

Referencias

Consejo de Europa (2001). *Convenio sobre la ciberdelincuencia.* Budapest: Council of Europe. Recuperado de http://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.coe.int%2Ft%2Fdghl%2Fstandardsetting%2Ft-cy%2FETS_185_spanish.PDF&ei=oDJaUPniBoi-9QS0poDwDQ&usg=AFQjCNH89PD_ieJFvv8VRRsdeXkslWK8rA

ANEXOS

ANEXOS

En la presente unidad podrán verificarse los instrumentos aplicados como encuesta cerrada y entrevistas a profundidad, resultados que fueron analizados en el capítulo 5 del texto.

Formato entrevistas a profundidad

ENTREVISTA A PROFUNDIDAD **EXPERTOS FORENSES INFORMÁTICOS** Proyecto de Investigación "Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009"
Objetivo general: establecer la evidencia digital requerida para dar soporte probatorio en la investigación de la comisión de los delitos informáticos expedidos con la Ley 1273 de 2009, desde los medios técnicos, tecnológicos y científicos que garanticen la validez y eficacia de la imputación o acusación conforme con el ordenamiento jurídico colombiano. Ejes temáticos de la investigación: delitos informáticos, computación forense, técnicas aplicadas en la investigación criminal, y técnicas y métodos utilizados por ciberdelincuentes. En la etapa de trabajo de campo proyectada para el presente proyecto de investigación, y con el propósito de alcanzar los objetivos propuestos, agradecemos se sirva resolver los cuestionamientos del presente instrumento tipo ENTREVISTA A PROFUNDIDAD, y a partir de sus conocimientos y experiencia responda cada una de las preguntas indicadas.

Nombre:		
Título profesional:	Pregrado:	Posgrado:
Actividad laboral actual:		Municipio:

Objetivo específico 1

Presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria.

Pregunta 1. ¿Conoce los delitos informáticos vigentes en la legislación penal de Colombia? En caso de ser afirmativo complemente en su respuesta lo siguiente: ¿Los delitos informáticos dispuestos por la legislación penal colombiana son suficientes y pertinentes como figuras que penalizan la ciberdelincuencia?

Pregunta 2. ¿Qué diferencia el conjunto de delitos informáticos en relación con los delitos tradicionales, dispuestos en la legislación penal colombiana?

Pregunta 3. Teniendo en cuenta su calidad de experto forense informático ¿cree que los ciberdelincuentes y los medios de ataque han quedado regulados en la legislación colombiana?

Pregunta 4. ¿Considera que las disposiciones normativas en Colombia se ajustan a las disposiciones internacionales en materia de delitos informáticos y protocolos forenses para tratamiento de evidencias digitales?

Pregunta 5. ¿Creería pertinente modificar, adicionar o derogar la redacción de uno o varios de los tipos penales consagrados en la Ley 1273 de 2009? En caso afirmativo, ¿de qué forma sería más pertinente su consagración normativa?

Objetivo específico 2

Listar los medios probatorios existentes a partir de la Ley 906 de 2004, que son generalmente aceptados en Colombia, y evidenciar cuáles son o si se pueden presentar como evidencia digital y física en relación con un tipo penal informático.

Pregunta 1.
A partir de la Ley 906 de 2004, en el capítulo de pruebas en general, cree usted que ¿la legislación colombiana cuenta con los medios probatorios pertinentes y suficientes para la obtención de pruebas válidas en los casos de delitos informáticos, Ley 1273 de 2009?

Pregunta 2.
¿Son pertinentes los medios probatorios de la legislación colombiana en materia penal informática?

Pregunta 3.
Partiendo de que el medio de prueba denominado *mensaje de datos* pertenece al grupo de pruebas documentales reguladas en el Artículo 424 de la Ley 906 de 2006, cree usted que ¿este medio de prueba se encuentra regulado de forma adecuada en el código de procedimiento penal y le evita problemas en la presentación de su informe forense? Favor justifique su respuesta.

Pregunta 4.
Partiendo del principio de libertad probatoria que consagra la libertad de utilización de los medios de prueba, siempre y cuando estos sean obtenidos en forma legal ¿son pertinentes los medios probatorios existentes en la legislación procesal penal para el tratamiento del EMP y la PRUEBA, en caso penal de delitos informáticos?

Pregunta 5.
En materia de aplicación de protocolos en el tratamiento forense no hay vigilancia y control por parte de una entidad competente del Estado, respecto de los protocolos que se aplican en un peritaje forense informático; igualmente, a nivel normativo hay ausencia de estándar de procedimientos en relación con las técnicas forenses, se podría decir ¿que la verdad probatoria en un proceso judicial de delitos informáticos depende del conocimiento y profesionalidad del experto forense? En caso afirmativo o negativo, favor indique brevemente su postura.

Objetivo específico 3

Identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia.

Pregunta 1.
¿Qué protocolo de tratamiento y recuperación de información en un incidente informático ocurrido en Colombia es más recomendable a partir de las disposiciones en el campo penal concordadas con los lineamientos del CONPES 3701 emitido el 14 de julio de 2011?

Pregunta 2.
¿Conoce los lineamientos que en materia de cibercriminalidad ha establecido el gobierno nacional con la expedición el día 14 de julio de 2011 del documento CONPES 3701 en materia de ciberseguridad y ciberdefensa? Indique su postura respecto a esto.

Objetivo específico 4

Verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis post-mortem de un incidente en Colombia.

Pregunta 1.
¿Cree pertinente el protocolo de cadena de custodia existente en Colombia para garantizar la validez del análisis post-mortem en los incidentes informáticos? En caso de respuesta afirmativa indique si ¿todos los tipos penales consagrados en la Ley 1273 de 2009 se protegen con este protocolo de cadena de custodia? En caso de respuesta negativa indique ¿qué le podría mejorar al protocolo?

Pregunta 2.
En la etapa de investigación de un incidente informático: ¿Cuáles son los eventos más frecuentes que presentan alteración del EMP y en consecuencia altera la evidencia digital obtenida en laboratorio?, en consecuencia ¿de qué forma podría evitarse este tipo de afectaciones para los EMP?

Objetivo específico 5

Analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal.

Pregunta.
El experto forense ante un incidente informático se encuentra en un paradigma frente a la elección del protocolo más adecuado para manejar, conservar y almacenar la evidencia digital, pudiendo garantizar la confiabilidad e integridad de la evidencia digital, ¿existen protocolos en Colombia que permitan ser aplicados en el tratamiento de un incidente, a prueba de errores del experto forense, y en consecuencia, la inexperiencia en la ejecución de la labor sea de fácil notoriedad con el fin de evitar la afectación al EMP presentado en juicio para obtener la prueba digital del argumento fundamentado por esta?

Pregunta.
Recientemente, en el documento CONPES 3701, se indicó que: el entrenamiento y formación de los funcionarios públicos y privados para reaccionar como primeros respondientes ante la comisión de los delitos informáticos es deficiente. En muchas ocasiones se pierde la cadena de custodia de la evidencia digital y se generan dificultades en la realización de las investigaciones forenses. ¿Cree usted que la ausencia significativa de recurso humano y de protocolos forenses específicos sea un estándar nacional o internacional, puede ser solucionada con que se acojan protocolos pertinentes para el tratamiento de las conductas tipificadas en Colombia? En caso afirmativo: ¿Qué protocolos sugeriría usted que pueden ser aplicados a todos los tipos penales existentes en la Ley 1273 de 2009?

ENTREVISTA A PROFUNDIDAD
EXPERTOS ABOGADOS Y JUECES

Proyecto de Investigación
"Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009"

Objetivo general: establecer la evidencia digital requerida para dar soporte probatorio en la investigación de la comisión de los delitos informáticos expedidos con la Ley 1273 de 2009, desde los medios técnicos, tecnológicos y científicos que garanticen la validez y eficacia de la imputación o acusación conforme con el ordenamiento jurídico colombiano.

Ejes temáticos de la investigación: delitos informáticos, computación forense, técnicas aplicadas en la investigación criminal, y técnicas y métodos utilizados por ciberdelincuentes.

En la etapa de trabajo de campo proyectada para el presente proyecto de investigación, y con el propósito de alcanzar los objetivos propuestos, agradecemos se sirva resolver los cuestionamientos del presente instrumento tipo ENTREVISTA A PROFUNDIDAD, y a partir de sus conocimientos y experiencias responda cada una de las preguntas indicadas.

Nombre:		
Título profesional:	Pregrado:	Posgrado:
Actividad laboral actual:		Municipio:

Objetivo específico 1

Presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria.

Pregunta.
¿A partir de su conocimiento jurídico considera usted que están correctamente tipificados los delitos informáticos en la Ley 1273 de 2009?

Pregunta.
¿Considerando el aumento del uso de la tecnología como medio de comunicación, pero el cual también puede ser utilizado para cometer un hecho punible, la norma será clara al plantear ciertos términos técnicos para que cualquier jurista pueda interpretar la misma?

Pregunta.
Recientemente el gobierno nacional emitió el CONPES 3710, en caso de conocer el texto del mismo, ¿es posible afirmar que el desarrollo legislativo actual en cuanto a tipos penales y medios de prueba aplicables en materia de delitos informáticos requiere una reforma urgente o por el contrario, el cambio en Colombia es frente al recurso físico y humano dedicado a las unidades de investigación de delitos informáticos en las distintas entidades del Estado y las entidades privadas?

Objetivo específico 2

Listar los medios probatorios existentes a partir de la Ley 906 de 2004, que son generalmente aceptados en Colombia, y evidenciar cuáles son o cuáles se pueden presentar como evidencia digital y física en relación con un tipo penal informático.

Pregunta. ¿Cuál sería para usted el medio probatorio más adecuado para cuando se cometan estas conductas punibles?

Pregunta. La evidencia digital en el proceso se puede equiparar a un documento, entonces ¿cuál es el medio en el que usted puede ampararse para defender a su cliente?

Objetivo específico 3

Identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia.

Pregunta. En cuanto a la prueba digital se refiere, para que esta sea válida en juicio ¿será que en Colombia existen expertos forenses informáticos, tanto en el campo privado como público, que puedan dar su peritaje y certificar su experiencia?

Pregunta. Desde su conocimiento jurídico ¿cree que basta tener sólo su conocimiento o necesita la experiencia de otro profesional para recuperar la información a través de cualquier medio probatorio?

Objetivo específico 4

Verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis post mortem de un incidente en Colombia.

Pregunta. Frente a los lineamientos de cadena de custodia existentes para el tratamiento y manipulación de los elementos materiales probatorios en un delito informático en Colombia ¿qué opina usted frente al reconocimiento y aplicación que se les da a estos por parte de la mayoría de la población, en la calidad de defensor contractual o público, y de la valoración que de esta hace el juez de control de garantías?

Pregunta.
En la etapa de investigación de un incidente informático ¿cuáles son los eventos más frecuentes en los que se presenta alteración de la evidencia digital y cómo se podrían evitar?

Objetivo específico 5

Analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal.

Pregunta.
El experto forense frente a un incidente informático se encuentra en un paradigma frente a la elección del protocolo más adecuado para manejar, conservar y almacenar la evidencia digital, pudiendo garantizar la confiabilidad e integridad de la evidencia digital, es por ello que ¿existen protocolos en Colombia que permitan ser aplicados en el tratamiento de un incidente, a prueba de errores del experto forense, y en consecuencia, la inexperiencia en la ejecución de la labor sea de fácil notoriedad, con el fin de evitar la afectación al EMP presentado en juicio para obtener la prueba digital del argumento fundamentado por esta?

Pregunta.
Recientemente en el documento CONPES 3710 se indicó que el entrenamiento y formación de los funcionarios públicos y privados para reaccionar como primeros respondientes ante la comisión de los delitos informáticos es deficiente. En muchas ocasiones se pierde la cadena de custodia de la evidencia digital y se generan dificultades en la realización de las investigaciones forenses. ¿Cree usted que la ausencia significativa de recursos humanos, y de protocolos forenses, sea este un estándar nacional o internacional, puede ser solucionada con que se acojan protocolos pertinentes para el tratamiento de las conductas tipificadas en Colombia?

Formato encuestas cerradas

ENCUESTA FISCALES: Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009

El Grupo de Investigaciones Jurídicas y Sociales de la Facultad de Derecho y Ciencias Políticas de la Fundación Universitaria Luis Amigó, el Grupo de Investigaciones en Responsabilidad Jurídica y Social Empresarial de la Corporación Universitaria de Colombia - IDEAS, y el Grupo de Investigación en Redes y Materiales de Distribución de la Facultad de Ingenierías de la Universidad EAFIT adelantan el citado proyecto de investigación. En la etapa de trabajo de campo proyectada para el presente proyecto de investigación, y con el propósito de alcanzar los objetivos propuestos, agradecemos se sirva leer detenidamente la siguiente ENCUESTA CERRADA, y a partir de sus conocimientos y experiencia responda cada una de las preguntas indicadas.

***Obligatorio**

DATOS PERSONALES*SEXO

- FEMENINO
- MASCULINO

DATOS DEL LUGAR DE TRABAJO*FISCALÍA NÚMERO...

UBICACIÓN DEL LUGAR DE TRABAJO*MUNICIPIO DONDE SE DESEMPEÑA COMO FISCAL

- COPACABANA
- BELLO
- MEDELLÍN
- SABANETA
- ITAGÜÍ
- ENVIGADO
- LA ESTRELLA
- CALDAS
- Otro

Objetivo: presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria.*¿Reconoce usted el conjunto de tipos penales informáticos vigentes en la legislación colombiana?

- SÍ
- NO

*En su desempeño como Fiscal ¿ha adelantado alguna investigación en materia de delitos informáticos?

- SÍ
- NO

*En su desempeño como Fiscal ¿ha adelantado alguna IMPUTACIÓN en materia de delitos informáticos?

- SÍ
- NO

*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
¿Considera usted que los tipos penales informáticos han sido correctamente divulgados y tratados por el sector jurídico, judicial y académico?	○	○	○	○	○
¿Cree usted que los tipos penales consagrados en la ley colombiana son suficientes para procesar las diferentes conductas que se desarrollan en el campo tecnológico?	○	○	○	○	○
¿Cree usted que el capítulo de los delitos informáticos vigente en la legislación colombiana tiene redactado de manera clara y comprensible cada tipo penal?	○	○	○	○	○

Objetivo: listar los medios probatorios existentes a partir de la Ley 906 de 2004, que son generalmente aceptados en Colombia, y evidenciar cuáles son o se pueden presentar como evidencia digital o física en relación con un tipo penal informático.*De los medios probatorios avalados en el Código de Procedimiento Penal, ¿conoce cuáles son pertinentes para probar la violación del bien jurídico tutelado en la Ley 1273 de 2009?

- ○ SÍ
- ○ NO

*

	TOTALMENTE DE ACUERDO	PARCIALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO
¿Comparte usted que la caracterización de la prueba para la defensa en juicio en materia de delitos informáticos es clara?					
¿Estima válido que los medios probatorios existentes en la Ley 906 de 2004 pueden ser usados como EVIDENCIA digital o física en un proceso por delito informático?					
¿Estima válido que los medios probatorios existentes en la Ley 906 de 2004 pueden ser usados como PRUEBA digital o física en un proceso por delito informático?					

Objetivo: identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia.*¿Conoce usted los protocolos forenses que deben aplicarse en Colombia para la investigación de un delitos informático?

- SÍ
- NO

*¿Conoce las calidades, capacidades, formación profesional y la certificación que debe poseer el experto forense informático para la obtención e informe como perito en pruebas electrónicas?

- SÍ
- NO

*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
¿Qué tan de acuerdo está con que en Colombia existan técnicas de tratamiento y recuperación de información en incidentes informáticos?	○	○	○	○	○
Como Fiscal ¿está de acuerdo en asegurar que cuenta con la capacitación suficiente para aplicar técnicas de tratamiento y recuperación de información en un incidente informático?	○	○	○	○	○

*¿Conoce qué protocolos de análisis debe seguir el investigador de forma para cada tipo penal informático que se investiga?

- ○ SÍ
- ○ NO

Objetivo: verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis *post mortem* de un incidente en Colombia.*¿Conoce el protocolo de cadena de custodia para el análisis de dispositivos de almacenamiento digital con fines forenses?

- ○ SÍ
- ○ NO

*¿Usted sabe cuáles requisitos formales y materiales debe verificar del EMP en el tratamiento de laboratorio forense con el fin de garantizar que la evidencia digital sea aceptada como prueba electrónica que soporte los hechos que se alegan?

- ○ SÍ
- ○ NO

Objetivo: analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal.*¿Conoce el procedimiento que aplica la unidad de investigación criminal de la policía para la recepción, análisis de elementos, materiales, prueba y que finaliza con la entrega del informe del investigador de laboratorio y los elementos materiales de prueba?

- SÍ
- NO

*Si su respuesta anterior fue afirmativa, responda: ¿Este procedimiento permite la aplicación de protocolos impertinentes en el tratamiento del EMP en el laboratorio forense informático?

- SÍ
- NO

*¿Cree usted que una técnica o protocolo mal aplicado puede viciar la evidencia digital que se espera sea avalada como prueba por el juez de control de garantías?

- SÍ
- NO

0

Enviar

Con la tecnología de Google DocsInformar sobre abusos-Condiciones del servicio-Otros términos

ENCUESTA JUECES: “Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009”

El Grupo de Investigaciones Jurídicas y Sociales de la Facultad de Derecho y Ciencias Políticas de la Fundación Universitaria Luis Amigó, el Grupo de Investigaciones en Responsabilidad Jurídica y Social Empresarial de la Corporación Universitaria de Colombia - IDEAS, y el Grupo de Investigación en Redes y Materiales de Distribución de la Facultad de Ingenierías de la Universidad EAFIT adelantan el citado proyecto de investigación. En la etapa de trabajo de campo proyectada para el presente proyecto de investigación, y con el propósito de alcanzar los objetivos propuestos, agradecemos se sirva leer detenidamente la siguiente ENCUESTA CERRADA, y a partir de sus conocimientos y experiencia responda cada una de las preguntas indicadas.

***Obligatorio**

DATOS PERSONALES*SEXO

- ○ MASCULINO
- ○ FEMENINO

Ejemplo de pregunta 2*JUZGADO

- ○ MUNICIPAL
- ○ CIRCUITO
- ○ ESPECIALIZADO
- ○ PROMISCUO

*MUNICIPIO DONDE SE DESEMPEÑA COMO JUEZ PENAL

- ○ COPACABANA
- ○ BELLO
- ○ MEDELLÍN
- ○ ENVIGADO
- ○ LA ESTRELLA
- ○ SABANETA
- ○ ITAGÜÍ
- ○ CALDAS

Objetivo: presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria.*¿Reconoce usted el conjunto de tipos penales informáticos vigentes en la legislación colombiana?

- SÍ
- NO

*¿Considera usted que los tipos penales informáticos han sido correctamente divulgados y tratados por el sector jurídico, judicial y académico?

- SÍ
- NO

*En su desempeño como Juez, ¿ha conocido procesos en materia de delitos informáticos?

- SÍ
- NO

*En su desempeño como Juez, ¿ha concedido la IMPUTACIÓN de algún delito informático solicitado por la Fiscalía en la correspondiente etapa del proceso?

- SÍ
- NO

*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
¿Está usted de acuerdo en que los delitos informáticos vigentes en Colombia son suficientes para atender las modalidades delictivas en las que incurren los sujetos activos de dichas conductas?	○	○	○	○	○
¿Está usted de acuerdo en que los delitos informáticos vigentes en la legislación colombiana permiten desde su redacción una adecuación típica poco problemática?	○	○	○	○	○
¿Usted está de acuerdo en que los tipos penales consagrados en la ley colombiana son suficientes para procesar las diferentes conductas que se desarrollan en el campo tecnológico?	○	○	○	○	○

Objetivo: listar los medios probatorios existentes a partir de la Ley 906 de 2004 que son generalmente aceptados en Colombia, y evidenciar cuáles son o cuáles se pueden presentar como evidencia digital o física en relación con un tipo penal informático.*De los medios probatorios avalados en el Código de Procedimiento Penal, ¿conoce cuáles son pertinentes para probar la violación del bien jurídico tutelado en la Ley 1273 de 2009?

- ○ SÍ
- ○ NO

*Teniendo en cuenta los medios probatorios indicados en la ley penal procesal ¿son suficientes para probar la violación y vulneración del bien jurídico tutelado en la Ley 1273 de 2009 con la ocurrencia de uno o varios tipos penales consagrados en la misma ley?

- ○ SÍ
- ○ NO

*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE / NO RESPONDE
Para usted ¿la caracterización de la prueba para la defensa en juicio en materia de delitos informáticos es clara?	○	○	○	○	○
¿Usted está de acuerdo con que los medios probatorios existentes en la Ley 906 de 2004 pueden ser usados como EVIDENCIA digital o física en un proceso por delito informático?	○	○	○	○	○

Objetivo: identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia.*¿Conoce usted los protocolos forenses que deben aplicarse en Colombia para la investigación de un delito informático?

- ○ SÍ
- ○ NO

Pregunta sin título*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
Si su respuesta anterior fue afirmativa, responda: ¿Qué tan de acuerdo está con que en Colombia no existan técnicas de tratamiento y recuperación de información acogidas por la legislación, en incidentes informáticos, y queda en manos del ingeniero forense la implementación y validación del protocolo aplicado, frente a la legalidad y pertinencia de la prueba?	○	○	○	○	○
Teniendo en cuenta los análisis recientes dados en el documento CONPES 3701 sobre ciberseguridad, como Juez responda: ¿Está de acuerdo en asegurar que cuenta con la capacitación y conocimiento suficiente para la valoración de técnicas de tratamiento y recuperación de información en un incidente informático, aplicadas por un perito forense informático, prueba aportada por las partes procesales en juicio?	○	○	○	○	○

*¿Conoce las calidades, capacidades, formación profesional y la certificación que debe poseer el experto forense informático para la obtención del informe como perito en pruebas electrónicas y que este concepto le sirva de soporte probatorio válido para sustentar su fallo?

- ○ SÍ
- ○ NO

Objetivo: verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis *post mortem* de un incidente en Colombia.*¿Conoce el protocolo de cadena de custodia a cumplirse en el análisis de dispositivos de almacenamiento digital que debe evidenciarse en el informe pericial del experto forense informático a fin de validar, en el caso de jueces de control de garantías, o valorar, en el caso de jueces de conocimiento, la evidencia digital como EMP o como prueba digital, y permita fallar en Derecho?

- ○ SÍ
- ○ NO

*En el caso de jueces de control de garantías que validan el EMP para ser presentado como prueba ante el juez de conocimiento que valora la evidencia digital como prueba digital ¿sabe usted cuáles son los requisitos formales y materiales a verificar, en el informe pericial presentado por el experto forense dando cuenta del resultado del tratamiento en el laboratorio forense, con el fin de garantizar que la evidencia digital sea aceptada como prueba digital que fundamenta los hechos que se alegan o se controvierten, posteriormente a valorarse para su fallo?

- ○ SÍ
- ○ NO

Objetivo: analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal.*¿Conoce el procedimiento que aplica la unidad de investigación criminal de la policía para la recepción, análisis de elementos materiales prueba y finaliza con la entrega del informe del investigador del laboratorio y elementos materiales de prueba?

- ○ SÍ
- ○ NO

*Si su respuesta anterior fue afirmativa como juez de control de garantías frente al EMP, responda: ¿Este procedimiento permite la aplicación de protocolos impertinentes en el tratamiento del EMP en el laboratorio forense informático?

- ○ SÍ
- ○ NO

*Si su respuesta a la pregunta 1 fue afirmativa como juez de conocimiento frente a la prueba digital, responda: ¿Este procedimiento permite la aplicación de protocolos impertinentes en el tratamiento del EMP en el laboratorio forense informático que posteriormente pueda enervar un trámite de nulidad procesal por prueba ilícita?

- ○ SÍ
- ○ NO

*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
¿Qué tan de acuerdo está frente a la necesidad de desarrollar una técnica que permita el hallazgo de información relevante en el transcurso de un caso de delito informático?					

Enviar

Con la tecnología de Google DocsInformar sobre abusos-Condiciones del servicio-Otros términos

ENCUESTA ABOGADO: “Informática forense y su aplicación en la investigación de los delitos informáticos consagrados en la Ley 1273 de 2009”

El Grupo de Investigaciones Jurídicas y Sociales de la Facultad de Derecho y Ciencias Políticas de la Fundación Universitaria Luis Amigó, el Grupo de Investigaciones en Responsabilidad Jurídica y Social Empresarial de la Corporación Universitaria de Colombia - IDEAS, y el Grupo de Investigación en Redes y Materiales de Distribución de la Facultad de Ingenierías de la Universidad EAFIT adelantan el citado proyecto de investigación. En la etapa de trabajo de campo proyectada para el presente proyecto de investigación, y con el propósito de alcanzar los objetivos propuestos, agradecemos se sirva leer detenidamente la siguiente ENCUESTA CERRADA, y a partir de sus conocimientos y experiencias, responda cada una de las preguntas indicadas.

***Obligatorio**

DATOS PERSONALES*SEXO

- ○ MASCULINO
- ○ FEMENINO

Pregunta sin título* MÁXIMO NIVEL DE FORMACIÓN

- ○ ABOGADO TITULADO
- ○ ESPECIALISTA EN DERECHO PENAL
- ○ ESPECIALISTA EN CRIMINOLOGÍA
- ○ MAGÍSTER
- ○ DOCTOR

Pregunta sin título* PRINCIPAL ACTIVIDAD LABORAL

- ○ LITIGIO
- ○ ASESORÍA JURÍDICA
- ○ ACADEMIA
- ○ INVESTIGACIÓN

Pregunta sin título* MUNICIPIO DONDE SE DESEMPEÑA LABORALMENTE

- COPACABANA
- BELLO
- MEDELLÍN
- LA ESTRELLA
- SABANETA
- ITAGÜÍ
- ENVIGADO
- CALDAS
- LA ESTRELLA

Objetivo: presentar el grupo de tipos penales informáticos existentes a partir de la Ley 1273 de 2009 y la legislación complementaria.*¿Reconoce usted el conjunto de tipos penales informáticos vigentes en la legislación colombiana?

- SÍ
- NO

Pregunta sin título*

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
¿Usted está de acuerdo con que los tipos penales informáticos han sido correctamente divulgados y tratados por el sector jurídico, judicial y académico?	○	○	○	○	○
¿Usted está de acuerdo con que los tipos penales consagrados en la ley colombiana son suficientes para procesar las diferentes conductas que se desarrollan en el campo tecnológico?	○	○	○	○	○
¿Usted está de acuerdo con que el capítulo de los delitos informáticos vigente en la legislación colombiana tiene redactado de manera clara y comprensible cada tipo penal?	○	○	○	○	○
¿Usted está de acuerdo con que la interpretación de cada tipo penal dada a instancias de los procesos de investigación es vigente con la consagración de los tipos penales en la Ley 1273 de 2009?	○	○	○	○	○

Objetivo: listar los medios probatorios existentes a partir de la Ley 906 de 2004 que son generalmente aceptados en Colombia, y evidenciar cuáles son o cuáles se pueden presentar como evidencia digital o física en relación con un tipo penal informático.*De los medios probatorios avalados en el Código de Procedimiento Penal, ¿conoce cuáles son pertinentes para probar la violación del bien jurídico tutelado en la Ley 1273 de 2009?

- ○ SÍ
- ○ NO

*¿Es clara para usted la caracterización de la prueba para la defensa en juicio en materia de delitos informáticos?

- SÍ
- NO

Pregunta sin título*¿Estima válida la falta de individualización en el capítulo de pruebas, sobre la evidencia digital, figura jurídica emergente con la tipificación del grupo de tipos penales denominado delitos informáticos a partir de la Ley 1273 de 2009?

- SÍ
- NO

Pregunta sin título*¿Sabe usted cuál o cuáles de los medios probatorios existentes en la Ley 906 de 2006 son los pertinentes para la investigación de delitos informáticos?

- SÍ
- NO

Pregunta sin título*Si su respuesta anterior fue afirmativa ¿conoce usted qué elementos tecnológicos y legales deben tener los elementos materiales probatorios para ser reconocidos como prueba digital en juicio, a partir de la Ley 906 de 2006?

- Sí
- NO

Pregunta sin título*¿Conoce usted el mensaje de datos consagrado por la Ley 906 de 2006 como medio de prueba documental, desde su definición hasta las modalidades tecnológicas aplicables?

- SÍ
- NO

Objetivo: identificar las distintas técnicas de tratamiento y recuperación de información en un incidente informático en Colombia.*¿Conoce usted el (los) protocolo(s) forense(s) que debe(n) aplicarse en Colombia para la investigación de un delito informático?

- SÍ
- NO

Pregunta sin título*¿Conoce las calidades, capacidades, formación profesional y la certificación del peritaje que el experto forense informático debe poseer para el tratamiento de la evidencia digital y la cadena de custodia de los dispositivos físicos como la información electrónica que estos contengan?

- SÍ
- NO

Pregunta sin título*¿Conoce usted protocolos internacionales para la obtención de evidencia digital en un laboratorio forense informático?

- SÍ
- NO

Objetivo: verificar los protocolos a seguir para la conservación de la cadena de custodia en el análisis *post mortem* de un incidente en Colombia. *¿Conoce usted los protocolos de cadena de custodia para que la recolección del elemento material probatorio, luego de su tratamiento en laboratorio, adquiera categoría de evidencia digital o física para ser reconocido en el juicio de delitos informáticos como prueba digital?

- SÍ
- NO

Pregunta sin título* Si su respuesta anterior fue positiva, responda: ¿Reconoce usted los protocolos de cadena de custodia como eficaces y pertinentes para la investigación forense en delitos informáticos?

- SÍ
- NO

Pregunta sin título*¿Establecería términos y condiciones adicionales al protocolo existente para el tratamiento del elemento material probatorio en una investigación forense de delitos informáticos?

- SÍ
- NO

Objetivo: analizar técnicas que permitan el hallazgo de información relevante en el transcurso de un caso penal *

	TOTALMENTE DE ACUERDO	DE ACUERDO	PARCIALMENTE DE ACUERDO	EN DESACUERDO	NO SABE/NO RESPONDE
¿Usted está de acuerdo con que los operadores judiciales, defensores e investigadores reconocen las técnicas de hallazgo probatorio presentado en juicio?	○	○	○	○	○
¿Usted está de acuerdo con que debería haber varios protocolos aplicables en Colombia para el tratamiento, recolección y entrega de informe forense informático?	○	○	○	○	○

Pregunta sin título*¿Intervino o interviene usted en algún caso penal donde se haya tenido como EMP un análisis de la evidencia digital desde la técnica (protocolo) aplicado para el hallazgo de la misma?

- ○ SÍ
- ○ NO

0

Enviar

Con la tecnología de Google DocsInformar sobre abusos-Condiciones del servicio-Otros términos

INFORMACIÓN DE LOS AUTORES

Juan Guillermo Lalinde Pulido: Matemático Universidad Nacional de Colombia, Ingeniero de Sistemas Universidad Eafit. Doctor en Ingeniería de Telecomunicaciones de la Universidad Politécnica de Valencia, España. Docente Investigador de la Escuela de Ingeniería de la Universidad Eafit. jlalinde@eafit.edu.co

Juan David Pineda Cárdenas: Ing. De Sistemas. Coordinador supercomputador EAFIT y UNIVERSIDAD PURDUE. Candidato a magíster en Seguridad Informática. Jpineda2@eafit.edu.co

Ana María Mesa Elneser: Abogada titulada de la Universidad de Medellín. Investigadora y Docente Universitaria. Especialista en Docencia Investigativa Universitaria. Egresada y Candidata a Magíster en Derecho Procesal Contemporáneo en la Universidad de Medellín. Catedrática de posgrados U de M, UNAULA, Funlam. Docente de pregrado de Facultad de Derecho de la Universidad Cooperativa de Colombia sede Medellín, de la Facultad de Derecho y Ciencias Políticas de la Fundación Universitaria Luis Amigó, de la facultad de derecho de la Universidad Autónoma Latinoamericana. Autora de varios escritos en derecho informático. Investigadora y experta en Derecho Informático. Asesora de empresas en Tecnología Informática y Datos Personales. ana.mesael@gmail.com y ana.mesael@amigo.edu.co

Jorge Eduardo Vásquez Santamaría. Editor. Abogado y candidato a Magister en Derecho de la Universidad de Medellín; especialista en Docencia Investigativa Universitaria de la Funlam. Docente investigador del Grupo de Investigaciones Ratio Juris de la Facultad de Derecho de la Universidad Autónoma Latinoamericana. Contacto: jorge.vasquez@unaula.edu.co