NUEVAS TECNOLOGÍAS EN LA INVESTIGACIÓN CRIMINAL

Aportes de la Informática a la Criminalística y las Ciencias Forenses

Compiladores Lilia Cortés Monsalve - Ana Haydee Di Iorio - Maribel Lagos Enríquez

Autores Lucía Belén Algieri - Enzo Ezequiel Cecchetti - Camilo Andrés Morales Ortiz
María Belén Álvarez Cestona - Bruno Constanzo - Lilia Cortes Monsalve
Isabela Conde Campos - Bryan Egea Suarez - Wilmer Mondragón Restrepo
Jovanne Esteban Ortiz Pérez - Oscar Vergara Taborda -Gerardo Elías Cortes Buitrago

NUEVAS TECNOLOGÍAS EN LA INVESTIGACIÓN CRIMINAL

Aportes de la Informática a la Criminalística y las Ciencias Forenses

NUEVAS TECNOLOGÍAS EN LA INVESTIGACIÓN CRIMINAL

Aportes de la Informática a la Criminalística y las Ciencias Forenses

COMPILADORES

Lilia Cortés Monsalve - Ana Haydee Di Iorio - Maribel Lagos Enríquez

AUTORES

Lucía Belén Algieri, Enzo Ezequiel Cecchetti, Camilo Andrés Morales Ortiz, María Belén Álvarez Cestona,

Bruno Constanzo, Lilia Cortes Monsalve, Isabela Conde Campos, Bryan Egea Suarez

Wilmer Mondragón Restrepo, Jovanne Esteban Ortiz Pérez, Oscar Vergara Taborda, Gerardo Elías Cortes Buitrago

Universidad libre

2020

Nuevas Tecnologías en la Investigación Criminal.
Aportes de la Informática a la Criminalística y las Ciencias Forenses
© Universidad Libre Seccional Cali - © Universidad de Fasta
© Compiladores: Lilia Cortés Monsalve - Ana Haydee Di Iorio - Maribel Lagos Enríquez
© Autores: Lucía Belén Algieri, Enzo Ezequiel Cecchetti, Camilo Andrés Morales Ortiz, María Belén Álvarez Cestona, Bruno Constanzo, Lilia Cortes Monsalve, Isabela Conde Campos, Bryan Egea Suarez, Wilmer Mondragón Restrepo, Jovanne Esteban Ortiz Pérez, Oscar Vergara Taborda, Gerardo Elías Cortes Buitrago
1a. Edición 200 ejemplares
Cali, Colombia - 2020v
ISBN:978-958-5545-78-6

Directivas Nacionales
Jorge Alarcón Niño
Presidente Nacional
Fernando Dejanon Rodriguez
Rector Nacional
Floro Hermes Gómez Pineda
Secretario General
Ricardo Zopó Méndez
Censor Nacional

Directivas Seccionales
Helio Fabio Ramirez Echeverry
Delegado Personal del Presidente
José Hoover Salazar Ríos
Rector Seccional
Ómar Bedoya Loaiza
Secretario Seccional
Gilberto Aranzazu Marulanda
Censor Seccional

Decano Facultad de Derecho, Ciencas Políticas y Sociales
Héctor Hernández Mahecha

Director Seccional de Investigaciones
Arnaldo Rios A.

Directora Centro de Investigaciones Facultad de Derecho, Ciencas Políticas y Sociales
Viviana A. Ramón Castro

José Hoover Salazar R.
Arnaldo Ríos A.
Viviana Ramón C.
María Mercedes Sinisterra
Armando Lucumi M.
Hugo Becquer P.
María Fernanda Jaramillo G.

Dirección Editorial
José Hoover Salazar Ríos
Arnaldo Ríos Alvarado
Viviana Ramón C.
María Mercedes Sinisterra
Armando Lucumi
Hugo Becquer Paz
María Fernanda Jaramillo G.

Dirección Editorial
Maria Fernanda Jaramillo Gonzalez

Diagramación e impresión
Artes Gráficas del Valle S.A.S.
Tel. 333 2742

©Editorial
Sello Editorial Universidad Libre Seccional Cali
Universidad Libre de Cali
Diagonal 37A No. 3-29 Barrio Santa Isabel
Teléfono: 524 0007 Ext- 1200, 1201, 1208
Cali – Colombia
2020

La responsabilidad de los textos contenidos en esta publicación es exclusiva de(l) (os) autor(es).
Prohibida la reproducción total o parcial, por cualquier medio fotográfico o digital, incluyendo las lecturas universitarias, sin previa autorización de(l) (os) autor(es).

CONTENIDO

Prólogo

Las tecnologías de la información y la comunicación han irrumpido en nuestra sociedad sin pedir permiso. Han cambiado nuestras vidas, las de todos, cualquiera sea la edad y ocupación, en todo lugar y durante todo el día; y esos cambios son irreversibles. Ya no tienen retorno. No hay vuelta atrás; ¡por el contrario!

El avance tecnológico es cada vez más veloz y su impacto cada vez más vertiginoso. El mundo es diferente y lo será cada vez más, cada día, todos los días. Nos despertamos cada mañana ante un mundo diferente que nos propone más y más cambios y nos exige adaptarnos para "sobrevivir"; adaptarnos a nuevas formas de interactuar, de estudiar, de trabajar, de pensar, en una sociedad con cada vez más problemas y más complejos.

Y en ese mundo, la Universidad, con su obligación moral de mejorar a la sociedad, a las personas, a las vidas. Con su deber social de crear conocimiento, divulgarlo, aplicarlo y transferirlo para dar lugar a nuevas tecnologías e innovaciones que harán que el mundo cambie un poco más todavía. En ese marco, la Universidad debe formar profesionales que sean capaces de vivir, contribuir, construir y seguir transformando el mundo para hacerlo mejor; y todo esto, sin comprometer los recursos de nuestras futuras generaciones. Un desafío institucional tremendo, pero, sobre todo, ¡apasionante!

Debemos cuidar la casa común para entregarla mejor a nuestros hijos y nietos, hacer una sociedad más justa, profesionales comprometidos, personas más solidarias, vidas más dignas, a partir del conocimiento.

Las universidades tampoco pueden desconocer, ni mucho menos ignorar la tecnología, como parte de su quehacer y de los conocimientos y competencias de los que debe dotar a sus graduados. La tecnología ayuda a generarlo y, a la vez, es producto de ese conocimiento. La investigación y desarrollo sin tecnología, hoy no tienen chance de impacto, pierden valor.

Lo mismo pasa en el campo profesional. La actuación profesional hoy está fuertemente determinada por la tecnología. En el campo de la investigación y práctica forense esto es evidente. Además de la responsabilidad estricta sobre las evidencias digitales, la tecnología en general y las TICS en particular, tienen un rol de "herramienta" o medio de auxilio al proceso forense en general y a la investigación criminal. La Investigación y Práctica Forense tienen un antes y un después de las TICS como herramienta. La Informática Forense afecta a todas las ciencias forenses, potencia sus métodos, les brinda efectividad y les proporciona

mejores evidencias. Fiscales y jueces se encuentran cada vez más frecuentemente con delitos que incorporan la tecnología como medio o como elemento contributivo para su ocurrencia, causas con evidencias digitales que considerar, y procesos de investigación que también incorporan medios tecnológicos para arribar a determinadas conclusiones.

La disciplina forense más antigua y paradigmática es la Medicina, que hoy se ve transformada sustancialmente por la disponibilidad de nuevos métodos y herramientas tecnológicas, cada vez más efectivas. El Médico Forense ya no puede actuar eficazmente sin recurrir a estas nuevas herramientas que han cambiado y seguirán cambiando permanentemente su tarea y le exigen nuevas competencias profesionales. La justicia y la sociedad toda hoy espera resultados de peritos que utilizan la última tecnología disponible para brindar pruebas objetivas fehacientes con respaldo científico. Lo mismo les pasa a los genetistas forenses, los odontólogos forenses, los físicos forenses, los químicos forenses, los contadores que hacen pericias contables, los licenciados en criminalística que coordinan los procesos de investigación y hasta los abogados, que requieren conocer las herramientas y métodos disponibles a efecto de dar valor a una prueba.

Hoy la tecnología interpela al derecho penal y desafía a la criminalística; "obtener pruebas" y "hacer justicia" requiere indefectiblemente del dominio de la tecnología, en particular de la informática aplicada. Esto hace que la informática se constituya en la herramienta fundamental de las Ciencias Forenses en la actualidad.

En este contexto, poner el foco en estas herramientas tecnológicas y su aplicación a la investigación y práctica en ciencias forenses es clave en el ámbito académico. La cooperación para el logro de estos objetivos es fundamental para nuestras instituciones y genera las posibilidades ciertas de desarrollo institucional y de nuestros estudiantes y egresados. Celebro, entonces, esta publicación conjunta, que viene a poner en evidencia el trabajo de nuestras Universidades en este campo y comparte generosamente nuestros desarrollos con la comunidad académico-científica internacional.

En nombre de la Universidad FASTA quiero felicitar a las compiladoras, autores y a todos quienes hicieron posible este libro. Agregar, que le dieron sentido al proyecto. Espero que sea sólo el primero de muchos proyectos de cooperación entre la UFASTA y la UNILIBRE.

Esp. Ing. Roberto Giordano Lerena
rogiord@ufasta.edu.ar
Decano, Profesor e Investigador Facultad de Ingeniería Universidad FASTA
Coordinador Comisión de Acreditación de Proyectos de Desarrollo Tecnológico Social del Ministerio de Educación, Cultura, Ciencia y Tecnología de la República Argentina

Presentación Maestría en Criminalística y Ciencias Forenses de la Universidad Libre Seccional Cali

La Universidad Libre de Colombia es una institución privada, de carácter laico, liberal, que inicio su funcionamiento en Bogotá el 13 de febrero de 1923, con las facultades de Derecho y Ciencias Políticas y de Ingeniería. Desde entonces, ha tenido por misión procurar a los colombianos una educación inspirada en los principios de libertad de cátedra y el pensamiento científico, inscrita en una visión humanista de la educación superior, por lo que todos sus programas académicos están orientados en este sentido. De allí que la ciencia al servicio del Derecho, que es el sentido primigenio de la criminalística y las ciencias forenses, ocupe un lugar importante dentro de la investigación adelantada en la Universidad Libre.

La actividad investigativa es central en el que hacer de la Universidad Libre, lo que le ha merecido el reconocimiento como una universidad acreditada de alta calidad, otorgado por el Ministerio de Educación de Colombia. En particular, la seccional Cali y su Facultad de Derecho, Ciencias Políticas y Sociales a la que está adscrita la Maestría, tiene 6 de sus grupos de investigación categorizados en A1, máxima categoría otorgada por Colciencias, institución gubernamental que en Colombia tiene a su cargo la coordinación de toda la actividad investigativa del país.

Las investigaciones que hoy presentamos ante la comunidad académica, representadas en dos capítulos de este libro, forman parte de los proyectos y líneas de investigación del grupo *Criminalística y Ciencias Forenses*, categoría A1 en Colciencias y fueron desarrollados por estudiantes de la Maestría. La Maestría desde que inició actividades en el año 2010, constituye una respuesta de la Universidad Libre Seccional Cali a la necesidad sentida en la región y el país, de contar con profesionales capacitados en la investigación académica dentro del campo de acción de la Criminalística y las Ciencias Forenses; profesionales con competencias suficientes para proponer y/o realizar proyectos de investigación que impacten en sus lugares de trabajo; en el sistema de justicia colombiano y en general, que contribuyan a la transformación y mejoramiento de la investigación forense mediante la creación o aplicación de los desarrollos y avances en esta área de conocimiento.

La investigación en la Maestría en Criminalística y Ciencias Forenses está articulada de manera directa con las líneas propuestas Colciencias. Dentro de la

clasificación de áreas de conocimiento y líneas de investigación realizada por esta Institución, los proyectos de investigación y los trabajos de producción investigativa de profesores y estudiantes de la Maestría en Criminalística y Ciencias Forenses están relacionados con los programas de ciencias básicas, humanas y sociales. En lo que atañe a las ciencias básicas la maestría investiga en temas relacionados con la Biología, Biomédicas, Física y Química, entre otros. En lo que respecta a las ciencias humanas y sociales, se adscriben al componente que Colciencias denomina conflicto, criminalidad, derechos, justicia y equidad.

El compendio que se presenta a la comunicada académica, está inscrito dentro de un emergente campo de investigación, cada vez más importante en el ámbito jurídico producido por la inclusión evidente de aparatos tecnológicos en todos los aspectos de las relaciones humanas, esta interacción ha ocasionado la inclusión de la Informática al mundo del derecho. La Informática es definida por algunos autores como una disciplina emergente e integradora, donde convergen diferentes disciplinas y/o ciencias como la computación, la electrónica, la cibernética, las telecomunicaciones, la matemática, la lógica, la lingüística, la ingeniería, la inteligencia artificial, la robótica, la biología, la psicología, las ciencias de la información, cognitivas, organización, entre otras; todas ellas orientadas al estudio y desarrollo de productos, servicios, sistemas e infraestructuras que la nueva sociedad de la información, el conocimiento y la red, demandan.

De acuerdo a lo anterior, en la Maestría en Criminalística y Ciencias Forenses cada vez es más frecuente que sus estudiantes y profesores se interesen por la investigación sobre las innovaciones, aportes, problemas y dificultades que se han presentados en la relación entre lo jurídico y la informática. Por eso, se seleccionaron para esta compilación dos trabajos de grado de maestría, el primero: *Análisis Estereoscópico de los Patrones de Impresión Producidos por los Sistemas de Suministro de Tinta de las Impresoras Epson Inkjet L120 y Xp231. Estudio De Caso*, realizado por Camilo Andrés Morales Ortiz y el segundo, lleva por título *Falencias en el Tratamiento de la Memoria Flash USB que Afectan la Validez Como Evidencia Digital y sus Consecuencias en el Sistema Penal Acusatorio Colombiano,* escrita por Wilmer Mondragón Restrepo y Jovanne Esteban Ortiz Pérez. Ambos trabajos abordan temas críticos y relevantes para la administración de justicia en Colombia.

Finalmente, se destaca de manera especial que este compendio es la primera actividad de cooperación académica entre la Universidad FASTA de Mar del Plata, Argentina y las Maestrías en Derecho Penal y Criminalística y Ciencias Forenses de la Universidad Libre Seccional Cali. Actividad que también hace parte de los fines planteados por la *Red Iberoamericana de Universidades e Institutos con Investigación en Derecho e Informática* - Red CIIDDI. Ha sido esta red la que ha posibilitado el intercambio de ideas y la movilidad de profesores, para la realización de proyectos conjuntos que pueden resultar de interés para el manejo de problemas comunes

que se presentan en los países que la integran. Esperamos que continúen estos esfuerzos académicos y que sea el comienzo de un fructífero camino de cooperación internacional propiciado desde las universidades e instituciones que pertenecen a la Red.

Doctora Maribel Lagos Enríquez
maribel.lagos@unilibre.edu.co
Coordinadora Académica de la Maestría en Criminalística y Ciencias Forenses
Profesora de la Facultad de Derecho, Ciencias Políticas y Sociales de la Universidad Libre Seccional Cali, Colombia

Presentación Licenciatura en Criminalística de la Universidad FASTA Mar del Plata Argentina

La Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA, incluye en su oferta académica la carrera de Licenciatura en Criminalística, cuyos objetivos principales son:

- Formar profesionales con capacidad de intervenir en la investigación criminal, basándose en los principios básicos de ética profesional y de la disciplina Criminalística.
- Colaborar en auxilio de las entidades judiciales locales, provinciales y nacionales, tanto en fueros penales como civiles así como a consultoras, aseguradoras, etc., y en la representación de particulares.
- Desarrollar la capacidad de razonar e identificar el caso que se presenta a examen para reconstruir la secuencia de la comisión del hecho delictual, a partir de los fundamentos de la medicina, la física, la química aplicada y la matemática.

El plan de estudios tiene una carga horaria de 2625 horas reloj y su Título Terminal es *Licenciado en Criminalistica* y Título Intermedio es *Técnico Universitario en Criminalística*. Comprende conocimientos en materias de ciencias exactas, biomédicas, humanísticas y el dominio de las tecnologías más modernas de aplicación. El Licenciado en Criminalística graduado de la Universidad FASTA está capacitado para:

- Ejercer funciones de perito como auxiliar de la Justicia Nacional y Provincial, fueros civiles y comerciales, Laboral, Penal (Criminal, Correccional y Contravencional); Administrativo y de Familia.
- Realizar Peritaciones extrajudiciales y consultorías técnicas.
- Desarrollar actividades en todo organismo donde se requiera verificar la autenticidad de documentación, sellos, firmas, etc.
- Practicar reconocimiento e identificación de huellas humanas y animales.
- Emplear los conocimientos de Papiloscopía para la determinación de la

relación madre e hijo en Clínicas y Hospitales en los recién nacidos.

- Participar en los asuntos concernientes a la Balística en los hechos en los que se utilizan armas de fuego.
- Colaborar en el esclarecimiento de los hechos de tránsito en cuanto a su origen, desarrollo y fases finales determinando las causas y consecuencias.
- Elaborar informes técnicos conteniendo cálculos estadísticos de lugares de conflicto y/o de la variable que se estudie.
- Determinar los componentes de las sustancias químicas mediante distintos métodos de separación para su posterior identificación y cuantificación.
- Brindar asesoramiento en cada una de las ramas nombradas en forma particular tendiente a esclarecer la producción de un presunto hecho delictuoso.
- Efectuar peritajes tendientes a la identificación de personas y elementos involucrados en un delito, utilizando los pilares de la Criminalística, los principios éticos que se transmiten en el período de enseñanza y, la verdad, herramienta principal plasmada en toda conclusión a la que se arriba tras cada intervención.
- Realizar estudios, informes, asesoramiento e investigaciones referidas a la prevención del delito.

Además, quienes se forman en esta disciplina en la Universidad alcanza una adecuada *formación práctica,* dado que participan intensa y frecuentemente en talleres y trabajos de campo, para lo cual se cuenta con distintos gabinetes forenses propios de la unidad académica y otros pertenecientes a instituciones con las que la Universidad ha celebrado convenios específicos para esos fines. Todo ello brinda al alumno la capacidad de razonar, reconocer y establecer las evidencias del caso que se presenta a examen para luego, mediante su aplicación específica, reconstruir las secuencias de la comisión del hecho, procurando la identidad del autor o de los autores, como así también establecer las bases e indicios pertinentes que posibiliten el esclarecimiento total del hecho.

Dra. María Paula Giaccaglia. Decana
Decana Facultad de Ciencias Jurídicas y Sociales
Universidad FASTA
decano.juridicas@ufasta.edu.ar

Presentación Maestría en Derecho Penal de la Universidad Libre Seccional Cali

Bajo la perspectiva del Sistema Penal Acusatorio, la administración de justicia penal colombiana debe hacer efectivos entre otros principios, el de verdad, reparación, ejercicio de las garantías del procesado y de la víctima; ello precisa de una respuesta de las instituciones involucradas en la investigación criminal, con lo que se busca lograr, la prevalencia de la justicia material - que es uno de los objetivos del Estado Social y Democrático de Derecho. El ejercicio de la acción penal en el SPA[1] ha evidenciado, para los operadores judiciales y sujetos procesales en todo el país, algunos retos y problemas derivados del uso de nuevas tecnologías y de las nuevas necesidades sociales que se precisa proteger, nuevos procedimientos y métodos, protocolos de investigación y nuevas pruebas. En ese contexto, la tecnología y la informática en el debate jurídico procesal plantea una nueva visión del proceso judicial, distinta de la visión tradicional – incluso la informática jurídica tradicional, limitada a equipos de cómputo personal y de protocolos de búsquedas de rastros digitales, en procesados individuales, ha sido superada por una redimensión de las tecnología y los sistemas de información que impacta la vida social y enfrenta a la ciencia forense a incesantes panoramas, tales como el peligro de obsolescencia, conflictos de resistencia al cambio tecnológico, la integralidad y multidisciplinariedad de los datos que se procesan a velocidades vertiginosas, la eficiencia en el desempeño de laboratorios de informática forense, la formación de redes de cooperación en informática forense, la creación de bases de conocimiento, los macrodatos y en particular las exigencias en materia de observancia de protocolos y normativas legales.

Con el propósito de generar espacios de investigación y de adquisición y difusión de nuevos conocimientos, se presentan los capítulos *la tecnología de la informática en el debate procesal y el tratamiento de los delitos informáticos en Colombia*, que constituyen resultados de investigación del Proyecto: *Visión analítica del Derecho Penal y de la Jurisprudencia Penal Colombiana*, del Grupo de investigación: *Criminalística Y Ciencias Forenses*[2], una obra que recoge el trabajo investigativo de Estudiantes del Semillero: *Instituciones Jurídico Penales*, [3] en nivel pregrado de la

1 Sistema Penal Acusatorio

2 Categoría A1 Colciencias Convocatoria 2018.

3 Grupo de Investigación: Criminalística y Ciencias Forenses.

Facultad de Derecho, Ciencias Políticas y Sociales y de posgrado de la Maestría en Derecho Penal de la Universidad Libre Seccional Cali.

Los trabajos presentados afrontan, desde la perspectiva académica, las profundas transformaciones sociales que marcan un derrotero en la Universidad Libre, en el proceso de formación en ciencias jurídicas – en especial en áreas de la criminalística y las ciencias forenses, de la región del suroccidente colombiano, en la que destaca en los procesos de construcción permanente del conocimiento científico, con el continuo fortalecimiento de una cultura investigativa, orientada formar líderes en la solución de problemáticas sociales, políticos y culturales.

El capítulo *La Tecnología y la Informática en el Debate Jurídico Procesal*, propone un análisis de la mensajería instantánea como un nuevo medio de prueba, en consideración a que las condiciones sociales y globales evidencian que la información que circula a través de mensajes instantáneos, contenedores de datos, fotos, conversaciones y videos, son instrumentos utilizados para la comisión de delito; la reflexión que se presenta, aborda la perspectiva del redimensionamiento de la prueba – de componente en tecnología e informática, en el debate probatorio procesal en Colombia. La importancia del estudio radica en que la mensajería instantánea como nuevo medio probatorio, pocas veces ha sido estudiado y ello influye negativamente en su aplicación dentro de los procesos jurisdiccionales.

Es una investigación teórica, descriptiva y bibliográfica, pues analiza el desarrollo social y jurídico de la mensajería como nuevo medio de prueba dentro del panorama probatorio y procesal de Colombia, denotando por medio de las diversas decisiones judiciales y la doctrina, el uso y desuso que se correlaciona a la valoración de esta clase de pruebas. Todo lo anterior bajo el criterio legislativo que establece el Código General del Proceso y el Código de Procedimiento Penal Colombiano en referencia a las pruebas y el procedimiento que se debe seguir para que estas sean tenidas en consideración.

En general, los delitos informáticos y con ellos, la incidencia, impacto y manejo de la prueba informática, plantea un escenario que, en el siglo XXI, constituye uno de los mayores retos que la sociedad debe afrontar, porque se trata en primer lugar de un ambiente desafiante y, en segundo lugar, por su vertiginosa mutación. A la par de los nuevos avances tecnológicos y sus amplios espectros de difusión, surgen con similar rapidez y complejidad, fenómenos criminales, que distan mucho de las formas tradicionales de delincuencia; los delitos contra el patrimonio económico, conductas que representan los índices más altos de criminalidad legal en Colombia (Nacion, 2019), ha migrado del modus operandi del asalto o sustracción de bienes muebles, propiciado por la oportunidad o descuido de la víctima, por sofisticados protocolos de sustracción en línea de bienes, cantidades de dinero y otros valores, de impacto y afectación masiva. Ahora el riesgo de la víctima del hurto, no se afronta

por exhibir bienes o dinero y en el caso de la estafa, por sucumbir ante el engaño y la maniobra fraudulenta bajo un convencimiento propiciado por el estafador y de entregar confiadamente bienes, sino por el ingenio y conocimiento, en muchas de las oportunidades, del criminal que aprovecha cualquier información que la red le brinde para agotar la conducta y trasladar bienes y dinero entre cuentas o lograr transferencias bajo promesas sustentadas en el fraude.

Es así que en el capítulo *El Tratamiento de los Delitos Electrónicos en Colombia. El Delito de estafa electrónica y su Modus Operandi"*, se presenta una valiosa aproximación, al concepto de delito informático y posteriormente en forma específica la estafa electrónica en la legislación colombiana; y para ello es conveniente advertir que, los avances de las tecnologías de la información y la comunicación (TIC.) y el acceso a ellas, por la mayoría de las personas en cada Estado o comunidades, los seres humanos enfrentamos en el universo de las relaciones e interacciones, una mayor interdependencia. En consecuencia, en los actos o negocios jurídicos que están mediados por dichas tecnologías, se empezaron a presentar acciones al margen de la ética, la moral, las buenas costumbres y de la ley, en detrimento patrimonial y moral de determinadas personas con la utilización de las herramientas expresadas, situación que es observada en cada Estado, comunidad o pueblo, lo cual ha servido de fundamento para que en cada Estado aborde el problema en cuestión; y con el acceso a dichas tecnologías, en el contexto internacional, se inició la tarea de elevar el rango de delitos informáticos a determinadas conductas en la utilización de las TIC., que fueren atentatorias con el patrimonio económico contra la vida, honra y bienes de las personas.

En Colombia desde hace no más de dos décadas que se viene prestando la debida atención al problema en cuestión, lo cual da origen al establecimiento de los delitos informáticos vigentes, destinados a la protección de la vida, honra y bienes de los colombianos: entre ellos, el denominado delito informático de estafa. Se pretende con este análisis dar respuesta acerca del interrogante ¿cuáles son las instituciones jurídicas que regulan el delito informático en la legislación Penal de Colombia y cuál es el modus operandi de la estafa electrónica?

El objetivo propuesto se orientó a realizar un abordaje descriptivo del tipo penal y los ingredientes de este; así como del marco normativo de las conductas penales que involucran componentes tecnológicos en su agotamiento. En el cuerpo central del trabajo, se analiza el modus operandi de la conducta, con lo que se busca entregar elementos para revelar aspectos no tratados en la literatura penal conocida, sobre las dinámicas criminales de los delitos informáticos, en especial los que atentan contra el patrimonio económico, y la concreta conducta del delito de estafa, tipo penal que brinda componentes útiles para el análisis por la frecuencia y diversidad que el modus operandi ha evidenciado.

Luego, teniendo como referente el problema planteado en la presente investigación, se presenta una interpretación de las factores asociados a dicho problema, que generan dificultades para los operadores judiciales en las investigaciones penales, por defraudaciones patrimoniales contra personas naturales y jurídicas, por medio de manipulaciones informáticas, cuyas conductas atentatorias contra el patrimonio económico de las personas, algunas de las cuales podrían quedar impunes por circunstancias relacionadas con aspectos normativos o procesales.

La metodología empleada en el análisis de fuentes documentales, indirectas, aplicó los métodos explicativo, descriptivo y propositivo, procurando el enriquecimiento, integración y retroalimentación de los mismos, para lograr articular sus objetivos, interrogantes y demás aspectos, por lo que se presenta un relevante resultado del análisis de la problemática que el delito informático plantea en la actualidad.

Lilia Cortes Monsalve
lilia.cortes@unilibre.edu.co
Docente Universidad Libre
Coordinadora Maestría en Derecho Penal

1 Análisis de Registros Fílmicos en Accidentes de Tránsito

Autores:
Lucía Belén Algieri
Licenciada en Criminalística
Universidad FASTA,
luciaalgieri@ufasta.edu.ar

Enzo Ezequiel Cecchetti
Licenciado en Criminalística; Universidad FASTA,
enzo.cecchetti@hotmail.com

Resumen

La ciudad de Mar del Plata, en Argentina, con alrededor de 800.000 habitantes estables, presenta una alta tasa de accidentes de tránsito, en relación a la media del país. Según los informes del Observatorio de Vial de la Municipalidad de General Pueyrredón, en 2018 la ciudad presentó un total de 1739 accidentes viales con lesionados y víctimas fatales, lo que equivale a 216 accidentes cada 100.000 habitantes, mientras que el promedio del país ronda en 176 cada 100.000 hab.

Debido a diferentes factores, ya sea las condiciones climatológicas, cuestiones mecánicas, o alteración de la escena, entre otros, en ocasiones los peritos accidentológicos se ven imposibilitados de determinar la velocidad de los vehículos intervinientes en un siniestro. La determinación de la velocidad actualmente se calcula en función de las huellas que deja el neumático al realizar una maniobra de freno, sin embargo, la implementación de los frenos ABS evitan el bloqueo del neumático, por lo tanto ya no dejan impresa ésta huella, por lo que el método tradicional con el tiempo caería en desuso.

Por otro lado, la Municipalidad de General Pueyrredón cuenta con un Centro de Operaciones y Monitoreo (COM-MGP) que tiene distribuidas en toda la ciudad alrededor de 1130 cámaras de seguridad públicas, a las que es posible sumar las aportadas por los particulares. Todos estos registros fílmicos son factibles de ser utilizados como evidencia en la resolución de un caso judicial.

Se presenta en este trabajo un estudio realizado en el que se empleó un método con el fin de probar la posibilidad de utilizar los registros fílmicos de las cámaras de seguridad para estimar la velocidad de los vehículos.

Este análisis parte de identificar puntos de referencia en el lugar del hecho, los cuales son inmutables en el tiempo. Luego, a partir de la toma de las distancias entre estos puntos identificados, y el dato de la velocidad de filmación, que se mide en FPS (frames por segundo), obtener el tiempo de recorrido entre los puntos, para finalmente obtener la velocidad de los vehículos implicados. La ventaja del uso de este método es que sortea la dificultad de realizar otro tipo de cálculo cuando no se tienen indicios físicos en el lugar del hecho.

Finalmente, luego del análisis realizado, se pudo concluir que el método utilizado es posible, con un porcentaje de error conocido y estable para el cálculo de velocidad de un vehículo, independientemente de la situación lumínica y climática del lugar del hecho.

Palabras clave: Accidentes de tránsito, Análisis de Video Digital, Velocidad Vehicular, Análisis Forense

Abstract

The city of Mar del Plata, Argentina, with a population of around 800.000, has a high traffic accident rate in relation to the country's average. According to the Vial Observatory's Report of the local governments, in the year 2018, there was 1739 road accidents, what represents 216 incidents for every 100.000 people.

Due to different factors: weather conditions, scene alterations, mechanical issues, among others, the road traffic accidents experts may not be able to determine the real speed of the vehicles involved in the case. Currently, the speed is calculated by skid marks left on the road in a braking maneuver. However, with the ABS brake, this trace longer appears, so this method will fall into disuse.

In addition, the local government has an Operating and Monitoring Centre, called COM, which manages around 1130 public security cameras along the city. This number of cameras is incremented with private ones that can be presented by individual citizens. All these films can be used as digital evidence in a judicial case.

This paper presents the results of a study in which we used a method to estimate vehicle speed by the use of digital video. The method begins with the identification of immutable reference points in the incident scene. Then, with the measure of the distance between the points, and the film frame rate (Frames Per Second), is possible

to get the travel time between the points, and finally, the vehicle speed. This method has the advantage that it doesn't need physical evidence in the scene.

Finally, after the analysis was made, it could be concluded that the method is feasible to use to calculate the vehicle's speed, because it has a known percent and stable error, regardless of the scenes's lightning or climatic situations.

Keywords: Traffic Accident, Digital Video Analysis, vehicle speed, Forensic Analysis

1.1 Introducción

En el año 2018, en Argentina, ocurrieron 81.592 siniestros viales. Este número total incluye los siniestros simples, es decir, todo aquel siniestro en el que no hay lesionados; siniestros con heridos; siniestros con víctimas fatales[4] y aquellos sin especificar. El saldo de estos siniestros fueron 5.472 víctimas fatales y 64.816 lesionados. [5] En este mismo período, en el partido de General Pueyrredón, ubicado al sur de la provincia de Buenos Aires, cuya ciudad cabecera es Mar del Plata, con una población estable de aproximadamente 800.000 habitantes ocurrieron 1.739 siniestros viales[6] con consecuencias lesivas o fatales.

Este trabajo propone realizar aportes desde las nuevas tecnologías a la criminalística y ciencias forenses, en particular a la accidentología vial, a partir del desarrollo y aplicación de un método de determinación de velocidad vehicular mediante el uso de la velocidad de filmación (Frames Por Segundo) del registro fílmico de cámaras de seguridad aportados por el COM-MGP.

Este Centro de Operaciones y Monitoreo comenzó a funcionar el 12 de Julio del 2012 y en la actualidad cuenta con 1.131 cámara (de tipo Domo y fijas), que se encuentran a disponibilidad de requerimientos judiciales o por demanda espontánea por parte de los particulares. Toda la información recabada por estas en la ciudad, es almacenada en un servidor dedicado con una duración máxima de 1 año.

---

4 El cómputo de víctimas fatales por siniestros viales, se realiza considerando aquellas que fallecen hasta los treinta (30) días de ocurrido el siniestro, siguiendo el criterio de armonización global establecido por la Organización Mundial de la SAlud (OMS) y son considerados tanto los siniestros ocurridos en la ciudad como rutas de jurisdicción provincial y nacional.

5 Datos oficiales del Ministerio de Transporte, Presidencia de la Nación. Argentina.

6 Datos oficiales del Observatorio vial, Municipalidad de General Pueyrredón, provincia de Buenos Aires. Argentina.

1.2 Registros fílmicos de Cámaras de Vigilancia

Un sistema de Seguridad es un conjunto de dispositivos e instalaciones destinados a prevenir y controlar riesgos con el fin de proporcionar protección a las personas y bienes materiales como así también minimizar pérdidas ante incidentes de inseguridad: robo, fraude, agresión, entre otros; y siniestros: incendios, fenómenos climatológicos, interrupción de suministro eléctrico, entre otros. Estos sistemas de seguridad, que se basan en gestión de video, detección y extinción de incendio, alarmas, pararrayos, UPS, entre otros, tienen la misión de detectar, ubicar y actuar automáticamente ante un riesgo, ya sea para suprimir o disminuirlo.

Los Sistemas de Gestión de Vídeo denominados usualmente CCTV (circuito cerrado de televisión) son sistemas de seguridad que permiten, por medio de imágenes, monitorear áreas en forma remota.

Estos sistemas están constituidos por dispositivos para captura de imágenes, de visualización, de control, de grabación, de procesamiento, de almacenamiento y el software que permite la acción de observación en tiempo real al mismo tiempo que registra la evidencia como soporte y facilita el procesamiento para su análisis en etapas posteriores.

Actualmente, los sistemas de seguridad por video ya no son un dispositivo reservado sólo para las empresas de seguridad. Muchos ciudadanos poseen estos sistemas instalados en sus domicilios particulares, edificios o comercios. Existen dos tipos principales de cámaras de vigilancia:

- *Cámaras analógicas:* Se utilizan principalmente en los CCTV (Circuito Cerrado de Televisión). Estas cámaras se conectan por un cable coaxial enviando una señal de corriente alterna, que varía en el tiempo con diferente amplitud, a un televisor o un monitor, donde las imágenes se visualizan. Asimismo, envían flujos continuos de datos (barrido) a un dispositivo de almacenamiento (DVR - registrador digital). Los DVR Stand Alone, son los encargados de convertir la imagen analógica en digital. De esta manera, es posible acceder a los videos digitales de éstas cámaras siempre que el sistema de cámaras de analógico se encuentra conectado a un DVR.

- *Cámaras Digitales:* Son aquellas que emiten un *stream* de video digital, que puede almacenarse en un archivo o enviarse mediante una conexión de red a un servidor.

Las imágenes pueden ser registradas y consultadas en tiempo real desde un dispositivo conectado al software correspondiente.

La tecnología de los siguientes elementos determinará la *calidad y resolución de la imagen*:

- *Sensor:* La calidad de resolución de la imagen depende principalmente del sensor con la que esté equipada, la tecnología de fabricación del mismo, y el tamaño de los elementos fotosensibles.

- *Objetivo:* El objetivo es la parte de la cámara que dirige los rayos de luz hacia el sensor. Consta de una o varias lentes de forma convexa que proyecta los rayos de luz que lo atraviesan en un punto llamado foco. Con él ajustamos la distancia focal (zoom) y el enfoque. La calidad de fabricación de los lentes es determinante para proyectar una buena imagen en el sensor.

Dependiendo del tipo de cámara y características, las grabaciones que resulten pueden variar su velocidad de filmación en cantidad de FPS[7].

1.2.1 Accidentes de Tránsito

Se puede definir a la Accidentología Vial como la rama de la criminalística y ciencias forenses que tiene por objeto de estudio el accidente de tránsito terrestre, y por finalidad la determinación de las circunstancias, condiciones y resultados de dicho suceso, así como también elaborar y coordinar programas de prevención y educación en base a problemáticas específicas.

Un accidente de tránsito es todo aquel suceso que ocurre en la vía pública o privada donde interviene al menos un vehículo en movimiento y que produce daños en las cosas y/o lesiones en las personas. Técnicamente, es una situación dinámica que implica una serie de acontecimientos que culminan en el hecho. Cada una de ellas es y debe ser estudiada primero por separado y luego en conjunto, no sólo para entender cómo sucedió el accidente, sino también para prevenir futuros accidentes.

El accidente de tránsito es el resultado final de un proceso en el que se encadenan diversos eventos, condiciones y conductas. Los factores que desembocan en un accidente, que produce un daño material al vehículo, y/o físico y anímico al conductor, surgen dentro de la compleja red de interacciones entre el conductor, el vehículo y la vía en unas determinadas condiciones ambientales. Estas causas, a los fines de estudio e investigación, son agrupadas en tres grupos o categorías, conformando lo que se denomina "triángulo accidentológico" o "triada accidentológica".

---

7 Se refiere al número de cuadros o fotogramas por segundo al cual se muestra o graba el video, es decir la velocidad (tasa) a la cual un dispositivo la capta. El término se aplica igualmente a películas y cámaras de video, gráficos computacionales y sistemas de captura de movimiento. Es decir que si una cámara que captura a 60fps el video está compuesto por 60 "fotos" por unidad de tiempo.

Por lo tanto, las causas de estos siniestros habrán de deducirse en función de los elementos de tránsito o de los elementos del accidente que en este análisis son tres: el hombre; el medio ambiente (incluyendo la vía) y el vehículo. Actualmente, para realizar los cálculos de velocidades, se utilizan los indicios físicos del lugar del hecho, principalmente las huellas de frenado que quedan impresas en el pavimento.

El freno consiste en la aplicación de una superficie fija sobre una giratoria. El rozamiento contiene el giro de la parte móvil, convirtiéndose la energía absorbida en calor, el cual se disipa por radiación a la atmósfera. La finalidad del freno es "retener" y "parar" el vehículo. Todo sistema de frenos debe cumplir con los siguientes requisitos:

- *Eficacia:* Con un esfuerzo mínimo sobre el pedal, en un tiempo y distancia mínima.
- *Estabilidad*: El vehículo debe conservar su trayectoria sin derrapes, desvíos ni reacciones en el volante.
- *Comodidad:* Recorrido y accionamiento progresivo y razonable del pedal. El sistema de frenos se dispone de manera tal que actúen más intensamente en las ruedas delanteras. Si un exceso de frenado bloquea la rueda, el neumático se desplazará sobre la superficie y la adherencia entre éstos será considerablemente menor, lo que generará una pérdida de control.

El cálculo de la velocidad utilizando las huellas de frenado ha estado perdiendo utilidad y confiabilidad debido al advenimiento de los frenos con tecnología ABS (Anti-lock Brake System).

El dispositivo ABS tiene sensores que se comunican con un sistema electrónico y hace variar la fuerza de frenado para evitar que los neumáticos se bloqueen y se deslicen sobre el suelo. El uso de estos frenos se ha tornado una medida obligatoria, en Argentina, para todos aquellos vehículos que salieron al mercado a partir del año 2014.[8]

8 Sancionada en el año 2008, la ley 26.363 - Ley de Tránsito y Seguridad Vial -dispone la creación de la Agencia Nacional de Seguridad Vial. En el art 29 de dicha ley se establece la obligatoriedad de incorporación en todos los automóviles 0 km de doble bolsa de aire para amortiguación de impactos (airbags) y sistema de antibloqueo de neumáticos (ABS) Normativa disponible en https://www.argentina.gob.ar/seguridadvial/normativa 9 Ésta experimentación se realizó con un vehículo Peugeot 208 circulando una velocidad conocida por la intersección de la Avenida Juan José Paso y la calle Santiago del Estero en la localidad de Mar del Plata. Dicha intersección cuenta con una cámara de monitoreo municipal. La circulación del vehículo fue realizada teniendo en cuenta las medidas de seguridad pertinentes y la velocidad enmarcada en lo que establece el art. 51 de la ley 24.449 (ley de tránsito).

Este trabajo presenta la posibilidad de utilizar otro método de cálculo de la velocidad de un vehículo en un siniestro, basado en el registro fílmico de las cámaras de seguridad de índole pública o privada.

1.3 Metodología

El trabajo parte de la recolección de información de las cámaras de seguridad que captan el movimiento automotor de un accidente de tránsito. Se utilizaron un total de siete videos provenientes del COM-MGP, tres de los cuales corresponden a accidentes de tránsito y los cuatro restantes corresponden a registros fílmicos de las cámaras de seguridad de una experimentación realizada con vehículo circulando a una velocidad conocida[9].

El método propuesto sigue los pasos que se detallan a continuación:

1. Se consiguieron las videograbaciones provenientes del COM-MGP y los fotogramas diurnos de los diversos sitios donde sucedieron los accidentes de tránsito.
2. El equipo se dirige a las ubicaciones de los accidentes con el fin de seleccionar y tomar las distancias de los puntos de referencias fijos, que serán utilizados luego en los cálculos.
3. Se obtiene información de la velocidad de grabación de los registros fílmicos.
4. Se realiza un estudio de la información obtenida en los puntos anteriores calculando las medidas correspondientes para la obtención de la velocidad de los vehículos automotores implicados en cada video.

Los *registros fílmicos* permiten:

- Determinar de los cuadros por segundo (FPS) de las cámaras de seguridad.
- Analizar la luminosidad ambiental de la filmación.
- Estimar la velocidad vehicular.

Se consideran las siguientes *variables de investigación* respecto al método propuesto:

- Ambiental: Se aplica el método propuesto utilizando material fílmico de accidentes de tránsito en dos condiciones ambientales: asfalto húmedo y asfalto seco.
- Luminosidad: Se aplica el método propuesto utilizando material fílmico de accidentes de tránsito de ocurrencia en horas diurnas y en horas nocturnas.

Se utilizan los siguientes i*nstrumentos* para la recolección de datos:

- Cinta métrica.
- Cámara digital para documentar fotográficamente lugar del siniestro.
- Cámara marca GoPro modelo Hero2 para almacenar los registros fílmicos en verificación de velocidad con circulación conocida.
- GPS marca Garmin modelo Nuvi 200.

En el *cálculo de distancias* se utiliza el siguiente método:

Primero se establecen *puntos de referencia* inamovibles del lugar de la medición, tanto en los extremos como intermedios. Se mide y registra la distancia entre esos puntos y se determina la distancia total. Posteriormente, se proyectan líneas paralelas sobre los puntos de referencia marcados, con el fin de obtener una plantilla de la zona.

Una vez obtenidas todas las distancias se procede a calcular el tiempo que insume el vehículo en recorrer estas distancias.

Si el registro fílmico en análisis corresponde a un accidente acaecido en horario nocturno, es importante contar con un material de la misma cámara con imágenes diurnas, con el fin de visualizar los puntos de referencia y así marcar la plantilla para montarla en el video original. Para *obtener el tiempo* en el que un vehículo recorre una determinada distancia se contabilizan la cantidad de fotogramas insumidos, y se lo divide por la velocidad de grabación, esto es: la cantidad de fotogramas por segundo- FPS- a los que graba la cámara correspondiente. El valor obtenido estará en segundos.

Conocidos *la distancia y el tiempo* es posible calcular la *velocidad del vehículo* con la siguiente fórmula:

$$v = \frac{x_f - x_i}{t}$$

- V: Representa la velocidad desarrollada por el vehículo.
- (xf- xi): Representa la distancia recorrida entre dos puntos definidos.
- t: Representa el tiempo insumido para recorrer dicha distancia.

1.4 Estudio de Casos

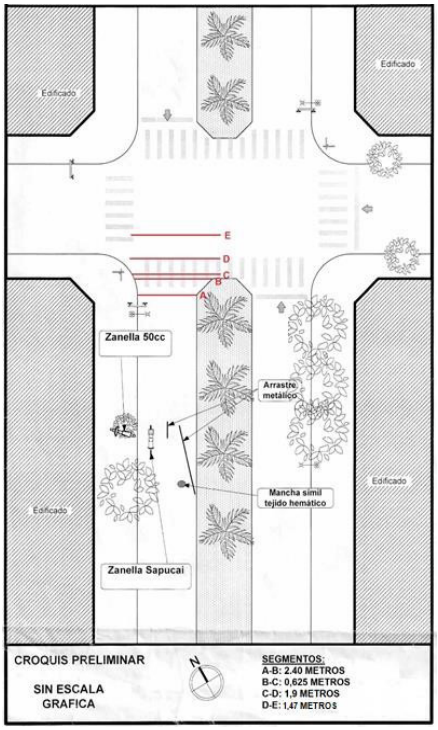
1.4.1 Caso 1 - nocturno y buenas condiciones ambientales

Se recibe un video de una cámara de seguridad perteneciente al COM-MGP en la cual se registra un accidente de tránsito en el que intervienen dos motovehículos en horas de la noche con buenas condiciones climáticas.

A continuación, se toma vista del registro fílmico y se contrasta con un fotograma diurno del mismo espacio, con el fin de identificar posibles puntos de referencia fijos para el cálculo de velocidad.

El equipo se dirige a la intersección correspondiente dónde se corroboraron los puntos de referencia fijos observados previamente, y se establece uno de ellos como el *punto de referencia inicial* y por consecuente distancia 0. Luego se mide la distancia entre los restantes puntos desde el punto de referencia inicial, materializando así la planimetría del hecho, tal como se muestra en la Figura 1. Es importante considerar que en cada figura mostrada en este trabajo los puntos de referencia se marcan con letras del alfabeto, y las paralelas son sus proyectadas.

Figura 1. Planimetría del lugar del hecho con los puntos de referencia identificados mediante líneas paralelas y señalización alfabética.



A continuación, utilizando un software de edición de video se realiza una plantilla proyectando las líneas paralelas fijadas a partir de los puntos de referencia fijos del lugar del siniestro.

Figura 2. Fotografía del lugar del hecho con los puntos de referencia marcados con líneas paralelas.

Posteriormente, se superponen las líneas paralelas con la referencia alfabética sobre el video original y se genera un nuevo video con dicha incorporación, respetando la velocidad de grabación - FPS, del registro fílmico original.

Figura 3. Fotograma del video con la plantilla que marca los puntos de referencia.

Cálculo de distancias:

Realizadas las mediciones correspondientes en el lugar se obtuvieron los siguientes resultados:

1. Distancia entre Puntos A y B: 2.40 metros
2. Distancia entre Puntos B y C: 0.625 metros
3. Distancia entre Puntos C y D: 1.9 metros
4. Distancia entre Puntos D y E: 1.47 metros

Distancia total entre A y E: 6.395 metros

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

5. Fotogramas insumidos en recorrer la distancia entre Puntos A y B: 3
6. Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 2

7. Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 3
8. Fotogramas insumidos en recorrer la distancia entre Puntos D y E: 2

Fotogramas totales insumidos entre A y E: 10 fotogramas

Fotogramas por segundo a los que graba la cámara 18 fotogramas

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia entre el punto A y el punto D, con la siguiente regla.

18 fotogramas ---------- 1 segundo

10 fotogramas ---------- *x= 0.555 segundos*

Utilizando los datos obtenidos en el cálculo de velocidad: Velocidad= Distancia/Tiempo, se obtiene el siguiente resultado.

$$v = \frac{X}{t}$$

$$v = \frac{6.395\ m}{0.555\ seg}$$

$$\boldsymbol{v = 11.511\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{11.511\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \boldsymbol{41.43\ Km/H}$$

La Unidad Fiscal de Instrucción nº 11 que tomó intervención en este caso no solicitó pericia accidentológica para el cálculo de velocidad debido a que el imputado fue condenado teniendo en cuenta otros aspectos tales como el cruce de la intersección con semáforo en rojo, sumado a pericias químicas que determinaron alcohol en sangre, entre otros.

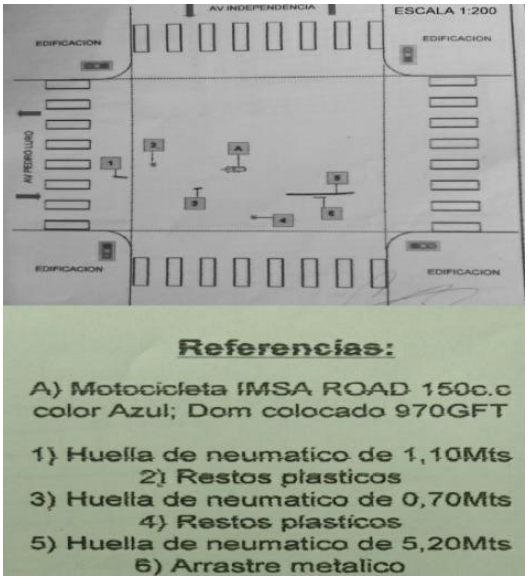
1.4.2 Caso 2 - diurno y buenas condiciones ambientales

Se recibe un video de una cámara de seguridad perteneciente al COM-MGP en la cual se registra un siniestro vial en el que un motovehículo impacta con un peatón en la intersección de dos avenidas en horas de la tarde con buenas condiciones climáticas.

Se toma vista del registro fílmico y se contrasta con fotograma diurno del mismo espacio, con el fin de identificar posibles puntos de referencia fijos para el cálculo de velocidad.

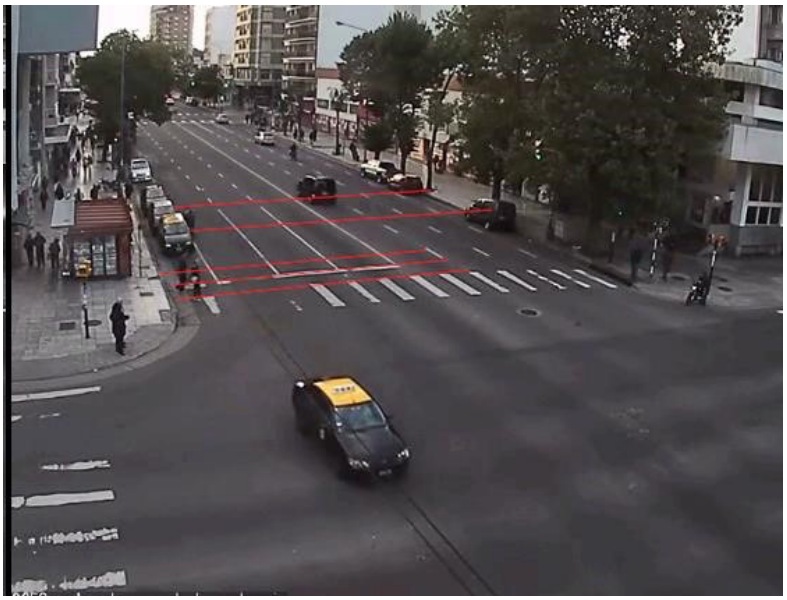
El equipo se dirige a la intersección correspondiente dónde se corroboraron los puntos de referencia fijos observados previamente, y se establece uno de ellos como el *punto de referencia inicial* y por consecuente distancia 0. A continuación se mide la distancia entre los restantes puntos desde el punto de referencia inicial, materializando así la planimetría del hecho que se muestra en la Figura 4.

Figura 4. Planimetría del lugar del hecho con sus respectivas referencias.



Utilizando un software de edición de video se realiza una plantilla proyectando las líneas paralelas a partir de los puntos de referencia fijos del lugar del accidente de tránsito.

Figura 5. Fotografía del lugar del hecho captada con la cámara de seguridad con los puntos de referencia señalados con líneas paralelas.



Posteriormente, se superponen las líneas paralelas con la referencia alfabética sobre el video original y se genera un nuevo video con dicha incorporación, respetando la velocidad de grabación - FPS, del registro fílmico original.

Cálculo de distancias:

Realizadas las mediciones correspondientes en el lugar se obtuvieron los siguientes resultados:

- Distancia entre Puntos A y B: 1.92 metros
- Distancia entre Puntos B y C: 3.20 metros
- Distancia entre Puntos C y D: 7.73 metros
- Distancia entre Puntos D y E: 8.78 metros

Distancia total: 21.63 metros

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

- Fotogramas insumidos en recorrer la distancia entre Puntos A y B: 2
- Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 2
- Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 9
- Fotogramas insumidos en recorrer la distancia entre Puntos D y E: 8

Fotogramas totales insumidos entre A y E: 21 fotogramas

Fotogramas por segundo a los que graba la cámara 18 fotogramas

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia entre el punto A y el punto E, con la siguiente regla:

18 fotogramas ---------- 1 segundo

21 fotogramas ---------- ***x= 1.1667 segundos***

Los datos obtenidos se reemplazan en el cálculo de velocidad:

$$v = \frac{X}{t}$$

$$v = \frac{21.63\ m}{1.16667\ seg}$$

$$\boldsymbol{v = 18.54\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{18.54\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \boldsymbol{66.74\ Km/H}$$

En la investigación penal de este caso intervino la Unidad Fiscal de Instrucción nº 11. La pericia accidentológica realizada por la Policía Científica de Mar del Plata, determinó una velocidad de 62 km/h aproximadamente. Dicha pericia fue realizada

a partir de los indicios físicos presentes en el lugar, particularmente mediante las huellas de frenado.

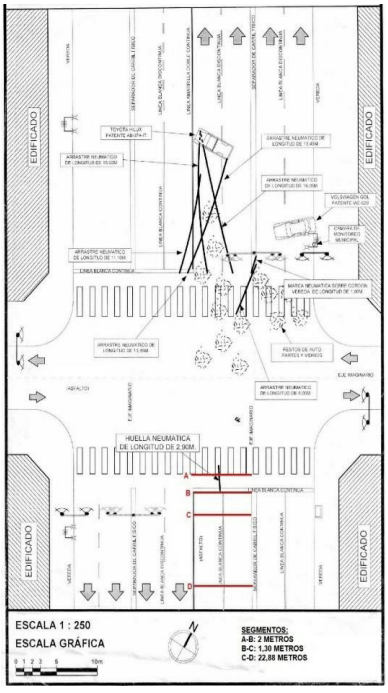
1.4.3 Caso 3 - nocturno y buenas condiciones ambientales

Se recibe un registro fílmico de una cámara de seguridad perteneciente al COM-MGP en la cual se registra un siniestro vial en el que intervienen dos automóviles en horas de la noche y con malas condiciones ambientales dado que el asfalto se encontraba húmedo producto de la lluvia.

Se toma vista del material y se contrasta con un fotograma diurno del mismo espacio, con el fin de identificar posibles puntos de referencia fijos para el cálculo de velocidad.

El equipo se dirige a la intersección correspondiente dónde se corroboraron los puntos de referencia fijos observados previamente, y se establece uno de ellos como el *punto de referencia inicial* y por consecuente distancia 0. A continuación, se miden las distancias entre los restantes puntos, desde el punto de referencia inicial, materializando así la planimetría del hecho que se muestra en Figura 6.

Figura 6. Planimetría del lugar del hecho con sus respectivas referencias.



Utilizando un software de edición de video se realiza una plantilla proyectando las líneas paralelas a partir de los puntos de referencia fijos del lugar del accidente de tránsito.

Figura 7. Fotografía del lugar del hecho con los puntos de referencia.

Posteriormente, se superponen las líneas paralelas con la referencia alfabética sobre el video original y se genera un nuevo video con dicha incorporación, respetando la velocidad de grabación - FPS, del registro fílmico original.

Figura 8. Fotograma del video original con la plantilla que señala los puntos de referencia

Cálculo de distancias:

Realizadas las mediciones correspondientes en el lugar se obtuvieron los siguientes resultados:

- Distancia entre Puntos B y C: 1.30 metros
- Distancia entre Puntos C y D: 22.88 metros

En este caso no la distancia entre los puntos A y B no se consideran, debido a que el impacto se produjo en el punto B, con la consecuente desaceleración del vehículo.

Distancia total recorrida: 24.18 metros

Una vez conocida la distancia total se procedió a realizar el conteo de fotogramas insumidos en estos puntos:

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

- Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 1
- Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 13

Fotogramas totales insumidos: 14

Fotogramas por segundo a los que graba la cámara: ***18 fotogramas***

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia entre el punto D y el punto B, con la siguiente regla:

18 fotogramas ---------- 1 segundo

4 fotogramas ---------- ***x= 0.778 segundos***

Los datos obtenidos se reemplazan en el cálculo de velocidad:

$$v = \frac{X}{t}$$

$$v = \frac{24.18\ m}{0.778\ seg}$$

$$\boldsymbol{v = 31.09\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{31.09\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \mathbf{111.92\ Km/H}$$

En la investigación penal de este caso intervino la Unidad Fiscal de Instrucción nº 11. Consultada esta UFI respecto a la pericia accidentológica de este caso, se informa que la misma no pudo ser realizada por la falta de indicios físicos en el lugar del hecho.

1.5 Verificación del Método

Finalizada la etapa investigativa se procede a realizar la verificación del método, con el objeto de conocer el margen de error de los cálculos realizados.

Para realizar este procedimiento, se utiliza el mismo método de cálculo, partiendo de la circulación a una velocidad conocida, y teniendo en cuenta las mismas variables: luminosidad y condiciones climáticas.

Se procedió a circular con un vehículo marca Peugeot modelo 208, el que fue equipado con una cámara GoPro modelo Hero 2 con el fin de registrar la velocidad de circulación mostrada por el tablero al momento de circular por la Avenida Juan José Paso intersección con calle Santiago del Estero, Mar del Plata, Buenos Aires, Argentina. En dicha intersección se encuentra situada una cámara de seguridad perteneciente al COM-MGP. Por otro lado, se procede a registrar al instante de cruce la velocidad detectada por el satélite, mediante un equipo GPS marca Garmin modelo Nuvi 200. Posteriormente fueron solicitadas al COM-MGP la remisión del material fílmico correspondiente.

Las cuatro experimentaciones realizadas se efectuaron en la misma ubicación y con el mismo vehículo, durante el mes de octubre del año 2018. A continuación, el equipo se dirigió a dicha intersección con el fin de realizar la planimetría del lugar, tal como se muestra en la Figura 9.

Determinados los puntos de referencia, se proceder a realizar las mediciones de las distancias existentes entre dichos puntos, obteniendo los siguientes valores:

- Distancia entre Puntos B y C: 2.02 metros
- Distancia entre Puntos C y D: 1.24 metros

- Distancia entre Puntos D y E: 1.60 metros
- Distancia entre Puntos E y F: 3.03 metros
- Distancia entre Puntos F y G: 7.83 metros

Distancia total: 15.72 metros

Figura 9. Planimetría del lugar con sus respectivas referencias.

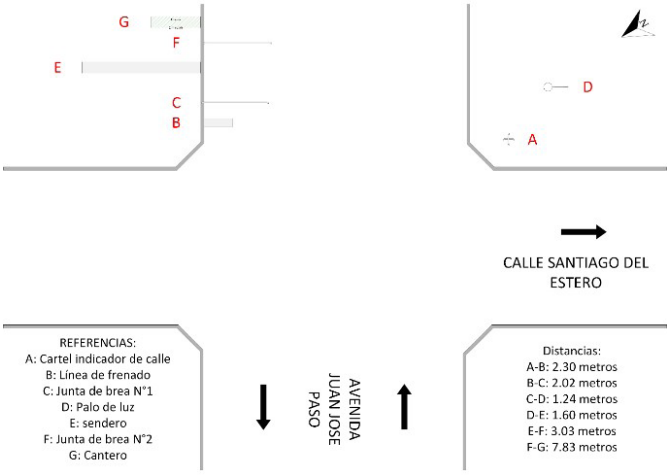
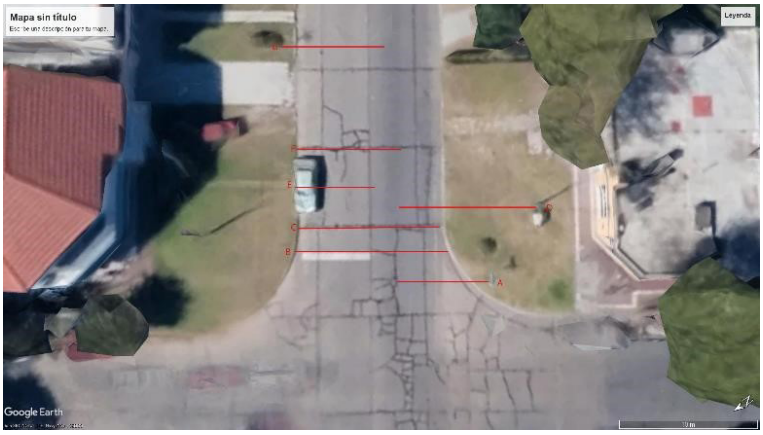


Figura 10. Fotografía del lugar captada desde GoogleEarth con los respectivos puntos de referencia.



1.5.1 Condición diurna sin precipitaciones

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados en el punto anterior se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 5

Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 3

Fotogramas insumidos en recorrer la distancia entre Puntos D y E: 8

Fotogramas insumidos en recorrer la distancia entre Puntos E y F: 5

Fotogramas insumidos en recorrer la distancia entre Puntos F y G: 26

Fotogramas totales insumidos: 47

Fotogramas por segundo a los que graba la cámara: 30

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia con la siguiente regla:

30 fotogramas ---------- 1 segundo

47 fotogramas ---------- ***x= 1.5667 segundos***

Los datos obtenidos se reemplazan en la fórmula de velocidad:

$$v = \frac{X}{t}$$

$$v = \frac{15.72\ m}{1.566\ seg}$$

$$\boldsymbol{v = 10.03\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{10.03\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \mathbf{36.12\ Km/H}$$

El tablero del vehículo indica una velocidad de circulación de 45 km/h, mientras que el marcador del GPS indica una velocidad de circulación de 42 km/h al momento de atravesar la intersección.

Se procede, entonces, a calcular el porcentaje de error entre la velocidad de GPS y la velocidad resultante del método, resultando para esta primera condición de luminosidad: diurno y ambiental: asfalto seco, un error del 14%.

Velocidad GPS – Velocidad Calculada = Diferencia de Velocidad

42 km/h – 36.12 km/h = Diferencia de Velocidad

5.88 km/h = Diferencia de Velocidad

42 Km/h ---------- 100%

5.88 Km/h ---------- **x= 14%**

1.5.2 Condición diurna con precipitaciones:

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

- Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 3
- Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 1

- Fotogramas insumidos en recorrer la distancia entre Puntos D y E: 5
- Fotogramas insumidos en recorrer la distancia entre Puntos E y F: 3
- Fotogramas insumidos en recorrer la distancia entre Puntos F y G: 16

Fotogramas totales insumidos: 28

Fotogramas por segundo a los que graba la cámara: 18

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia con la siguiente regla:

18 fotogramas ---------- 1 segundo

28 fotogramas ---------- ***x= 1.556 segundos***

Los datos obtenidos se reemplazan en la fórmula de velocidad:

$$v = \frac{X}{t}$$

$$v = \frac{15.72m}{1.556\ seg}$$

$$\boldsymbol{v = 10.11\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{10.11\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \boldsymbol{36.38\ Km/H}$$

El tablero del vehículo indica una velocidad de circulación de 45 km/h, mientras que el marcador del GPS indica una velocidad de 42 km/h al momento de atravesar la intersección.

Se procede, entonces, a calcular el porcentaje de error entre la velocidad de GPS y la velocidad resultante del método, resultando para ésta condición de luminosidad: diurna y ambiental: asfalto húmedo, un error de 13,38%.

Velocidad GPS – Velocidad Calculada	=	Diferencia de Velocidad
42 km/h – 36.38 km/h	=	Diferencia de Velocidad
5.88 km/h	**=**	**Diferencia de Velocidad**

42	Km/h ----------	100%
5.61	Km/h ----------	**x= 13.38%**

1.5.3 Condición nocturna sin precipitaciones:

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

- Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 3
- Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 3
- Fotogramas insumidos en recorrer la distancia entre Puntos D y E: 4
- Fotogramas insumidos en recorrer la distancia entre Puntos E y F: 4
- Fotogramas insumidos en recorrer la distancia entre Puntos F y G: 9

Fotogramas totales insumidos: 23 fotogramas

Fotogramas por segundo a los que graba la cámara: 14.53 fotogramas

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia entre los puntos con la siguiente regla:

14.53 fotogramas ---------- 1 segundo

23 fotogramas ---------- ***x= 1.58 segundos***

Los datos obtenidos son reemplazados en la fórmula de velocidad previamente enunciada:

$$v = \frac{X}{t}$$

$$v = \frac{15.72\ m}{1.58\ seg}$$

$$\boldsymbol{v = 9.93\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{9.93\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \boldsymbol{35.75\ Km/H}$$

El tablero del vehículo indica una velocidad de circulación de 44 km/h, mientras que el marcador del GPS indica una velocidad de 41 km/h al momento de atravesar la intersección.

Se procede, entonces, a calcular el porcentaje de error entre la velocidad de GPS y la velocidad resultante del método, resultando para ésta condición de luminosidad: nocturna y ambiental: asfalto seco, un error de 12,80%.

Velocidad GPS – Velocidad Calculada	=	Diferencia de Velocidad
41 km/h – 35.75 km/h	=	Diferencia de Velocidad
5.24 km/h	=	Diferencia de Velocidad

41 Km/h ---------- 100%

5.24 Km/h ---------- **x= 12.80%**

1.5.4 Condición nocturna con precipitaciones:

Cálculo de Tiempo:

Sobre cada uno de los puntos de referencias fijos identificados se contabiliza la cantidad de fotogramas que insume el vehículo correspondiente en recorrerlos.

- Fotogramas insumidos en recorrer la distancia entre Puntos B y C: 4
- Fotogramas insumidos en recorrer la distancia entre Puntos C y D: 2
- Fotogramas insumidos en recorrer la distancia entre Puntos D y E: 6
- Fotogramas insumidos en recorrer la distancia entre Puntos E y F: 4
- Fotogramas insumidos en recorrer la distancia entre Puntos F y G: 12

Fotogramas totales insumidos: 28 fotogramas

Fotogramas por segundo a los que graba la cámara: 18 fotogramas

Finalmente, es posible establecer el tiempo insumido en recorrer la distancia entre los puntos con la siguiente regla:

18 fotogramas ---------- 1 segundo

28 fotogramas ---------- ***x= 1.5556 segundos***

Los datos obtenidos son reemplazados en la fórmula de velocidad previamente enunciada:

$$v = \frac{X}{t}$$

$$v = \frac{15.72\ m}{1.5556\ seg}$$

$$\boldsymbol{v = 10.11\ m/s}$$

Dado que la velocidad está expresada en metros por segundo, se procede a convertir al sistema convencional de Km/h. Resultando:

$$\frac{10.11\ m}{1\ seg} \times \frac{3600\ seg}{1\ hora} \times \frac{1\ km}{1000\ m} = \mathbf{36.38\ Km/H}$$

El tablero del vehículo indica una velocidad de circulación de 45 km/h, mientras que el marcador del GPS indica una velocidad de 42 km/h al momento de atravesar la intersección.

Se procede, entonces, a calcular el porcentaje de error entre la velocidad de GPS y la velocidad resultante del método, resultando para ésta condición de luminosidad: nocturna y ambiental: asfalto húmedo, un error de 13,38%.

Velocidad GPS – Velocidad Calculada		=	Diferencia de Velocidad
42 km/h – 36.38 km/h		=	Diferencia de Velocidad
5.24 km/h		=	Diferencia de Velocidad
41	Km/h ----------	100%	
5.61	Km/h ----------	**x= 13.38%**	

1.6 Resultados

En la verificación del método implementado en los casos prácticos, se transitó a velocidades conocidas y se obtuvieron los siguientes resultados:

RESULTADOS DE LA EXPERIMENTACIÓN REALIZADA				
	Imágenes diurnas sin lluvia	Imágenes diurnas con lluvia	Imágenes nocturnas sin lluvia	Imagenes nocturnas con lluvia
Resultado siguiendo el método	36.12km/h	36.38 km/h	35.75 km/h	35.38 km/h
Tablero vehicular	45 km/h	45 km/h	44 km/h	45 km/h
Pantalla de GPS	42 km/h	42 km/h	41 km/h	42 km/h
Error	14%	13.38%	12.8 %	13.38 %
Promedio de error: 13.39%				

El promedio de error del método desarrollado, de acuerdo a la verificación realizada, es de 13.39%.

La interpretación de los hechos observados, permiten concluir que las grabaciones de cámaras de monitoreo en la vía pública, resultan un medio fehaciente para la determinación de las velocidades de circulación de vehículos en la vía pública.

Los informes técnicos de las empresas automotrices indican que el velocímetro con el que viene dotado cada vehículo, consiste en un instrumento orientativo de la velocidad desarrollada. Esto ha motivado a verificar los valores indicativos de la velocidad con otro instrumento, el GPS.

En la aplicación del método a los tres casos reales, en diferentes condiciones ambientales y de luminosidad se obtuvieron los siguientes resultados:

De estos tres casos estudiados, sólo ha sido posible obtener el dato de la pericia accidentológica del caso 2, cuya velocidad aproximada fue de 62 km/h. Considerando este valor como el verdadero, el error del método aplicado para este caso fue del 7,64%.

Asimismo, ha sido posible corroborar que los comparativos entre el método propuesto en el presente trabajo y los observados en dichos instrumentos, mantienen una estrecha correlación, aún en condiciones climáticas disímiles.

1.7 Conclusiones

El método propuesto ha sido satisfactorio, y ha resultado ser una alternativa complementaria del tradicional procedimiento de medición de velocidad por medio de pericias sobre las huellas de frenado.

La tecnología de procesamiento de imágenes está teniendo un desarrollo vertiginoso, hecho que impulsa una propensión sostenida a la baja de los costos de los sistemas de monitoreo en la vía pública, lo cual permite vislumbrar una tendencia, cada vez más marcada, hacia la proliferación de estos equipamientos, tanto en la esfera pública como en el ámbito privado.

Se puede afirmar la idoneidad del método dado que, con los estudios de casos presentados y las experiencias de campo realizadas, se obtuvo un resultado certero considerando un margen de error en promedio del 13.39% lo que da fidelidad al método y permite que el mismo sea apto para la determinación de velocidades vehiculares partiendo de las grabaciones de las cámaras de seguridad independientemente de las condiciones lumínicas y climáticas presentes en el ambiente.

1.8 Referencias Bibliográficas

ARIAS PAZ, Manuel. (2004). Manual de automóviles. Ed. Cie Dossat 2000 S.L..

ALBA LOPEZ, Juan José, GONZÁLEZ, Jesús M. e IGLESIAS PULLA, Alberto. (2001). Accidentes de tráfico: manual básico de investigación y reconstrucción. Ed. del Grupo de Seguridad Vial y Accidentes de tráfico, Universidad de Zaragoza,

Academia de Tráfico de la Guardia Civil. (2000). "Investigación De Accidentes De Tránsito" Editorial Dirección General de tráfico, 2da edición, Madrid.

LÓPEZ, H. O. (2014). Investigación de Huellas de Neumático. Revista Skopein: La justicia en manos de la Ciencia, (4), 19-37. - Accidentología vial, disponible en: https://ricardobadillograjales.blog/accidentologia-vial/

Introducción a la accidentología. Disponible en:

http://principiodeidentidad.blogspot.com.ar/2008/01/introduccin-la-accidentologa-vial.html Accedido el 27/10/2018

Informe Observatorio vial, Municipalidad de General Pueyrredón. Disponible en:

https://www.mardelplata.gob.ar/informesobservatoriovial accedido el 08/05/2019 - Informe del Ministerio de transporte, presidencia de la Nación Argentina. Disponible en:

https://www.argentina.gob.ar/transporte accedido el 08/05/2019

2 Análisis Estereoscópico de los Patrones de Impresión Producidos por los Sistemas de Suministro de Tinta de las Impresoras Epson Inkjet 1120 y XP231. Estudio de Caso

Camilo Andrés Morales Ortiz[9]

Resumen

La falsificación documental es una problemática que aqueja la sociedad desde tiempos inmemoriales, por cuanto sus métodos e instrumentos varian según los desarrollos técnico-científicos. En la actualidad, la impresión digital, entre esta la tecnología inkjet, es el medio nuevo para la creación, diseño y producción de documentos espurios, mismos que se hacen valer como auténticos en diferentes escenarios sociales, económicos, comerciales en entornos físicos y virtuales, etc. Por esta razón, el presente trabajo, es un estudio de caso donde se realizó un análisis estereoscópico a los documentos impresos por los sistemas de suministro de tinta de las impresoras Epson inkjet, L120 y XP231. El objetivo fue establecer la existencia, o no, de patrones de impresión que permitieran diferenciar entre uno u otro sistema de abastecimiento y, a su vez, discriminar entre los documentos producidos por éstos. Los resultados obtenidos permiten concluir, parcialmente, la existencia de un patrón de impresión.

Palabras Claves: Impresión digital, Impresora Inkjet, Patrones de impresión, Falsificación documental, Documentología Forense, Pericia Documentos Impresos, Informática Forense.

9 Profesional en Criminalística, Magister en Criminalística y Ciencias Forenses. Técnico en Criminalística Defensoría del Pueblo de Colombia. Correo electrónico, camo1989@hotmail.com

Abstract

Documentary falsification is a problem that has afflicted society since time immemorial, because its methods and instruments have varied according to technicalscientific developments. Currently, digital printing, including inkjet technology, is the new medium for the creation, design and production of spurious documents, which are asserted as authentic in different social, economic, commercial. For this reason, the present work is a case study where a stereoscopic analysis was performed on the documents printed by the ink supply systems of the Epson inkjet, L120 and XP231 printers. The objective of the previous was to establish the existence or not of patterns of printing that allowed to differentiate between one or another supply system and, in turn, to discriminate between the documents produced by them. The results obtained allow to conclude, partially, the existence of a printing pattern.

Key words: Digital Printing, Inkjet Printer, Printing Patterns, Document Forgery, Forensic

Documentology, Questioned Documents Examination, Computer Forensics

2.1 Introducción

La globalización y el desarrollo de la tecnología no sólo ha permeado la cotidianidad de las personas, también ha transformado las formas para comunicarse entre sí. En la actualidad, la información no sólo se transmite a través de medios físicos, también se realiza mediante la digitalización. Esto último, en algunos casos, ha permitido efectuar trámites comerciales o relaciones interpersonales en un entorno virtual, sin que necesariamente intervenga un documento físico, o papel.

A pesar de eso, "aunque dicha comunicación electrónica es muy conveniente para las personas, los documentos en papel todavía se utilizan ampliamente" (Szafarska, Wietecha-Posłuszny, Woźniakiewicz, y Kościelniak, 2011b, p. 78, *trad*. a), no obstante que la era del internet y la comunicación digital impera en la sociedades, con mayor prevalencia en las occidentales, "(…) el papel se utiliza como un importante portador de información" (Shang, Memon, y Kong, 2014, p. 2, *trad*. a).

La comunicación electrónica (Szafarska, Wietecha-Posłuszny, Woźniakiewicz, y Kościelniak, 2011b), generada por los desarrollos tecnológicos, permite gestionar y procesar la información utilizada en la vida cotidiana (Amatoa, Cozzolinoa, Moscatoa, y Moscato, 2019) y utilizarla en entornos digitales para fines sociales, comerciales, religiosos, económicos, etc. Dentro de esta sociedad surge la informática, como una herramienta que posibilita el manejo de la información y que se ha insertado en todos los espacios de relación humana, pero esto no ha sido igual para todos, provocando que se puedan diferenciar dos grupos de personas, las que tienen acceso a la informática y los que carecen de ella.

Por otro lado, las múltiples utilidades que se pueden dar a las tecnologías de la información son opacadas por los diferentes usos que puede tener también para cometer delitos, esto es lo que denominan, Darahuge y Arellano González (2011), como falsa panacea de la informática. La red permitió a las actividades humanas que requerían presencialidad efectuarse en entorno virtuales y algunas de ellas pueden llegar a ocasionar la comisión de conductas punibles, tales como pornografía infantil, tráfico de estupefacientes y de armas de fuego, hurtos, falsificaciones, entre otros.

En estos escenarios virtuales se crean e intercambian documentos, sobre los cuales recae la presunción de autenticidad y ostentan los mismos efectos jurídicos que los impresos o manuscritos, los cuales también se pueden digitalizar para que entren y operen en estos entornos digitales. Es así como la falsificación documental se extiende más allá de los soportes tradicionales, como por ejemplo el papel, generando las mismas consecuencias económicas y judiciales, como problemas de identidad individual, trasferencias bancarias no autorizadas por el titular, suscripción de contratos espurios, etc. En este sentido, Darahuge y Arellano González (2011) afirman:

> Por consiguiente, al estar involucrado el ser humano, aparecen diversas conductas relacionadas con el uso de las computadoras. La actitud delictiva del ser humano es inevitable y se encuentra reflejada de diversas formas, una de las que afecta al resto de los integrantes de este entorno de trabajo es el delito cibérnetico (p.8).

Como una paradoja, los avances tecnológicos permiten el desarrollo de una sociedad, pero a su vez son la causa de su deterioro, aunque no sólo desde la óptica criminal; basta con mencionar los problemas psicológicos que han emergido por el uso de las tecnologías de la información. Pero retomando lo punible, estas interacciones virtuales son un reto para la criminalística y las ciencias forenses, porque inevitablemente conducen a la comisión de hechos delictivos cibernéticos, donde en muchos casos intervienen documentos digitales.

La indagación de hechos delictivos tradicionales ha exigido que la investigación criminal sea multidisciplinar, donde las diferentes disciplinas de la criminalística y ciencias forenses se han articulado. Los delitos cibernéticos exigen igual requerimiento, es por ello que la administración de justicia a través de sus operadores judiciales, debería articular a los peritos informáticos forenses con otros profesionales, para la investigación de casos relacionados con falsificaciones documentales digitales donde también se requiere conocimientos en grafología y documentología forense.

El acceso y masificación de los sistemas de impresión digital, para este caso la tecnología inkjet, permiten la divulgación de ideas y del pensamiento mismo; de igual forma, posibilita el intercambio de información y la realización de muchas actividades comerciales. No obstante lo anterior, también son utilizados para falsificar documentos, logrando con esto crear problemas en la autenticidad de los mismos, o en términos de Heudt, Debois, Zimmerman, Köhler, Bano, Partouche y Pauw (2012, *trad. a.*): "(…) las impresoras de inyección de tinta son ampliamente utilizadas por personas con ideas fraudulentas para producir documentos sospechosos que se acercan mucho al original" (p.64).

Así como la escritura, los textos escritos e impresos han atravesado diferentes etapas evolutivas hasta las formas que se conocen en el presente; también la falsificación tiene una larga historia, ligada a los métodos para detectarla y a las personas que han ejercido esta profesión: la que hoy se llama Documentología Forense (DF). Respecto a los primeros, los estudios se han divido en exámenes, no invasivos y destructivos.

La falsificación documental afecta la credibilidad de las diversas transacciones comerciales, económicas, sociales, entre otras; que se realizan constantemente dentro

de las sociedades; ejemplo de ello es la circulación de dinero espurio que perturba las finanzas de un país. Esta problemática se profundiza en la actualidad por cuanto anteriormente falsificar un documento requería conocimientos especializados en el tema; hoy en día con el advenimiento y masificación de la impresión digital esto es posible sin que medie un saber técnico, sólo basta el manejo de ciertos dispositivos cotidianos para lograrlo.

Debido a lo anterior, la impresora inkjet y sus tintas son cada día más estudiadas internacionalmente en el ámbito legal-forense, porque son una herramienta que permite la falsificación documental, misma que es un hecho punible en muchos Estados. Respecto a esto Cruces-Blanco, Gámiz–Gracia, y García-Campaña (2007) señalan que la creación de documentos fraudulentos está asociada a la impresora inkjet. Por esta razón, la literatura académica sobre este punto está en aumento pues su finalidad es producir conocimiento científico que permita a la administración de justicia relacionar un documento impreso con una determinada impresora inkjet, lo cual allanaría el camino para ubicar al responsable de la conducta punible antes indicada.

Sobre lo anterior, las investigaciones científicas se han centrado en los estudios destructivos, un campo más ligado a la aplicación de la química como ciencia forense. Aunque son importantes sus aportes, los mismos no pueden considerarse la panacea del conocimiento sobre las falsificaciones mediante documentos impresos, pues se configuran muchas variables que impiden sostener tal afirmación. Por su parte, los análisis no invasivos no ocupan un lugar preponderante dentro de las publicaciones académicas, porque, entre otras cosas, están orientados a la subjetividad del perito. Este punto es evitable si media el método científico y, sobre todo, se genera más investigación aplicada al respecto, tal como lo propone este trabajo.

A modo de orientación y con el ánimo de lograr un mejor entendimiento del lector, las impresoras inkjet se clasifican, a parte del tipo de tinta y marca, por el sistema de suministro de tinta: unas utilizan los cartuchos y otras la recarga continúa. Esta forma de abastecimiento diferencia la muestra de impresoras aquí estudiadas y es la base de los resultados más adelante señalados.

Este trabajo tuvo como punto de partida la problemática brevemente señalada en los párrafos precedentes, porque exploró, mediante un análisis no destructivo, la relación existente entre las impresoras inkjet, EPSON L120 y XP-231, con los documentos impresos producidos por las mismas, mediante los posibles patrones de impresión que éstas transfirieran a estos últimos debido a sus diferencias en el abastecimiento de tinta. Por esta razón y con las anotaciones efectuadas, este trabajo plateó como hipótesis lo siguiente: La tecnología inkjet presenta dos formas para el suministro de tinta, ya sea mediante recarga continua o a través de cartuchos, las cuales configuran procesos mecánicos disímiles entre sí. Cuando un documento

es impreso, transita por uno u otro sistema de abastecimiento, traspasándoles a éste sus respectivos patrones de impresión. Lo anterior está en concordancia con los principios de producción, transferencia, correspondencia e identidad de la criminalística.

Señalada la hipótesis, la pregunta que transversalizó los resultados de este estudio fue considerar si las formas de abastecimiento de tinta de las impresoras inkjet producían, o no, patrones de impresión en los documentos originados de las mismas, y si aquellos eran observables y descriptibles para identificar su fuente de origen.

Para desarrollar la hipótesis y responder la pregunta antes señalada, se trazó como objetivo general lo siguiente: establecer si existen, o no, patrones de impresión que permitan diferenciar e identificar entre las impresoras ink-jet que utilizan cartuchos y las que emplean el sistema de recarga continúa para el suministro de tinta. A su vez, se platearon como objetivos específicos: a) describir las firmas intrínsecas plasmadas en un documento tanto por las impresoras ink-jet que utilizan cartuchos y las que emplean el sistema de recarga continúa para el suministro de tinta; b) comparar las firmas intrínsecas plasmadas en un documento tanto por las impresoras ink-jet que utilizan cartuchos y las que emplean el sistema de recarga continúa para el suministro de tinta.

Los resultados permiten afirmar, parcialmente, la presencia de un patrón de impresión que permitiría comparar y diferenciar entre muestras cuestionadas. Para alcanzar este producto, se elaboró un diseño metodológico cualitativo, de tipo descriptivo, inductivo y transversal.

2.2 La Utilización de las Impresoras Inkjet y su Impacto en la Sociedad

La humanidad desde la prehistoria ha intentado mediante diferentes formas comunicarse con su entorno y sus semejantes. La invención de la escritura es una de estas, ya que: "(…) el hombre satisfizo la necesidad, experimentada desde las más tempranas etapas de su evolución cultural, de extender las comunicaciones en el espacio y en el tiempo". (Velásquez Posada, 1979, p.16). Lo anterior, debido a lo etéreo que entraña el lenguaje gestual, sonoro y hablado, que sólo perdura en el tiempo si genera relevancia en la memoria del interlocutor.

Durante largos periodos de tiempo los textos escritos se elaboraron con diferentes sustancias animales y/o vegetales, lo que se llama material escritor, y utilizaban como soportes las rocas, las paredes, el papiro, el pergamino, la piel animal, la arcilla, etc. (Orellana Wiarco y Orellana Trinidad, 2013). Cada uno de

estos elementos han tenido desarrollos independientes; sin embargo, los mismos se han producido por la usanza, y sus necesidades derivadas, de uno y otro.

El desarrollo del papel, la tinta, el bolígrafo, el lápiz, entre otros, permitieron que el hombre dejara huella de un determinado hecho a través de textos escritos; después la imprenta y los sistemas de impresión posibilitaron la creación de textos impresos, logrando así masificar la producción de documentos. Cada una de estas invenciones ha cambiado la forma de comunicación y han significado pasos importantes para la creación de otros: se destaca el sistema de impresión digital, tanto el inkjet, como el electrográfico.

En la actualidad, la tecnología y el fácil acceso a sus desarrollos posibilitan el entorno descrito por Bai, Zhang, Liu, Meng, Wang,Wu y Chen (2010, *trad. a*.), cuando afirman que: "(..) hoy en día, casi todas las oficinas y los hogares están equipados con una impresora" (p.288). Precisamente, el actual mercado de los equipos periféricos de salida integrado, entre otros por las impresoras electrográficas e inkjet, se ha convertido según estos mismos autores: "(…) en el tercer (3) negocio más importante dentro de las tecnologías de la información" (p.288); consolidando lo que se denomina la impresión digital (ID).

En la actual era digital, los avances tecnológicos han posibilitado mejoras en los sistemas de impresión inkjet, también denominada chorro de tinta e inyección de tinta y electrográficos, permitiendo que estas tecnologías dominen el mercado y se inserten en la cotidianidad de las instituciones, oficinas, hogares y, por qué no, en el ámbito personal, debido a su alto rendimiento, velocidad, calidad en el color y, sobre todo, la asequibilidad. Estas características son gradualmente renovadas con modelos que superan versiones anteriores; por ello, las empresas dedicadas a la fabricación de las tecnologías de impresión inkjet y electrográficas intentan conseguir el equilibrio entre eficacia y eficiencia, pues se optimizan las calidades del producto permitiendo impresiones de alta calidad, pero a precios bajos. Lo anterior se ha dado en aproximadamente 40 años de comercialización de estas tecnologías, especialmente la electrográfica, donde con el tiempo se han desarrollado y renovado así mismas (Biedermann, Taroni, Bozza y Mazzella, 2011).

La globalización ha permitido que estos desarrollos tecnológicos estén al alcance de las personas debido a los bajos precios y a su inmediata disponibilidad, modificando en cierta medida su entorno social, político, económico, religioso, entre otros. En igual sentido, Wensing, Schripp, Uhde y Salthammer (2008) plantean que:

> Desde el comienzo los medios electrónicos eran utilizados para trasmitir información y procesar datos, ahora se han generalizado a la vida diaria, como por ejemplo, los televisores, las grabadoras de vídeo, los ordenadores con sus periféricos como monitores e impresoras, escáneres y fotocopiadoras (p.418).

Cada día el uso de estos equipos ocupa espacios que antes eran restringidos al entorno laboral. Además de los documentos manuscritos, los impresos ocupan un lugar importante dentro de la sociedad contemporánea, donde cualquier persona puede crearlos por sí mismo o a través de otro. En efecto, esto obedece a que este medio permite plasmar y concederle valor probatorio a muchas actividades, transacciones civiles, legales, económicas y comerciales, esto en gran medida está ligado a la disponibilidad de computadoras, por ello, actualmente impresora y computador forman una díada fácilmente ubicable en casas y empresas. En este sentido, se debe tener en cuenta que la impresora inkjet *per se* no actúa de forma aislada, por cuanto requiere de un ordenador para funcionar (Daly, Harrington, Martin y Hutchings, 2015). Es así como, Akao, Kobayashi y Seki (2005), afirman que ambas tecnologías: "(…) se utilizan para fabricar ilegalmente documentos como falsos testamentos, contratos y recibos que pueden utilizarse para perpetrar crímenes" (p.1, *trad. a.*). Para explicar mejor esto, la computadora permite editar los datos y envía los mismos mediante un lenguaje de programación a la impresora, ésta los interpreta y procede a la impresión.

En lo concerniente a la era digital, donde la información es trasmitida y almacenada mediante computadores, se pensaría que la usanza del papel estaría limitada a ciertos campos sociales, cuya tendencia en el tiempo se configuraría a desaparecer. No obstante lo anterior, Kumar, Kumar y Sharma (2017), indican que: "(…) han pasado más de doscientas décadas desde el descubrimiento del papel y todavía se utiliza como medio para almacenar datos o portar de información […] la última década ha sido testigo de un aumento del 35% en el consumo de papel" (p.19, *trad. a.*). El papel se sigue utilizando como soporte para muchas actividades, entre ellas, la falsificación de documentos oficiales y/o privados (Szafarska et al., 2011b).

No obstante la existencia del entorno digital, el papel es ampliamente utilizado en la sociedad para realizar o recibir cualquier tipo de transacción comercial, social o simplemente para plasmar una idea. Por consiguiente, por un lado, es uno de los medios de mayor uso para transmitir información y, por el otro, el más sensible para ser modificado porque: "(…) los métodos para perpetrar falsificación y alteración de documentos son cada vez más sofisticados" (Braz, López-López, y García-Ruiz, 2013, p. 206). Lo anterior, sin que necesariamente intervengan conocimientos especializados en el tema, solo basta con un equipo, la impresora.

La impresión digital ha permitido el desarrollo de muchas industrias, como la publicitaria, las comunicaciones, la litográfica, etc. Sin embargo, este tipo de recursos también terminan siendo utilizados para la "(…) falsificación de documentos, tales como el robo de identidad, los contratos modificados, fraude de seguros, la falsificación de documentos de seguridad y falsificación de moneda que están afectando a los ciudadanos, la seguridad nacional e incluso la economía mundial"

(Trejos, Corzo, Subedi y Almirall, 2014, p. 09). Dicha situación está relacionada con el acceso fácil e inmediato que se dispone para obtener y utilizar una impresora, tanto inkjet, como láser, que es inevitable encontrarlas en cualquier entorno laboral o doméstico (Byeon y Kim, 2012).

Szafarska, Wietecha-Posłuszny, Woźniakiewicz, y Kościelniak (2011), relacionan directamente los métodos de impresión inkjet y electrográfico con la creciente falsificaciónalteración documental. Según aquellos, dicha díada es un flagelo que está permeando a la sociedad porque la mayoría de documentos son tachados de espurios en su integridad y procedencia. En el mismo sentido, Cruces-Blanco, Gámiz–Gracia, y García-Campaña (2007), afirman que: "(…) los documentos impresos y fotocopiados están involucrados en la falsificación, el fraude y el terrorismo" (p.224). Aunque las fotocopiadoras no son tema dentro de esta investigación, también integran el mercado de la ID y, además, son unas herramientas utilizadas para la comisión de hechos punibles.(Cruces-Blanco et al., 2007). Lo anterior obedece, en términos de LaPorte (2004), a que: "(…) este tipo de sistemas están ampliamente disponibles en el hogar y en la oficina, convirtiéndolos en un recurso oportuno para la actividad criminal" (p.610, *trad. a.*).

En el mismo sentido, tanto De Almeida, Correa, Rocha y Scafivy Pop (2013), como YingjianXu, Xin-xinZhou y Xiao-fanShi (2016), plantean que el aumento de las falsificaciones documentales se deben a tres factores: 1. La eclosión-disponibilidad de marcas y modelos de impresoras basadas en tecnología de chorro de tinta y electrográfica; 2. Los pocos conocimientos técnicos y la falta de experiencia requerida para manejarlas; y 3. La calidad de las impresiones que simulan a los documentos originales. Estas variables explican las causas asociadas al aumento de documentos espurios, las cuales contrastan con las facilidades que dichos dispositivos propician a las labores cotidianas dentro de una sociedad. Siguiendo la anterior, Calcerrada y García Ruiz (2015), ofrecen los siguientes datos:

> Durante los últimos años el aumento en las ventas de impresoras es incuestionable. Algunos datos recogidos de la literatura avalan este hecho: en 2002 se vendieron 74 millones de impresoras en el mundo entero y se reportaron 5000 casos reales donde éstas son utilizadas para la falsificación en Japón; en Polonia en el año 2008, el 59% de los casos de falsificación se hicieron con impresoras (p.155).

Por su parte, Noronha, Basheer, Vijay, Alnajjar, Sharma y Singh (2017), afirman que en septiembre del año 2016 el Statistic Brain Research Institute realizó un estudio donde hasta esa anualidad se vendieron 106 mil millones de impresoras a nivel mundial, dato que corresponde tanto a la tecnología inkjet como la electrográfica.

Por otro lado, en ventas la primera representó 18 mil millones de dólares, mientras la segunda 30 mil millones. Nótese como desde el periodo del 2002 hasta el 2017 la comercialización de impresoras incrementó sustancialmente, aspecto que muestra su adquisición fácil y su inserción en ámbitos domésticos. Por esto último, Noronha et al. (2017), plantean que existe una mayor probabilidad de encontrar una impresora en casi todas las casas y oficinas.

Seguramente estas cifras, si se piensa a escala mundial, para el día de mañana serán insignificantes, debido a la necesidad de consumo que tendrá la sociedad y a la simplicidad para manejar dichos dispositivos. Todo lo anterior permite, según Szafarska et al. (2011a), que: "Las impresoras se utilicen con frecuencia en la falsificación, para crear, adaptar o imitar documentos con la intención de engañar" (p.1234, *trad. a.*).

El fraude de documentos mediante la utilización de impresoras inkjet y eletrográficas no sólo representa problemas a la seguridad de los ciudadanos, como por ejemplo robo de identidad, también a los intereses de un país y a la economía mundial (Trejos, Corzo, Subedi, y Almiral, 2014). Respecto a esto último, en 1995 el Servicio Secreto de los Estados Unidos (EE.UU) mostró que el costo de la moneda nacional espuria osciló entre US$174.924 y US$2.440.229 (LaPorte y Ramotowski, 2003). De igual forma, esta misma agencia, reportó que en el año 2001 representó entre US$1.151.791 y US$18.403.257, donde el factor común fueron las tecnologías inkjet y electrográfica. Si se observa, en el segundo año señalado se originó un incremento significativo de dinero falsificado, que en cierta medida se traduce en una problemática de mayor escala que afecta la economía de un Estado. En Estados Unidos, por ejemplo, en el año 2013 se decomisaron 88 millones en moneda fraudulenta (LaFrance, 2014), donde las autoridades del Estado de Indiana reportaron incautaciones que ascendían a la suma US$77.000 (McCleery, 2013).

En igual sentido, Kula, Król, Wietecha-Posłuszn, Woźniakiewicz y Kościelniak (2014), consideran que las falsificaciones mediante documentos impresos representan un problema en la actualidad, esto debido a que es un flagelo que: "(…) está creciendo rápidamente en todos los ámbitos públicos y afecta la mayoría de los documentos relacionados con dichos campos" (p.78, *trad. a*). Estos autores convergen en que la principal herramienta de producción de los mismos son las impresoras de inyección de tinta, las cuales tienen una calidad considerable debido a sus frecuentes desarrollos tecnológicos.

Como ya se ha mencionado, una de las repercusiones de más impacto generadas por la falsificación son las relacionadas con los billetes. Para De Almeida, Correa, Rocha y Scafivy Pop (2013) y Ying-jianXu, Xin-xinZhou y Xiao-fanShi (2016) este es un problema cuyas consecuencias son de impacto mundial y se refleja en la economía de cada país. En la literatura científica también se ha documentado las experiencias

de otros países, a parte de Estados Unidos, respecto a esta problemática: Brasil es uno de éstos. En dicha nación, desde 1994, se oficializó el Real como su moneda oficial y a partir de esa misma fecha ha aumentado, vertiginosamente, la falsedad de esta divisa; por cuanto, al parecer, el billete de 50 presenta características semejantes a otras denominaciones, lo que ha generado que esta denominación esté relacionada con el 70% de las incautaciones de billetes apócrifos en dicho país (De Almeida et al. 2013). A propósito de la falsificación documental:

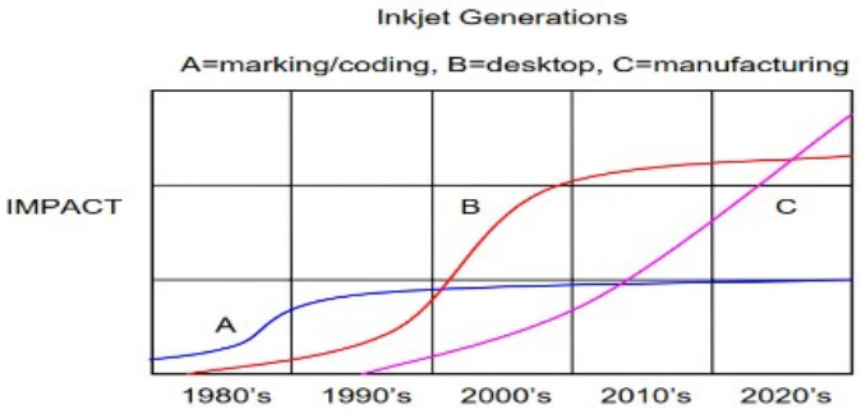
> El servicio secreto de los Estados Unidos (USSS) tiene una base de datos de 90,000 especímenes, entre tarjetas de crédito, cheques, licencias de conducir, pasaportes, tarjetas de registro de extranjeros, tarjetas de seguro social y registros de nacimiento, donde el 61.6% de los documentos han sido creados utilizando inyección de tinta, tóner o una combinación de las dos tecnologías (LaPorte y Ramotowski, 2003, p. 1).

Llama la atención que más de la mitad de los elementos a disposición de la USSS fueron elaborados por los sistemas inkjet, electrográfico o la combinación de ambos, mostrando así que el 39.4% de dichos objetos son elaborados mediante otros métodos, seguramente los tradicionales.

Los datos que muestra el USSS revisten una gran relevancia para la economía de los Estados Unidos y, seguramente, para otros países, pero las cifras pueden ser mayores si aparte de los billetes se cuantifica el valor que representa la adulteración de documentos de identidad, pasaportes, facturas, licencias de conducción, etc., o los documentos públicos y privados.

Los datos antes vistos asocian la impresora inkjet a actividades delictivas por cuanto tal como lo refieren Guo, Patanwala, Bognet y Ma (2017), es la tecnología más utilizada en la actualidad. Para que esto fuera así, la misma ha atravesado numerosos desarrollos y mejoras a partir de la década de 1960 y 1970, período en el cual nació como una herramienta a utilizar en las artes gráficas y en la codificación de productos. Sin embargo, su usanza se extendió a otras aplicaciones y campos. Respecto a esto último, Hoath y Hutchings (2008) señalan, que los dispositivos de chorro de tinta están representados entre tres generaciones: la primera está relacionada con la marcación; la segunda con su utilización en el ámbito doméstico y laboral; y la tercera, se vincula a la industria decorativa en textiles, cerámicas, alimentos, puertas, etc, (*ver figura 1)*. También se ha explorado en el ámbito microscópico, como por ejemplo, la impresión de muestras biológicas en diferentes soportes (Allain, Stratis-Cullum y VoDinh, 2004).

Figura 1. Muestra evolución y proyección de las diferentes aplicaciones de las impresoras inkjet



Fuente: Hoath y Hutchings (2008, p.2)

De la anterior figura, nótese la relación entre la impresora inkjet y su inserción paulatina en el ámbito doméstico, donde la utilización de la misma antes del año 2000 era inferior respecto al período y proyecciones siguientes. La explicación a esto puede estar relacionada con la globalización y al acceso fácil de desarrollos tecnológicos que trae consigo este momento histórico de la sociedad. Se destaca el hecho que durante el período comprendido entre 2010 y 2020, la tecnología chorro de tinta mantendrá su inserción en el hogar y en la oficina, esta situación Hudd la denomina "*presencia omnipresente*" (2010, p. 3). Esto no es para menos, si se tienen en cuenta, según este autor, que desde 1984 hasta finales del 2007 se vendieron más de 500 millones de impresoras inkjet, destinadas precisamente a este mercado.

Aunque no fue objeto de esta investigación, se puede afirmar que la impresora láser es uno de los dispositivos de impresión más utilizados, según lo afirman (Ferreira, Navarro, Pinheiro, dos Santos, y Rocha, 2015); para Cruces-Blanco et al. (2007), ha aumentado su uso durante los últimos 20 años. En este mismo sentido, Skenderović Božičević, Gajović y Zjakić, (2012) afirman que: "(…) entre otros equipos utilizados para la falsificación, los sistemas de impresión de tóner, sin duda, ocupan un lugar importante" (p. 314). La cualidad anteriormente descrita de esta tecnología hace que: "(…) el número de exámenes forenses efectuados a los documentos elaborados mediante impresoras láser se incremente" (Chu, Cai, Tsoi, Yuen, Leung, y Cheung, 2013, p. 4311). Aparte de esta tecnología, su materia escritora es ampliamente requerida por sus características físico-químicas, según Bai et al. (2010), es: "(…) uno de los consumibles más grandes en el trabajo diario de oficina, su popularidad es cada vez mayor debido a las impresoras y fotocopiadoras.

Se estima que la demanda mundial de tóner es de alrededor de 240,000-260,000 toneladas" (p.289). Según lo antes citado, las impresoras láser son muy importantes, tanto por su relación con la falsificación, como por su necesidad de consumo, lo que ha generado investigaciones relevantes sobre el tema, como las realizadas por Chu et al. (2013); Ferreira, Navarro, Pinheiro, Dos Santos y Rocha. (2015); Spagnolo (2006), entre otras.

En varios apartes se ha mencionado que tanto la tecnología de inyección de tinta, como la electrográfica, son ampliamente empleadas para fines delictivos. En este sentido, LaPorte y Ramotowski (2003), afirman que la primera representa un porcentaje mayor en usabilidad, debido al costo bajo en su adquisición y en los consumibles que requiere. A parte de esto, ofrece una capacidad mejor para procesar las tintas dando resultados óptimos para los fines delincuenciales. Este mismo argumento lo comparten Kula et al. (2014), pues afirman que:

"Los documentos cuestionados producidos en equipos de oficina modernos son un problema frecuente en el mundo de hoy. Una gran parte de falsificaciones se refiere a documentos impresos por inyección de tinta" (p.92, *trad. a*.).

Las ventajas y usos de la tecnología inkjet se traducen en actividades delictivas, porque ofrecen alta calidad en la imagen, grandes cantidades de impresión por minuto, fácil manejo, no requieren exigentes requisitos técnicos para su montaje, son asequibles, no requieren conocimientos especializados en artes gráficas por parte del operador, consumen pocos recursos, los repuestos son económicos, son dispositivos pequeños y fáciles de trasportar.

(Byeon y Kim, 2012); peero sobre todo, si se deterioran, el mercado siempre los reemplazará por equipos con mejores especificaciones. Estas características, según Skenderović Božičević, Gajović, y Zjakić (2012): "(…) representan la mayor amenaza debido a su capacidad para producir grandes cantidades de falsificaciones en un período muy corto…" (p.314); sobre todo, porque la proliferación de las falsificaciones documentales provienen, tanto de aficionados como de profesionales (Szafarska et al., 2011), un campo que anteriormente estaba reservado a estos últimos, mientras los primeros han encontrado su nicho en la impresión digital. Szafarska et al. (2011a) planten que no sólo lo anterior es preocupante, también lo es la reproducción tan especializada que realizan las impresoras, las cuales pueden ser operadas por profesionales o aficionados, lo cual hace que: "(…) las falsificaciones sean más difíciles de detectar" (p.78).

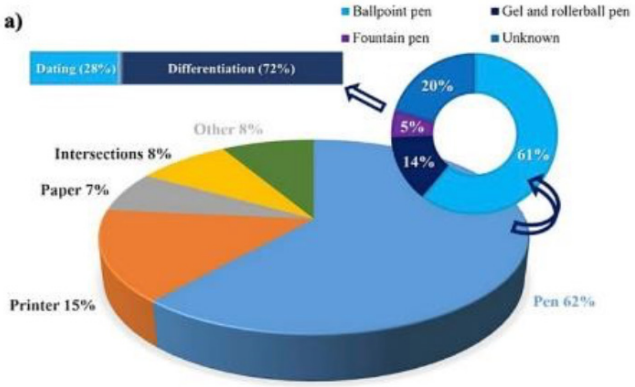
En igual sentido, se afirma que: "(…) las tecnologías nuevas de impresión proporcionan copias muy similares de los documentos originales, aumentando el problema de la falsificación" (Calcerrada y García-Ruiz, 2015, p. 155). Es así como la falsificación documental se ha convertido en una de las problemáticas más recurrentes dentro de las sociedades modernas, cuyo centro son los documentos

impresos mediante la impresión digital. Respecto a esto último Khanna, Mikkilineni, Chiu, Allebach, y Delp (2008) destacan lo siguiente:

> Lo mismo es válido para el documento impreso, que en muchos casos es un accesorio directo a muchos actos criminales y terroristas. Los ejemplos incluyen la falsificación o alteración de documentos utilizados para fines de transacciones de identidad, seguridad, o de grabación. Además, el material impreso se puede utilizar en el curso de la realización de actividades ilícitas o terroristas. Los ejemplos incluyen manuales de instrucciones, listas de los equipos, notas de reuniones y correspondencia (p.22, *trad. a.*)

Del panorama referido en los párrafos precedentes se infiere que la falsificación documental efectuada a través de las impresoras inkjet, es objeto importante de estudio por parte de la Criminalística y las Ciencias Forenses, cuyos resultados permiten a la administración de justicia de cualquier Estado, investigar los hechos punibles perpetrados a través de documentos impresos. Como señala Spagnolo (2006): "(…) el problema de la falsificación es un problema que despierta gran interés en la ciencia forense" (p.102), especialmente para la Documentología Forense (DF). Esta disciplina de la criminalística ha estudiado las falsificaciones y alteraciones documentales en sus diversas presentaciones tecnológicas, pasando de la búsqueda de patrones grafonómicos a los generados por impresión. En la actualidad, el estudio forense de impresoras inkjet y electrográficas está ocupando un lugar especial dentro de las investigaciones científicas. En la figura 2 se muestra un cuadroresumen realizado por Calcerrada y García-Ruiz (2015) donde se observa la tendencia antes descrita entre los años 2000 y 2014, aunque su porcentaje sea del 15%, no deja de ser significativo, máxime que dichos equipos son cada días más utilizados.

Figura 2. Tendencia de la literatura relacionada con la Documentología Forense
Fuente: Calcerrada y García Ruiz (2015, p.145)



Fuente: Calcerrada y García Ruiz (2015, p.145)

Antes del advenimiento de la ID moderna, compuesta principalmente por los sistemas inkjet y electrógrafico, el mercado en este tema ofrecía las siguientes tecnologías: manual y mecánica; ahora, además de las anteriores ofrece los denominados como periféricos. La primera son los instrumentos de escritura, siendo los más utilizados: el lápiz, el bolígrafo, las plumas fuente, los marcadores, los roller ball y los útiles con tintas gel (Ezcurra y Grávalos,

2010). En consecuencia, no es extraño que el esfero ocupe un 62% dentro de la revisión bibliográfica realizada por Calcerrada y García-Ruiz (2015), porque es una de las invenciones del siglo XX que le ha permitido al ser humano, e indudablemente lo seguirá siendo, aunque en un porcentaje más bajo, escribir su propia historia. Por su parte, la segunda está compuesta por las máquinas de escribir. Por último, la tercera está integrada por las impresoras de PC, subdivididas según su tecnología de impresión (Ezcurra Gondra y Grávalos, 2012) en: con impacto, donde se destacan las matriciales y las térmicas; y sin contacto, integradas por los sistemas inkjet y láser. Es importante resaltar que el porcentaje asignado a las impresoras dentro de la investigación antes citada obedece a la segunda categoría.

Revisando la figura 2, en este gráfico estadístico es evidente que el porcentaje asignado a las impresoras es inferior al establecido para el bolígrafo, pero desde la óptica forense, también significa que estos últimos han perdido su hegemonía como el único elemento impresor, porque: "(…) en el mundo moderno de los ordenadores, escáneres e impresoras, el número de documentos escritos a mano se ha reducido drásticamente (Kula et al., 2014, p. 118), y por consiguiente, el uso de éstas ha originado varias investigaciones científicas, en la medida en que: "(…) su uso masivo está generando duda sobre la autenticidad de los documentos impresos" (Ferreira,

Navarro, Pinheiro, dos Santos, y Rocha, 2015, p.105). Es por ello que la criminalística y las ciencias forenses tienen que ofrecer sus mejores herramientas para abordar dicha problemática, muchas veces transmutada en delitos de gran escala, como los cometidos contra la vida, la libertad, la administración pública, etc.

2.3 Observación y descripción de patrones de impresión

A modo de resumen, durante las páginas de este trabajo se han planteado dos hechos surgidos desde la literatura académica y científica: el primero, está relacionado con el aumento de falsificaciones mediante impresoras inkjet. En cuanto al segundo, referido al análisis de documentos impresos dudosos, el reto para la Criminalística y las Ciencias Forenses es ser capaz de discriminarlos e identificar la marca y modelo de la impresora que lo ha elaborado.

Como se ha visto anteriormente, este trabajo se centró en las impresoras de inyección de tinta, no obstante que las electrográficas también son importantes. A parte de las razones que se han señalado hasta este punto, varios artículos investigativos de contexto forense han tratado con este objeto de estudio, destacándose los trabajos de: Guo, Patanwala, Bognet y

Ma (2017); Lennard, El-Deftar y Robertson (2015); Król, Karoly y Kościelniak (2014); Heudt et al. (2012); Szafarska, Wietecha-Posłusznya, Woźniakiewic y Kościelniak (2011b); Akao , Kobayashi y Seki (2005). De igual forma, se ha analizado ampliamente la marca Epson, *ver figura 3*, la cual es una de las más examinadas junto a Hewlett Packard, Brother, Canon y Lexmark (Allain et al., 2004).

Figura 3. Relación de marcas de impresoras utilizadas en la investigación desarrollada por LaPorte (2004)

Inkjet Printers	Laser Printers	Photocopy Machines
HP DeskJet 656C	HP LaserJet 4L	Kodak Image Source 50
HP DeskJet 855 C	HP LaserJet 5P	Xerox Document Center 425 DC
HP DeskJet 870 Cse (1)	HP LaserJet 6MP	Savin 2527
HP DeskJet 870 Cse (2)	HP LaserJet 1100	
HP DeskJet 870 Cse (3)	HP LaserJet 1200	
HP DeskJet 970 Cxi	HP LaserJet 2100	
HP DeskJet 970 Cxi	HP LaserJet 2200d (1)	
HP DeskJet 932C	HP LaserJet 2200d (2)	
HP DeskJet 5550	HP LaserJet 3100	
Canon BJC 6000	HP LaserJet 3200	
Canon Multipass C500	HP LaserJet 4000N	
Lexmark Z12	Lexmark Optra T610	
Epson Stylus Color 600		
Epson Stylus Color 740		
Epson Stylus Color 900		
Epson Stylus CX 5200		
Epson Stylus Photo 785 EPX		

Fuente: LaPorte (2004**,** p.3)

Ahora bien, diferentes autores como: Shang et al. (2014), Heudt et al. (2012), Khanna et al. (2008), Dasari y Bhagvati (2006), LaPorte, (2004) LaPorte y Ramotowski (2003), Arbouine y Day (1994), entre otros; orientan sus investigaciones a identificar la marca y modelo de la impresora que ha elaborado el documento analizado. Pero en este trabajo de investigación, al contrario de lo propuesto por los autores mencionados, no comparte dicha premisa por cuanto las marcas de tecnología inkjet utilizan insumos y partes compatibles entre las mismas, más aún, las economías emergentes han propiciado la eclosión de genéricos. Dado estas variables es más factible aplicar métodos para discriminar muestras dubitadas entre sí que intentar relacionar su procedencia, es decir, es infructuoso dirigir la labor pericial en determinar la marca y el modelo de una impresora inkjet cuando en el mercado se utilizan suministros universales, aplicables a cualquier dispositivo de impresión sin distinción de su casa fabricante.

Lo que se realizó en esta investigación estuvo entonces orientado a proponer el sistema de suministro de tinta, ya sea continuo o mediante cartucho, como un elemento nuevo en el análisis de documentos impresos mediante la tecnología inkjet. Quiere decir lo anterior, que la intención aquí es generar herramientas para que el perito pueda discriminar, mediante el examen descriptivo y comparativo, documentos dudosos producidos mediante el sistema de inyección de tinta. A parte de esto, como se ha mencionado anteriormente, también se pretende sugerir una

categoría de análisis nueva al protocolo propuesto por Ezcurra Gondra y Grávalos (2012) para tal fin. Estos autores señalan que: "(…) para facilitar el trabajo del perito, sugerimos un protocolo a seguir para la realización del cotejo de impresoras de tinta inkjet, que no pretende ser el único, simplemente es el que nuestra experiencia nos hace entender como más adecuado" (p.128, *trad. a.*). Según esto, ellos plantean las siguientes fases:

1. Establecer el tipo de impresión: en este ítem se caracteriza el tipo de impresión inkjet, es decir, si es de flujo continuo o gota a demanda.

2. Observación de posibles marcas dejadas por los rodillos de arrastre del papel: los rodillos de la impresora ejercen presión cuando el soporte es transportado por la misma.

3. Definición de matrices: consiste en examinar y comparar si los caracteres impresos son coincidentes y producidos por una misma matriz.

4. Dirección de la impresión: se establece debido a las gotas satélites, puesto que las mismas caen después de la gotita principal, localizándose así en el área inmediatamente exterior (zona perigramática) al carácter. Con esto se puede determinar si los cabezales de impresión imprimen moviéndose a la izquierda, a la derecha o en ambos sentidos.

5. Localización de posibles rayas horizontales y distancia entre ellas: a veces el cabezal de impresión deja zonas sin tinta, visualizándose como una raya blanca.

6. Estudio de las posibles pautas que tengan los puntos de una impresora concreta: aquí se estudia la forma y el tamaño de los puntos, así como también el patrón de caída y formación de los mismos.

7. Identificación y caracterización de defectos: se examinan los defectos por degaste y uso que presenta la impresora.

Visto lo anterior, Gondra y Grávalos (2012) no incorporaron dentro del primer paso la identificación del sistema de suministro de tinta. Es importante acotar que la mayor proporción de impresoras de inyección en tinta ubicadas en los hogares y oficinas están basadas en el sistema de gota a demanda, mientras que las de flujo continuo son más utilizadas en el ámbito industrial. No significa esto que estas últimas no estén relacionadas con la comisión de hechos punibles, empero, la literatura especializada, tal como se ha señalado en diferentes oportunidades, asocia las impresoras domésticas con el aumento de la falsedad documental. Pero, no quiere decir, que lo postulado por estos autores no sea importante, sino que se deben adicionar elementos de análisis nuevos como, por ejemplo, el sistema de suministro

de tinta, que permita abordar la falsificación documental mediante impresoras inkjet desde diferentes áreas del conocimiento, como la Documentología Forense.

El sistema de suministro de tinta empleado por las impresoras inkjet es una característica que permite clasificar las mismas en dos categorías únicas, oscilante entre suministro a través de cartuchos, o mediante recarga continúa. Por esta razón, esta distinción adquiere valor en el campo pericial, en la medida que posibilita la configuración de un criterio adicional para el examen de documentos impresos mediante la inyección de tinta.

2.4 Metodología de Estudio Aplicada

Ya en la introducción se mencionó la metodología de investigación que se aplicó en esta investigación. Por lo tanto, se explicará en detalle para presentar el análisis y procesamiento de los datos obtenidos de la muestra objeto de estudio, la cual necesariamente conduce al campo disciplinar de la DF.

El método que se empleó es el signalético o señalético (Velásquez Posada, 2004). Éste es ampliamente utilizado en pericias grafo y documentológicas, puesto que, el análisis que se realiza está mediado por la estructura del método científico, permitiendo así, el tránsito por varios estadios para obtener el conocimiento objetivo sobre determinada realidad o hecho. Estos son: observación, señalamiento-descripción de hallazgos distintivos, confrontación o comparación, y juicio de valor o conclusiones.

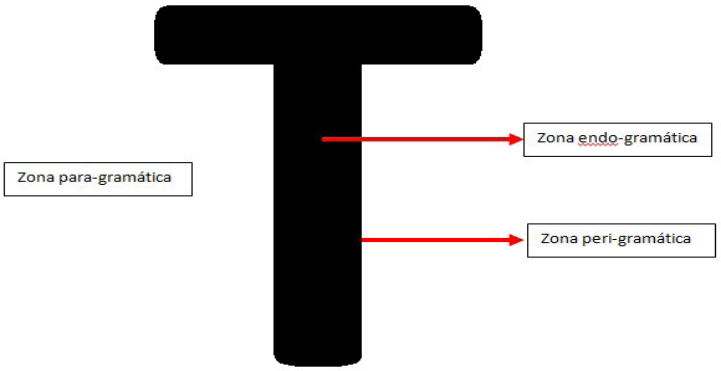
El método signalético no permite realizar un análisis comparativo para discriminar e identificar semejanzas y diferencias entre las muestras examinadas (Subedi, Trejos y Almirall, 2015; Metzinger, Rajkó y Galbács, 2014). Es más, se traduce en una forma básica para investigar documentos impresos mediante la tecnología inkjet (Król, Karoly y Kościelniak, 2014), permitiendo la observación y descripción de sus características específicas que se traducen en valor probatorio (Arbouine y Day, 1994) dentro de la administración de justicia. A parte de lo señalado anteriormente, también se aplicó la guía estándar para el examen de documentos impresos mediante el sistema inkjet, por cuanto señala que todo el proceso de análisis de diferencias debe estar debidamente documentado.

2.5 Presentación de los Resultados

Estructura del carácter. Los símbolos, letras, números e imágenes impresas en un documento se denominan, según la Real Academia Española, caracteres. A efectos de descripción se emplearán los términos utilizados por Velásquez Posada (2004)

para detallar el trazo, puntualmente este trabajo acogerá las zonas, endo-gramática, peri-gramática y paragramática, *ver figura 3*. La primera permite ubicar los patrones de impresión dentro del carácter, la segunda en sus contornos, mientras la última en sus regiones aledañas.

Figura 4. Zonas del carácter



Fuente: Elaboración del investigador (2018)

Características de las impresoras inkjet estudiadas. Epson L120[10]: es un dispositivo que se basa en la tecnología gota a demanda y en el sistema piezoeléctrico. Utiliza las tintas de forma separada y el suministro de las mismas es externo, es decir, recarga continua.

Epson XP-231[11]: es una impresora que se basa en la tecnología gota a demanda y en el sistema piezoeléctrico. Utiliza las tintas CMYK de forma aislada y el suministro de las mismas se realiza mediante cartuchos.

Hipótesis. La tecnología inkjet presenta dos formas para el suministro de tinta, ya sea mediante recarga continua, o a través de cartuchos, las cuales configuran procesos mecánicos disímiles entre sí. Cuando un documento es impreso, transita por uno u otro sistema de abastecimiento, traspasándoles a éste sus respectivos patrones de impresión. Lo anterior está en concordancia con los principios de producción, transferencia, correspondencia e identidad de la Criminalística. Es importante resaltar que, la hipótesis atrás planteada surge del aporte realizado por la investigación efectuada por Noronha et al. (2017).

10 Información obtenida https://epson.com.co, consultada 12/11/2017

11 Información obtenida https://epson.com.co, consultada 12/11/2017

Es importante señalar que las impresoras antes señaladas se adquirieron nuevas, puesto que, el sistema de suministro de tinta se cataloga como una variable dependiente a la usanza de estos dispositivos. Esto significa que el uso y el desgaste de la impresora es una variable de interferencia que afecta la asociación de los hallazgos con un determinado patrón de impresión.

Materiales e instrumentos de análisis

- Microscopio estereoscópico binocular marca Amscope, referencia Se306r-p20 con objetivos de 2X y 4X.
- Cámara fotográfica Canon EOS REBEL T1i, resolución 15 megapixeles.

Criterios de inclusión de las muestras

- Las impresoras objeto de estudio se compraron para esta investigación, es decir, son nuevas y sin uso previo.
- La tinta de impresión es la original de fábrica y es acuosa.
- Papel Reprograf para impresión, color blanco, tamaño carta con gramaje de 75 gr x m2.
- Impresión de caracteres a color y a blanco y negro. Los párrafos siguieron el formato Arial con un tamaño 10 y una alineación justificada.
- Las muestras se obtuvieron de las impresoras Epson L120 y Epson XP-231.

Criterios de exclusión de las muestras

- No se utilizaron otros soportes fuera del papel Reprograf
- No se analizaron muestras diferentes a las obtenidas de las impresoras Epson L120 y Epson XP-231.

Tamaño de la muestra y etapas de análisis. La investigación aplicada se dividió en dos fases, la primera consistió en un prueba piloto para definir los alcances de las hipótesis planteadas, así como también las variables de observación, descripción y comparación para descartar o aceptar las mismas dentro de este trabajo. En la segunda, se emplearon los resultados obtenidos anteriormente. Para ambas etapas se definió una muestra estadística.

Prueba piloto-definición de la muestra. Las investigaciones que se han citado en este trabajo carecen de la definición de una muestra estadística, desconociéndose así, si sus conclusiones pueden generalizarse a partir de la misma o por el contrario, son relativas a la cantidad de material examinado. Como este estudio plantea unos objetivos orientados al análisis de patrones de impresión, es importante definir un número estadísticamente significativo para que los mismos se configuren.

Potencia 0,9

phi	r	27,1445
10,8578		

$$r = \frac{2a\sigma^2\phi^2}{b\Delta^2}$$

Alfa 0,05 error 0,05

Diferencia 0,2

phi 2,33

Tratamientos 2

La fórmula anterior se traduce así: r es el número de impresiones a sacar; "a" es el número de tratamientos, en este caso son dos, puesto que son dos impresoras; "b" es el número de niveles del factor de tratamiento, en este caso solamente hay 1 nivel; "delta" o es la diferencia mínima que se quiere detectar en la variable respuesta; "varianza" o es la varianza que se espera encontrar en la variable respuesta. En una investigación realizada anteriormente se pudo definir que esa varianza es de 0,05. Finalmente, "phi" o Φ, es un valor adimensional que depende de la potencia y el alfa que se busca.

La fórmula anterior fue planteada por Dean y Voss en 1999, en donde se tiene en cuenta, no solamente la varianza esperada, sino también la cantidad de tratamientos, la diferencia entre ellos y demás. Esta fórmula es bastante importante para calcular el número de muestra óptimo para ejercicios de diseño de experimentos como lo es este caso. Principalmente, va a tener una muestra para realizar la prueba piloto, en donde se definirán específicamente las variables de esta fórmula. Como conclusión, la muestra para la prueba piloto será de 27 réplicas por cada impresora, sin embargo, 10 de ellas bastaría para los análisis a realizar.

Luego, se trazó como estrategia de exploración, dividir el interior de cada réplica en cuatro cuadrantes: el número uno es el superior izquierdo, el número dos el superior derecho, el número tres es el inferior izquierdo y el número cuatro el inferior derecho. Los hallazgos de cada área se promediaron o contabilizaron según el caso. Producto de lo anterior se obtuvo un patrón de impresión (PI), *ver figura 5,* que permiten aceptar parcialmente la hipótesis planteada, puesto que, es una característica que se repite en diferentes réplicas configurándose así como un patrón. Éste se definió como:

PI-1 Presencia de gotas en zonas paragramáticas de los caracteres. Se entiende las gotitas ubicadas por fuera del carácter y que no forman parte del mismo. Este patrón no fue constante en las réplicas obtenidas de las dos impresoras, puesto que, sólo se observó en las impresiones a color.

Figura 5. Tabla de resultados obtenidos en la prueba piloto

Impresora	Réplica Blanco y Negro (BN) Color (C)	Número de gotas en zona paragramática Variable cuantitativa continua
1 L120	réplica 1 (BN)	0
1 L120	réplica 2 (C)	8
1 L120	réplica 3 (BN)	0
1 L120	réplica 4 (C)	7
1 L120	réplica 5 (BN)	0
1 L120	réplica 6 (C)	9
1 L120	réplica 7 (BN)	0
1 L120	réplica 8 (C)	11
1 L120	réplica 9 (BN)	0
1 L120	réplica 10 (C)	9
2 XP 231	réplica 1 (BN)	0
2 XP 231	réplica 2 (C)	1
2 XP 231	réplica 3 (BN)	0
2 XP 231	réplica 4 (C)	1
2 XP 231	réplica 5 (BN)	0
2 XP 231	réplica 6 (C)	2
2 XP 231	réplica 7 (BN)	0
2 XP 231	réplica 8 (C)	1
2 XP 231	réplica 9 (BN)	0
2 XP 231	réplica 10 (C)	3

Fuente: Elaboración del investigador (2018)

Segunda fase-definición de la muestra. Con los resultados obtenidos anteriormente y verificada parcialmente la hipótesis planteada, se procedió a calcular el tamaño muestral de réplicas necesarias para estimar constantes los patrones de impresión antes señalados. Por ello se aplicó lo siguiente:

	Datos		
Impresora	Cuenta de Réplica	Var de Presencia de gotas en zona paragramática	Variable cuantitativa continua
1 L120	27		3,43019943
2 XP 231	27		0,230769231
Total general	54		6,743885395

$$S^2 = \frac{\sum_{j=1}^{n} (X_j - \bar{X})^2}{n-1}$$

varianza 1 3,43019943

varianza 2 0,230769231

valor t 1,461117

$$n = (s_1^2 + s_2^2)\left(\frac{t_{\alpha,v}}{e}\right)^2$$

0,05	3126,266452	3126
0,1	781,566613	782
0,15	347,3629391	347
0,2	195,3916532	195
0,25	125,0506581	125

Error	Tamaño		Tamaño para cada impresora
0,05	3126	VERDADERO	1563
0,1	782	VERDADERO	391
0,15	347	FALSO	173
0,2	195	FALSO	97
0,25	125	FALSO	62

Para el cálculo de la muestra se debe tener en cuenta la varianza de las variables, el error permitido y el nivel de significancia. En este caso se tiene que la variable, número de gotas en zona paragramática, es la que mayor variabilidad tiene. Las dos variabilidades en la fórmula es la variabilidad de la impresora uno y la variabilidad de la impresora dos, esto permite recoger mayor información. Adicionalmente se usa un error de 15% tanto de error y de significancia, lo que lleva a calcular un tamaño de 173 réplicas para cada impresora.

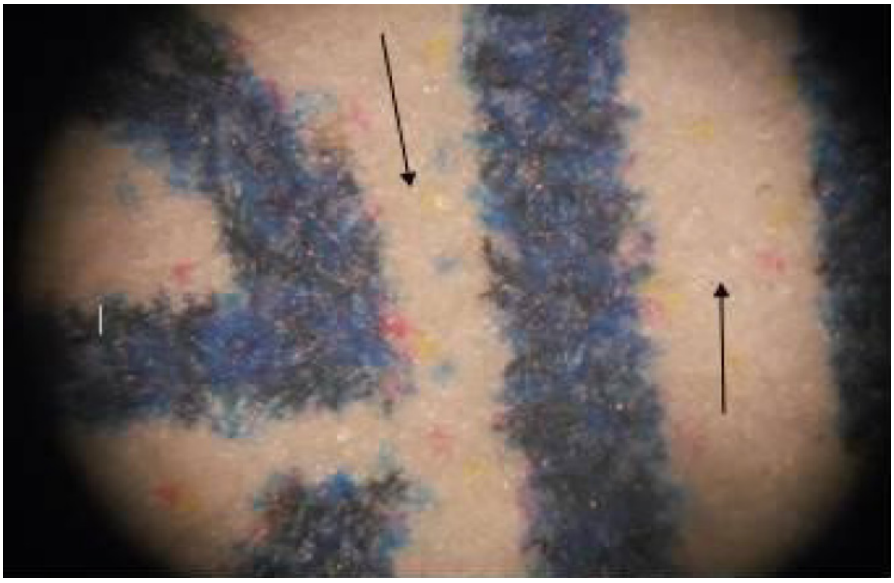
También se calculó el valor de distribución t, pues permite conocer la varianza de la variable, "número de gotas en zona paragramática", para cada impresora estudiada. Es así como la distribución depende del conocimiento de las varianzas poblacionales, si no se conocen se asume un sesgo, y por eso se escoge la distribución t.

Las observaciones y descripciones no variaron respecto a la prueba piloto, pues el PI-1 presenta el mismo comportamiento allí señalado, *ver figuras 6 y 7*. Esto puede estar asociado a las diferencias de presión manejadas en cada sistema de suministro

de tinta, los cuales son cartucho y recarga continúa. En ambos, al parecer, se controla bajo una misma constante la eyección de tinta cuando las impresiones son a blanco y negro, por ello no se observan gotas en las zonas paragramáticas de los caracteres.

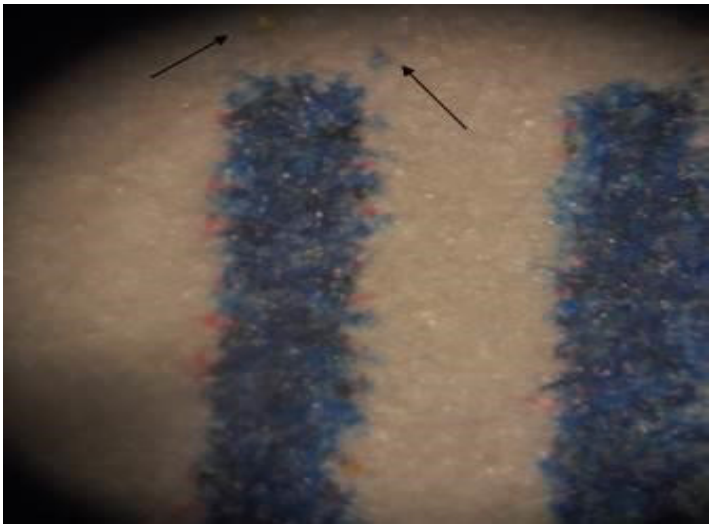
La situación antes planteada es diferente cuando las impresiones son policromáticas, puesto que, en las impresoras estudiadas se observan diferentes intensidades de presión, posiblemente, causadas por la interacción de las cuatro tintas (CMYK) en el cabezal de impresión. En el sistema de cartuchos se hallaron en promedio dos gotas en las zonas paragramáticas de los caracteres, en tanto en la recarga continua la media es de nueve gotas. Esta divergencia puede estar asociada a la misma estructura, puesto que, en el primero la tinta sólo experimenta la presión generada dentro del cartucho; mientras en el segundo, aparte de lo anterior, se produce una fuerza adicional cuando se requiere aprovisionamiento de tinta y ésta transita por las mangueras.

Figura 6. Réplica 183 de la impresora Epson L120, flechas negras señalan ubicación de varias gotas de tinta en zonas paragramáticas del carácter. Ampliación 2X



Fuente: Elaboración del investigador (2018)

Figura 7. Réplica 183 de la impresora Epson XP 231, flechas negras señalan ubicación de escasas gotas de tinta en zonas paragramáticas del carácter. Ampliación 2X



Fuente: Elaboración del investigador (2018)

2.5 Conclusiones

La hipótesis planteada consistente en: *La tecnología inkjet presenta dos formas para el suministro de tinta, ya sea mediante recarga continua o a través de cartuchos, las cuales configuran procesos mecánicos disímiles entre sí. Cuando un documento es impreso, transita por uno u otro sistema de abastecimiento, traspasándoles a éste sus respectivos patrones de impresión. Lo anterior está en concordancia con los principios de producción, transferencia, correspondencia e identidad de la criminalística*. La conclusión de esta investigación es que la hipótesis es parcialmente aceptada por cuanto el Patrón de Impresión-1 (PI-1) permitió, mediante el análisis de las muestras impresas a color, identificar y discriminar el sistema de suministro de tinta empleado por las impresoras EPSON estudiadas.

En el estudio se escogieron las impresoras inkjet de la marca Epson porque son las más utilizadas mundialmente en el ámbito comercial junto Hewlett Packard, Brother, Canon y Lexmark. En igual sentido, en la literatura académica también ocupan un lugar importante, por cuanto las falsificaciones actuales se realizan mediante estos dispositivos, convirtiéndose así en objeto de estudio de las pericias documentológicas.

El número de gotas en las zonas paragramáticas de los caracteres es un patrón, posiblemente asociado al sistema de suministro de tinta y no al desgaste

de las impresoras; por cuanto, las mismas se adquirieron nuevas para este estudio. Se realizaron 183 impresiones en cada impresora y el PI-1 no sufrió modificación alguna.

El sistema de cartuchos y recarga continua experimentan, al parecer, la misma presión cuando las impresiones son a blanco y negro; sin embargo, cuando éstas son a color se configuran diferentes intensidades, traducidas en la cantidad de gotas presentes en las zonas paragramáticas de los caracteres. Significa lo anterior que en el campo pericial el PI-1 sólo permite discriminar elementos dubitados que presenten impresiones a colores, por cuanto en las muestras en blanco y negro dicho patrón no es observable.

Los resultados obtenidos son la antesala a posteriores investigaciones dirigidas a potencializar los exámenes descriptivos y comparativos, puesto que, estos últimos, permiten observar y documentar patrones de impresión que permitan diferenciar muestras analizadas.

El sistema de abastecimiento de tinta de las impresoras inkjet deja patrones de impresión en documentos que tienen más de un color en su elaboración, los cuales son perceptibles en el estereomicroscopio y se constituyen en un elemento descriptivo y comparativo para discriminar en el ámbito pericial muestras cuestionadas.

Los análisis no destructivos, como el presente caso, permiten obtener información valiosa en el estudio de documentos cuestionados. Esto, para la Documentología Forense, es un paso de suma importancia para coadyuvar a la administración de justicia sobre este punto, lugar que indiscutiblemente y con avances muy significados ha estado reservado a los estudios invasivos propuestos desde la Química Analítica con aplicación forense. Estos análisis presentan las siguientes críticas: en primer lugar, se pretende diferenciar la tinta mediante su composición elemental, cuando el mercado de dicha sustancia presenta muchas fórmulas químicas, las cuales son similares entre los fabricantes; segundo, se requiere extracción de la muestra y por ende alteración del soporte, lo que supondría en Colombia la afectación del principio de mismidad que garantiza la cadena de custodia; tercero, se requiere equipos instrumentales que son costosos, tanto para adquirirlos como su mantenimiento, y requieren profesionales idóneos para su manejo mediante capacitación (Ferreira et al., 2015).

La Documentología Forense mediante la aplicación de su enfoque disciplinar puede producir conocimiento científico que permita a la administración de justicia operar en los delitos relacionados con la falsificación documental, por cuanto las partes dentro de un proceso judicial, especialmente el penal, podrán generar en el juzgador conocimiento más allá de duda razonable respecto a este tipo hechos punibles. Esto desde el punto de vista jurídico, ahora bien, desde la óptica pericial, los resultados de este trabajo le permitirán a los expertos disponer de una unidad de análisis más para discriminar entre muestras dubitadas.

2.6 Referencias Bibliográficas

Agnieszka, k., Małgorzata, K., Wietecha-Posłuszn, R., Woźniakiewicz, M., & Kościelniak, P. (2014). Application of CE-MS to examination of black inkjet printing inks for forensic purposes (Disponible en https://doi.org/10.1016/j.talanta.2014.04.004). *Talanta, 128*, 92101.

Akao , Y., Kobayashi, K., & Seki, Y. (2005). Examination of Spur Marks Found on Inkjet-printed Documents (Disponible en www.astm.org). *Journal of Forensic Sciences, 50*, 1-9.

Allain, L., Stratis-Cullum, D., & Vo-Dinh, T. (2004). Investigation of microfabrication of biological sample arrays using piezoelectric and bubble-jet printing technologies. *Analytica Chimica Acta (Disponible en https://doi.org/10.1016/j.aca.2004.04.065), 518*, 77-85.

Amatoa , F., Cozzolinoa , G., Moscatoa , V., & Moscato, F. (2019). Analyse digital forensic evidences through a semantic-based methodology and NLP technique. *Future Generation Computer Systems (Disponible enhttps://doi.org/10.1016/j.future.2019.02.040)*, 297-307.

Arbouine, M., & Day, S. (1994). The use of drum defects to link laser-printed documents to individual laser printers . *Journal of the Forensic Science, 34*, 99-104.

Bai, R., Zhang, L., Liu, Y., Meng, L., Wang, L., Wu, Y., … Chen, C. (2010). Pulmonary responses to printer toner particles in mice after intratracheal instillation. *Toxicology Letters*, *199*(3), 288–300. http://doi.org/10.1016/j.toxlet.2010.09.011

Biedermann, A., Taroni, F., Bozza, S., & Mazzella, W. D. (2011). Implementing statistical learning methods through Bayesian networks (Part 2): Bayesian evaluations for results of black toner analyses in forensic document examination. *Forensic Science International*, *204*(1-3), 58–66. http://doi.org/10.1016/j.forsciint.2010.05.001

Braz, A., López-López, M., & García-Ruiz, C. (2013). Raman spectroscopy for forensic analysis of inks in questioned documents. *Forensic Science International*, *232*(1-3), 206–12. http://doi.org/10.1016/j.forsciint.2013.07.017.

Byeon, J. H., & Kim, J.-W. (2012). Particle emission from laser printers with different printing speeds. *Atmospheric Environment*, *54*, 272–276. http://doi.org/10.1016/j.atmosenv.2012.02.002.

Calcerrada, M., & García Ruiz, C. (2015). Analysis of questioned documents: a review (Disponible en http://doi.org/10.1016/j.aca.2014.10.057). *Analytica Chimica Acta, 853*, 143–166.

Chu, P. C., Cai, B. Y., Tsoi, Y. K., Yuen, R., Leung, K. S. Y., & Cheung, N. H. (2013). Forensic analysis of laser printed ink by X-ray fluorescence and laser-excited plume fluorescence. *Analytical Chemistry*, *85*, 4311–4315. http://doi.org/10.1021/ac400378q

Cruces-Blanco, C., Gámiz–Gracia, L., & García-Campaña, A. M. (2007). Applications of capillary electrophoresis in forensic analytical chemistry. *TrAC Trends in Analytical*

Chemistry, *26*(3), 215–226. http://doi.org/10.1016/j.trac.2006.12.007

Daly, R., Harrington, T., Martin , G., & Hutchings , I. (2015). nkjet printing for pharmaceutics – A review of research and manufacturing. *International Journal of Pharmaceutics (Disponible en https://doi.org/10.1016/j.ijpharm.2015.03.017), 494* , 554-567.

Darahuge, M., & Arellano González, L. (2011). La problemática de la informática forense. En M. E. Darahuge, & L. Arellano González, *Manual de informática forense* (págs. 5-9). Buenos Aires : Errepar.

Dasari, H., & Bhagvati, C. (2006). Identification of Printing Process Using HSV Colour Space.

In P. J. Narayanan, S. K. Nayar, & H.-Y. Shum (Eds.), *Computer Vision – ACCV 2006* (pp.

692–701). China: Springer. Retrieved from http://goo.gl/46ZPe0

De Almeida, M., Correa, D., Rocha, W., Scafi, F., & Pop, R. (2013). Discrimination between authentic and counterfeit banknotes using Raman spectroscopy and PLS-DA with uncertainty estimation. *Microchemical Journal (Disponible en https://doi.org/10.1016/j.microc.2012.03.006), 109*, 170-177.

Ezcurra Gondra, M., & Grávalos, G. (2010). *Análisis forense de documentos: instrumentos de escritura manual y sus tintas.* Buenos Aires: Ediciones La Roca.

Ezcurra Gondra, M., & Grávalos, G. (2012). *Análisis forense de documentos: sistemas de impresión y sus tintas.* Buenos Aires: Ediciones La Roca.

Ferreira, A., Navarro, L. C., Pinheiro, G., dos Santos, J. A., & Rocha, A. (2015). Laser printer attribution: exploring new features and beyond. *Forensic Science International*, *247*, 105–

25. http://doi.org/10.1016/j.forsciint.2014.11.030

Gómez Galán, A. (2013). *Materias y productos en impresión. ARGI0310.* Málaga: IC Editorial.

Guo, Y., Patanwala, H., Bognet, B., & Ma, A. (2017). Inkjet and inkjet-based 3D printing:

connecting fluid properties and printing performance. *Rapid Prototyping Journal (Disponible en https://doi.org/10.1108/RPJ-05-2016-0076), 23*, 562-576.

Heudt, L., Debois , D., Zimmerman, T., Köhler , L., Bano, F., Partouche, F., . . . Pauw, E. (2012). Raman spectroscopy and laser desorption mass spectrometry for minimal destructive forensic analysis of black and color inkjet printed documents (Disponible en https://doi.org/10.1016/j.forsciint.2011.12.001). *Forensic Science International, 219*, 6475.

Hoath, S., & Hutchings , I. (2008). Inkjet printing-The physics of manipulating liquid jets and drops (Disponible en https://www.researchgate.net/publication/231100170) . *Journal of Physics Conference Serie*, 1-16.

Hudd, A. (2010). Inkjet Printing Technologies. En S. Magdassi, *Chemistry Of Inkjet Inks (Disponible en EBSCO Discovery Service)* (pág. 345). Singapore: World Scientific Publishing.

Khanna, N., Mikkilineni, A. K., Chiu, G. T. C., Allebach, J. P., & Delp, E. J. (2008). Survey of scanner and printer forensics at Purdue University. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5158 LNCS*, 22–34. http://doi.org/10.1007/978-3-540-85303-9_3

Król, M., Karoly, A., & Kościelniak, P. (2014). Raman spectroscopy and capillary electrophoresis applied to forensic colour inkjet printer inks analysis. *Forensic Science International (Disponible en https://doi.org/10.1016/j.forsciint.2014.06.031), 242*, 142-149. Obtenido de Raman spectroscopy and capillary electrophoresis applied to forensic colour inkjet printer inks analysis: https://doi.org/10.1016/j.forsciint.2014.06.031

Kula, A., Król, M., Wietecha-Posłuszn, R., Woźniakiewicz, M., & Kościelniak, P. (2014). Application of CE-MS to examination of black inkjet printing inks for forensic purposes. *Talanta (Disponible en https://doi.org/10.1016/j.talanta.2014.04.004), 128*, 92-101.

Kumar, R., Kumar, V., & Sharma, V. (2017). Fourier transform infrared spectroscopy and chemometrics for the characterization and discrimination of writing/photocopier paper types: Application in forensic document examinations. *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy (Disponible en https://doi.org/10.1016/j.saa.2016.06.042), 170*, 19-28.

Kwon, K.-S., Choi , Y.-S., & Go, J.-K. (2013). Physical Inkjet jet failures and their detection using piezo self-sensing. *Sensors and Actuators A (Disponible en https://doi.org/10.1016/j.sna.2013.07.027), 201*, 335-341.

Kwon, O.-S., Kim, H., Ko, H., Lee, J., Lee, B., Jung, C.-H., . . . Shin, K. (2013). Fabrication and characterization of inkjet-printed carbon nanotube electrode patterns on paper. *Carbon (Disponible en https://doi.org/10.1016/j.carbon.2013.02.039), 58*, 116-127.

Kwon, K.-S. (2009). Measurement Speed measurement of ink droplet by using edge detection techniques. *Measurement (Disponible en https://doi.org/10.1016/j.measurement.2008.03.016), 42*, 44-50.

LaFrance, A. (08 de 05 de 2014). *The Atlantic*. Recuperado el 10 de 11 de 2017, de How Inkjet Printers Are Changing the Art of Counterfeit Money: https://www.theatlantic.com/technology/archive/2014/05/how-inkjet-printers-arechanging-the-art-of-counterfeit-money/361946/

LaPorte,, G., & Ramotowski, R. (2003). The Effects of Latent Print Processing on Questioned Documents Produced by Office Machine Systems Utilizing Inkjet

Technology and Toner. *Journal forensic sciences (disponible en www.astm.org), 48*(3), 1-6.

LaPorte, G. (2004). The Use of an Electrostatic Detection Device to Identify Individual and Class Characteristics on Documents Produced by Printers and Copiers—A Preliminary Study (Disponible en www.astm.org) . *Journal of Forensic Sciences, 49*, 610-620.

Lennard, C., El-Deftar, M., & Robertson, J. (2015). Forensic application of laser-induced breakdown spectroscopy for the discrimination of questioned documents. *Forensic Science International (Disponible en https://doi.org/10.1016/j.forsciint.2015.07.003), 254*, 68-79.

McCleery, B. (12 de 03 de 2013). *Usa Today*. Recuperado el 10 de 11 de 2017, de Inkjet and color printers make printing fake bills easier than ever:

https://www.usatoday.com/story/news/nation/2013/03/12/counterfeit-money-onrise/1983067/

Noronha, S., Basheer, S., Vijay, M., Alnajjar, A., Sharma, B., & Singh , N. (2017). Comparative Study of Different Printed Documents to Estimate the Type of Printer Used (Disponible en http://www.jscholaronline.org/articles/JFRC/A-Comparative-Study-of-DifferentPrinted-Documents.pdf). *Journal of Forensic Research and Crime Studies, 2*, 1-7.

Orellana Wiarco, O., & Orellana Trinidad, O. (2013). *Grafoscopía: autenticidad o falsedad de manuscritos y firmas* . México: Porrúa.

Shang, S., Memon, N., & Kong, X. (2014). Detecting documents forged by printing and copying. *EURASIP Journal on Advances in Signal Processing*, *2014*(1), 140. http://doi.org/10.1186/1687-6180-2014-140.

Singh Saroa, J., & Saini, K. (2013). Physical examination of PhotocoPied documents (Disponible en http://www.forensicscience.pl). *Problems of Forensic Sciences, 94*, 485–501.

Skenderović Božičević, M., Gajović, A., & Zjakić, I. (2012). Identifying a common origin of toner printed counterfeit banknotes by micro-Raman spectroscopy. *Forensic Science International (Disponible en https://doi.org/10.1016/j.forsciint.2012.10.007), 223*, 314320.

Spagnolo, G. S. (2006). Potentiality of 3D laser profilometry to determine the sequence of homogenous crossing lines on questioned documents. *Forensic Science International*, *164*(2-3), 102–9. http://doi.org/10.1016/j.forsciint.2005.12.004

Subedi, K., Trejos, T., & Almirall, J. (2015). Forensic analysis of printing inks using tandem Laser Induced Breakdown Spectroscopy and Laser Ablation Inductively Coupled Plasma Mass Spectrometry. *Spectrochimica Acta Part B: Atomic Spectroscopy (Disponible en https://doi.org/10.1016/j.sab.2014.11.011), 103–104*, 76-83.

Szafarska, M., Wietecha-Posłuszny, R., Woźniakiewicz, M., & Kościelniak, P. (2011a). Examination of colour inkjet printing inks by capillary electrophoresis. *(Disponible en https://doi.org/10.1016/j.talanta.2010.12.024), 84* , 1234-1243.

Szafarska, M., Wietecha-Posłusznya, R., Woźniakiewicz, M., & Kościelniak, P. (2011b). Application of capillary electrophoresis to examination of color inkjet printing inks for forensic purposes. *Forensic Science International (Disponible en https://doi.org/10.1016/j.forsciint.2011.05.017), 212* , 78-85.

Trejos, T., Flores, A., & Almirall, J. R. (2010). Micro-spectrochemical analysis of document paper and gel inks by laser ablation inductively coupled plasma mass spectrometry and laser induced breakdown spectroscopy. *Spectrochimica Acta Part B: Atomic Spectroscopy*, *65*(11), 884–895. http://doi.org/10.1016/j.sab.2010.08.004

Trejos, T., Corzo, R., Subedi, K., & Almiral, J. (2014). Characterization of toners and inkjets by laser ablation spectrochemical methods and Scanning Electron Microscopy-Energy Dispersive X-ray Spectroscopy. *Spectrochimica Acta Part B (Disponible en https://doi.org/10.1016/j.sab.2013.11.004), 9*(22), 9-22.

Velásquez Posada, L. G. (2004). *Falsedad documental y laboratorio forense.* Medellín: Señal Editora.

Wensing, M., Schripp, T., Uhde, E., & Salthammer, T. (2008). Ultra-fine particles release from hardcopy devices: sources, real-room measurements and efficiency of filter accessories. *The Science of the Total Environment*, *407*(1), 418–27. http://doi.org/10.1016/j.scitotenv. 2008.08.018

Ying-jianXu, Xin-xinZhou , & Xiao-fanShi. (2016). HPLC and HPLC/MS analysis of red ink on counterfeit 100-yuan notes. *Forensic Science International (Disponible en https://doi.org/10.1016/j.forsciint.2015.11.018), 259*, 47-52.

3 Fotografía Forense Digital en la Escena del Hecho Forensic Digital

Autores
María Belén Álvarez Cestona
Bruno Constanzo.

Resumen

En los últimos años, la fotografía experimentó una revolución de la mano de los sensores de imágenes digitales, que reemplazaron a las películas fotográficas y su proceso químico abriendo nuevas posibilidades. Sin embargo, esta rama de la criminalística no se ha actualizado completamente y no se aprovechan las fortalezas del medio digital. En este capítulo, se presenta un estudio detallado del estado de la fotografía forense, sus técnicas, herramientas y objetivos. A partir, de la teoría básica de las imágenes digitales, se relacionan estos conceptos para brindar un marco teórico/práctico actualizado de la fotografía forense digital. Además, se plantea la aplicación de técnicas y algoritmos de procesamiento y análisis de imágenes digitales, brindando nuevas herramientas que ayuden a los criminalistas. Más importante aún, se propone una Guía de Buenas Prácticas que tiene en cuenta las características particulares de la fotografía digital, y, por lo tanto, los guía en la obtención de registros fotográficos de mayor utilidad y mejor calidad. Esta guía se refuerza, gracias a la experimentación mediante casos de estudios donde se implementa, como así también, las herramientas analizadas para verificar su utilidad en situaciones concretas.

Palabras claves: *Fotografía forense - Imágenes digitales – Guía de buenas prácticas - Procesamiento de imágenes.*

Abstract:

In recent years, photography has undergone a revolution at the hands of digital image sensors, which have replaced photographic films and their chemical process, opening up new possibilities. However, this branch of criminalistics has not been fully updated and the strengths of the digital media are not taken advantage of. In this chapter, a detailed study of the state of forensic photography, its techniques, tools and objectives is presented. From the basic theory of digital images, these concepts are related to provide an updated theoretical / practical framework of digital forensic photography. In addition, the application of techniques and algorithms for processing and analysis of digital images is proposed, providing new tools that help criminal investigators. More importantly, a Good Practice Guide is proposed that considers the particular characteristics of digital photography, and therefore, guides them in obtaining photographic records of greater utility and better quality. This guide is reinforced, thanks to experimentation through case studies where it is implemented, as well as the tools analyzed to verify its usefulness in specific situations.

Keywords: *Forensic photography – Digital images – Best practices guideline – Image processing.*

Introducción

La fotografía forense es la disciplina que tiene por objeto la documentación gráfica de las condiciones en las que se encuentra el lugar de los hechos o de todos los indicios localizados en él.

La correcta preservación de la escena del hecho por medios fotográficos es de suma importancia, ya que registra el estado del lugar y los indicios presentes en él. Una mala preservación, al contrario, traerá inconvenientes y complejidades adicionales para el estudio posterior que deben llevar a cabo los especialistas. El objetivo final es colaborar con el esclarecimiento de los hechos a través de las imágenes tomadas en el lugar, y brindar apoyo a la investigación.

En un principio, se plantea la idea de poder implementar una mejora sobre la fotografía, sin alteraciones, para que esta pueda tener utilidad en el Juicio Oral.

Se tuvieron en cuenta las siguientes problemáticas como eje de este trabajo:

1. ¿Cómo realizar mejoras sobre una fotografía manteniendo su valor jurídico?
2. ¿Se pueden implementar nuevas tecnologías en el ámbito de la fotografía forense? Para esto se plantearon como objetivos primordiales:

   Incorporar mejoras en una fotografía a nivel informático.

   Agregar herramientas necesarias para lograr una correcta optimización de la fotografía y que ésta posea utilidad en juicio oral.

   Reproducir los errores más comunes en casos de estudio, haciendo prueba de las herramientas y analizar su funcionalidad.

   Desarrollar y proponer una Guía de Buenas Prácticas para los profesionales, a fin de mejorar las fotografías tomadas en la escena, además de su calidad y valor probatorio.

3.1 Metodología

1. Se formuló una guía de buenas prácticas, con los principios básicos de la toma fotográfica, para que de esta manera, el especialista lo pueda consultar antes de arribar a la escena y recibir las recomendaciones básicas para proceder ante ella.

2. Se realizó una selección de fotografías brindadas por especialistas de escenas del crimen, junto con una búsqueda exhaustiva de diferentes técnicas y algoritmos de procesamiento de imágenes que serían de ayuda para mediciones y mejoras, a fin de seleccionar las más adecuadas para salvaguardar los errores más comunes, presentes en la fotografía forense.

3. Se armaron casos de estudio sobre escenas del crimen, tomando imágenes de referencia, para analizar con qué algoritmos y herramientas de procesamiento de imágenes se podrían compensar sus deficiencias. Los recursos utilizados fueron:

    - Fotografías de escenarios del crimen brindadas por los especialistas.
    - Búsqueda de softwares informáticos o complementos de software existente para el procesamiento de imágenes.
    - Fotografías tomadas por los autores en casos de estudio.

3.2 Marco Conceptual

3.2.1 Fotografía:

El término fotografía procede del griego y quiere decir "diseñar o escribir con luz". Se denomina fotografía al proceso de capturar imágenes mediante algún dispositivo tecnológico sensible a la luz, que se basa en el principio de la cámara oscura. El sistema original de fotografía que se mantuvo hasta hace algunos años actuaba con películas sensibles con el propósito de almacenar la imagen capturada para luego imprimirla.

Una cámara fotográfica es un dispositivo utilizado para capturar imágenes o fotografías. En los comienzos, se usaba la cámara oscura, la cual es un mecanismo antiguo, que data del siglo XVI, para proyectar imágenes, en el que una habitación entera desempeñaba las mismas operaciones que una cámara fotográfica actual por dentro, con la diferencia de que en aquella época no había posibilidad de guardar la imagen a menos que ésta se trazara manualmente. Las cámaras actuales se combinan con elementos sensibles (películas o sensores) al espectro visible o a otras porciones del espectro electromagnético, y su uso principal es capturar la imagen que se encuentra en el campo visual.

Las cámaras fotográficas constan de una cámara oscura cerrada, con una abertura en uno de los extremos para que pueda entrar la luz, y una superficie

plana de formación de la imagen o de visualización para capturar la luz en el otro extremo. La mayoría de las cámaras fotográficas tienen un objetivo formado de lentes, ubicado delante de la abertura de la cámara fotográfica para controlar la luz entrante y para enfocar la imagen, o parte de la imagen. El diámetro de esta abertura (conocido como apertura) suele modificarse con un diafragma, aunque algunos objetivos tienen apertura fija.

Mientras que la apertura y el brillo de la escena controlan la cantidad de luz que entra por unidad de tiempo en la cámara durante el proceso fotográfico, el obturador controla el lapso en que la luz incide en la superficie de grabación. Por ejemplo, en situaciones con poca luz, es necesario utilizar una velocidad de obturación menor, para que el objetivo permanezca abierto una mayor cantidad de tiempo con el objeto de permitir que la película reciba la cantidad de luz necesaria para asegurar una exposición correcta.

Se entiende por fotografía al acto mediante el cual una persona, a través del uso de una cámara fotográfica preparada para reflejar la realidad que se observa a partir del uso de lentes y del trabajo con la luz, retrata un instante o momento particular de la vida. La fotografía tiene como característica que genera una imagen que sirve como recuerdo de ese momento que tal vez no vuelva a repetirse y que, además, es visto y comprendido a través de los ojos de quien saca la fotografía, lo cual puede hacer que esa imagen también se vuelva irrepetible por ese hecho ya que nadie tal vez vuelva a tener la misma mirada.

3.2.2 Tipos de cámaras fotográficas

- Cámara Oscura: consistía en una especie de caja cerrada cuya única fuente de luz era un pequeño orificio practicado en uno de los laterales, por donde entraban los rayos luminosos reflejando los objetos del exterior en una de sus paredes. El orificio funciona como una lente convergente y proyecta en la pared opuesta, la imagen del exterior invertida tanto vertical como horizontalmente.

- Cámara Analógica: Los rayos que refleja el sujeto son refractados por un objetivo que, a través del obturador, los proyecta en la película, sobre la que forma una imagen boca abajo y lateralmente invertida. Cuando el obturador se dispara, la luz incide sobre la película durante un tiempo que depende de la velocidad del obturador.

- Cámara Digital: es una cámara fotográfica que, en vez de captar y almacenar fotografías en película química como las cámaras de película fotográfica, utiliza un sensor de imagen digital para generar y almacenar imágenes.

- Cámara Réflex: las cámaras réflex digitales están divididas en dos componentes separados: el cuerpo de la cámara como tal, y el objetivo, que es intercambiable. El objetivo contiene, por lo general, un mecanismo para la regulación de la luz, el diafragma y un mecanismo de enfoque. El cuerpo de la cámara contiene un espejo, ubicado a 45° respecto al plano de la imagen, cuya función es desviar los rayos hacia un pentaprisma. A su vez, la función de este es desviar la imagen hacia el observador y enderezarla, puesto que el objetivo la proyecta de forma invertida. En el momento del disparo, el espejo se levanta y se abre el mecanismo obturador, para dejar pasar los rayos de luz directamente hacia el dispositivo de captura (el cual es un sensor o película de imagen digital).

- Cámara compacta: es una cámara fotográfica sencilla cuyo objetivo no es desmontable. Las cámaras compactas suelen ser más sencillas de manejar que las cámaras Réflex y más económicas. Normalmente su funcionalidad está limitada en comparación con las réflex, aunque suelen ser más ligeras y fáciles de transportar, lo que las hace ideales para llevarlas de viaje. Se clasifican en digital (con sensor y almacenas fotografías electrónicamente) o APS (con película).

3.2.3 Partes y funciones de la cámara fotográfica

Toda cámara posee una abertura en su parte frontal y, en su parte posterior, el material que va a ser impresionado por la luz. Al mismo tiempo, está compuesta por:

- Caja o cuerpo de la cámara: Estuche cerrado a la luz que constituye el cuerpo de la cámara.

- Película: Material fotosensible que experimenta una alteración química cuando

- es iluminado. Esta modificación es la que guarda la información visual del objeto en cada fotografía. Hay diferentes tipos de películas y varios formatos que determinan las características requeridas del conjunto de rayos necesario.

- Sensor: es el elemento que detecta y captura la información que compone la imagen. Esto se logra al convertir la atenuación de las ondas de luz (cuando estas atraviesan o son reflejadas por cuerpos) en señales eléctricas. Las ondas capturadas por el sensor pueden ser luz u otro tipo de radiación electromagnética.

- Diafragma: Dispositivo a base de laminillas móviles intercaladas, que se cierran para dejar paso a la luz para que la película se pueda imprimir. El diafragma regula esa luz según unos números que pertenecen a las distintas aberturas. Cuanto mayor sea la apertura, dichos números son menores.
- Obturador: Regula el tiempo que actúa la luz sobre la película sensible. Existen dos tipos:

  Central: Cuando está situado en el propio objetivo.

  De cortinilla o plano focal: Cuando está colocado ante la película, como parte de la propia cámara y no del objetivo. Corrientemente, cuanta más luz haya, menor será la abertura.
- Visor: Pequeña ventana para mirar por ella, puede tener una lente propia o utilizar un aparato que le permita ver a través del cuerpo de la cámara. Gracias a él, el fotógrafo ve y compone el tema.
- Objetivo: Reproduce, sobre la película, el motivo. Estos pueden acoplarse a las cámaras. Hay de varios tipos, los cuales diferencia por su distancia focal:
- Flash: Su función es iluminar objetos sin luz, o con luz insuficiente. El flash se desarrolló desde los primitivos sistemas que recurrían a la explosión de polvos de magnesio hasta las modernas bombillas y dispositivos electrónicos, que controlan la intensidad lumínica requerida.

Diafragma, obturador y lentes hacen posible la proyección de la imagen sobre el material sensible de una manera adecuada. Para que esto ocurra es preciso ajustar la distancia entre las lentes del objetivo y la película. Esta distancia es variable según la cercanía o alejamiento del objeto por fotografiar respecto de la cámara. De esta manera, existe una relación numérica en el objetivo, a través de la cual el experto ajusta la imagen a la distancia. Algunas cámaras automáticas pueden realizar por sí solas esta operación.

También es primordial señalar otros elementos de la cámara, como por ejemplo la profundidad de campo, que se vincula con el intervalo de distancias dentro del cual la imagen por fotografiar resulta bien definida en el enfoque. Esta será menor cuanto más abierto esté el diafragma, y mayor, a medida que se cierre.

Otros elementos que pueden formar parte de la cámara son los filtros, que cambian la forma en que una película registra colores o valores tonales. Los filtros son discos de cristal y gelatina que se colocan delante del objetivo que pueden estar

coloreados en función del efecto que se persigue. Existen diferentes tipos, como los polarizados, que corrigen el efecto de los reflejos; los ultravioletas, que absorben los rayos ultravioletas; y los infrarrojos, que se usan para hacer visibles efectos pobremente iluminados para la visión común.

3.2.4 Fotografía forense:

La Fotografía Forense es una técnica auxiliar de la investigación criminal que permite fijar y reproducir imágenes de personas, lugares y objetos que estén relacionados con hechos sujetos a investigación pericial. De esta forma, permite ilustrar escenas y demás elementos que requieren los investigadores, autoridades, jueces, fiscales, peritos y demás expertos para contar con un registro gráfico de lo sucedido[12].

Su propósito, además de complementar los informes periciales y auxiliar a los órganos que procuran justicia, es ayudar a las otras ciencias forenses sirviendo de apoyo para crear bases de datos e identificación de personas, tatuajes, señas particulares, armas de fuego, casquillos, proyectiles, entre otros.

En el caso de hechos delictivos el suceso no acaba en el momento en que los investigadores procesan la escena, ya que una vez levantados todos los indicios, los investigadores deben realizar una secuencia fáctica de lo sucedido. La fotografía puede utilizarse, también en otras instancias, tal es el caso de vigilancias o seguimientos a sujetos en determinadas investigaciones y que deban documentarse para luego ser presentadas como pruebas.

En todos los casos, la fotografía debe cumplir con dos requisitos fundamentales: exactitud y nitidez, entendiendo a la exactitud como el ajuste completo o fidelidad de un dato, cálculo, medida, expresión y a la nitidez como la relación con la calidad de la imagen.

Hay varios aspectos a tener en cuenta a la hora de realizar un levantamiento fotográfico, en primer lugar, el fotógrafo debe ser completamente neutral y limitarse únicamente a tomar la foto sin alterar lo que está viendo. Además, en el informe se debe indicar fecha, hora y descripciones de cada foto. Las descripciones deben ser objetivas, no deben incluir hipótesis ni inclinarse hacia ninguna de las partes involucradas en el hecho. Se recomienda la toma de diferentes imágenes de un mismo objeto, con flash y sin flash, de diferentes ángulos, fotos panorámicas y de acercamiento.

12 Andrea Castellón Sossa. Disponible en: https://criminologiacr.com/2015/02/24/fotografia-forense/

Se detallan a continuación indicaciones básicas para la toma de fotos:

1. Fotografiar áreas exteriores de la escena, siempre y cuando éstas tengan relevancia para la investigación. Se recomienda ubicar puntos de referencia importantes, como edificios, casas o comercios, esto servirá para que el investigador pueda identificar posibles testigos del hecho o la reconstrucción posterior de la escena.

2. Ubicar vías de acceso y huida, como puertas y ventanas, calles, techos, escaleras.

3. En el caso de existir personas fallecidas, se debe mostrar su ubicación dentro de la escena y su relación con los demás objetos. Se recomienda detallar las heridas presentes en el cuerpo o cualquier otro detalle de relevancia en la investigación. También se debe tomar fotos cuando el cuerpo está siendo movido ya que pueden encontrarse más indicios debajo del cuerpo que se perderán una vez que el cuerpo haya sido retirado del sitio.

4. Se deben fotografiar todos los indicios físicos que se ubiquen dentro de la escena.

Para el caso de fotografías de seguimiento o vigilancia, se requiere de una técnica más especializada, ya que las fotos deben tomarse a cierta distancia para evitar poner en alerta al objetivo. Tal como se indicó anteriormente, estas deben ser muy claras y nítidas para evitar confusiones posteriores, a fin de crear un contexto de la escena para posteriores análisis, como comercios, casas o edificios a los que ingresa el sujeto de investigación, número de calles, avenidas, placas, personas con las que entra en contacto.

Dentro del procesamiento de la escena del crimen, pueden pasar inadvertidos ciertos elementos, por no ser perceptibles a simple vista humana. Por esto, la fotografía ayuda a captar y mostrar el estado original en que se encontró el lugar de los hechos, brindando registros tangibles y verificables para la validez de los elementos materiales y físicos, que pueden llegar a revelar indicios y constituirse como un medio de prueba.

La fotografía, de esta manera, se convierte en un documento fijo e inmutable, objetivo e imparcial. En su estudio sobre las imágenes en las escenas del crimen, Gustavo Infantes, establece que:

> La fotografía forense, tiene como objetivo la fiel documentación de las evidencias materiales (objetos, rastros, huellas, entre otros) a fin de coadyuvar

> en la investigación y la fiel interpretación de la realidad de los hechos criminales. El fotógrafo debe documentar indiscutiblemente todo cuanto se relaciona con la escena del delito y sus adyacencias, antes de que se toque o remuevan los indicios o se modifiquen las condiciones de la escena; documentar fotográficamente la totalidad del lugar y también realizar tomas a detalle. La técnica determina la obtención de todas las fotografías necesarias, que puedan describir por sí sola el escenario del suceso, elementos, y todo aspecto relevante para la investigación[13].

El registro fotográfico debe ser organizado y representado por la toma de lo general a particular. La evidencia fotográfica debe ser tratada en la misma forma de preservación y protección[14], como cualquier otra forma de evidencia. Sirve para complementar las descripciones escritas, como en el caso de los Planos (Planimetría Forense) realizados. Es un elemento de prueba jurídica y es el elemento clave para todo equipo forense. Conserva las constataciones hechas en el lugar (Escena del Crimen). La Fotografía Forense busca:

- Fijar el sitio de suceso donde ocurrió el Crimen, de lo General a lo Particular.
- Fijación de las Evidencias encontradas.

Es importante considerar que sólo una vez se tiene acceso a la escena del crimen, por tal motivo al entrar en ella el criminalista tiene que asegurar el área y preservarla, de modo que el perito en fotografía realice sus tomas plasmando en ellas el escenario original del lugar y demás objetos sospechosos, antes de que las cosas y objetos marcados como indicios sean palpados, levantados o trasladados del lugar. Se debe prestar atención a cualquier indicio por insignificante que parezca, enfocar y capturarlo, que cada fotografía describa por si sola lo ocurrido. La ventaja de las fotografías, es que pueden ser estudiadas una y otra vez, de modo que, si en un primer instante se escapó algún detalle, más adelante es posible percibirlo.

---

13 Teleley. Infantes Aragón, Gustavo. Imágenes en las escenas del crimen. Perú. 2009. http://www.teleley.com/articulos/art_infantes.pdf.

14 Di Iorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B., ... & Greco, F. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense. P 55-59

Existen cuatro tipos de fotografías que se toman en el lugar de los hechos:

1. Vista General: son tomas fotográficas desde diferentes ángulos, donde se muestra de forma total el lugar de los hechos.
2. Vistas Medias: medios acercamientos, de diferentes ángulos.
3. Acercamientos: ej. un suicidio u homicidio, se tomará la fotografía del cuerpo.
4. Grandes Acercamientos: ej. a la víctima, lesiones que estén presentes, la mano que sostiene un arma, casquillos, etc. y de los indicios que estén junto al cuerpo, siempre acompañados de un testigo métrico.

3.2.5 Procesamiento digital de imágenes

Se denomina *procesamiento digital de imágenes* al uso de algoritmos y transformaciones matemáticas sobre imágenes digitales con el objetivo de mejorar su calidad (de acuerdo con alguna métrica), su interpretabilidad por un experto, o, en general, facilitar la extracción de información de estas.

Una de las representaciones más simples de una imagen digital es la de atriz de intensidades[15], donde la imagen es una grilla de números, y cada uno de estos representa la intensidad de la luz en ese punto. A cada punto en la imagen se lo denomina *pixel* (de *picture element*, o elemento de imagen). En el caso de las imágenes a color, cada pixel se compone no de un solo número, sino de 3, que representan la intensidad de los colores rojo, verde y azul para cada elemento.

Teniendo esto en cuenta, entonces procesar las imágenes es operar matemáticamente sobre las intensidades (de luz o de color), en búsqueda de facilitar el trabajo de los expertos, para este caso, criminalistas y forenses.

3.3 Propuestas de mejoras a partir de Herramientas de Software

A continuación, se presentan diferentes herramientas de software (tanto algoritmos como herramientas existentes en softwares de edición de imágenes o complementos de estos), y casos de estudio en lo que se las aplica para procesar una fotografía.

15 C. Rafael, Gonzalez, E. Woods Richard, & Masters, B. R. (2009). Digital Image Processing Third Edition. Ed. Pearson Education, Inc.

3.3.1 Medición por referencia a objetos conocidos

Es posible realizar una estimación de las medidas de un objeto presente en una imagen, si en la misma también se encuentra otro objeto cuyas dimensiones se conocen. El procedimiento consiste en tomar las medidas en pixels del objeto conocido, y luego establecer una correspondencia con sus medidas en centímetros (o metros, etc) tal que:

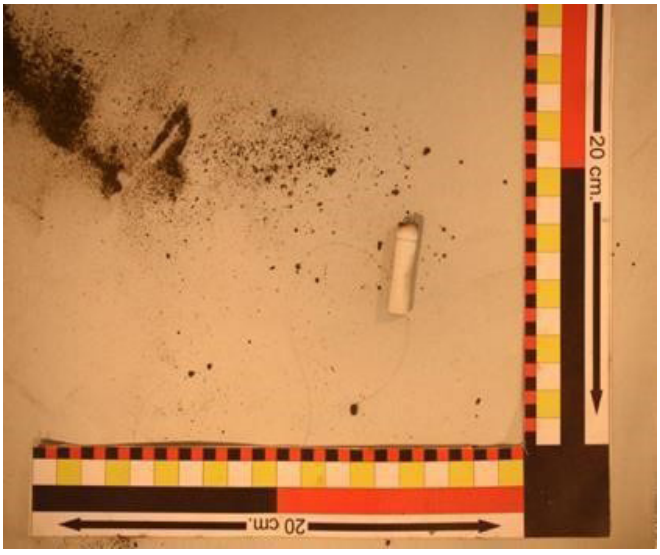
$$r = medidareal\ medidapixels$$

Luego se puede multiplicar por la medida en pixels del objeto de interés para obtener su estimación de tamaño, tal que:

$$medida'real = medida'pixels \cdot r$$

Dependiendo el punto de vista y la perspectiva de la imagen, las medidas que se obtengan por este método tendrán mayor o menor confiabilidad, pero de todos modos permiten obtener un estimado, a falta de mediciones concretas.

Figura 1. Colilla de cigarrillo de la cual no se puede obtener una medición exacta de la imagen sino es por medio de la señalética que se encuentra cercana a la misma. ML (Medición de largo), MA (Medición de ancho) y MR (Medición de referencia).



3.3.2 Transformación de grilla

Cuando un elemento de interés se encuentra en una imagen, pero por alguna razón se encuentra deformado, o con una perspectiva demasiado pronunciada, es posible utilizar transformaciones geométricas para compensar esta situación. En su caso más simple, esto se traduce en cambiar la perspectiva de un plano, y en casos más complejos, establecer un mapeo que permita deformar una superficie con respecto a otra. La correspondencia entre ambas superficies se establece de acuerdo a grillas equivalentes entre sí.

Figura 2. A) Imagen original. B) Grilla de transformación sobre (A). C) Resultado de transformar la grilla en (B) a una grilla regular. D) Igual que (C), pero con la grilla graficada previo a la transformación, para mostrar la grilla regular utilizada como objetivo de la proyección.

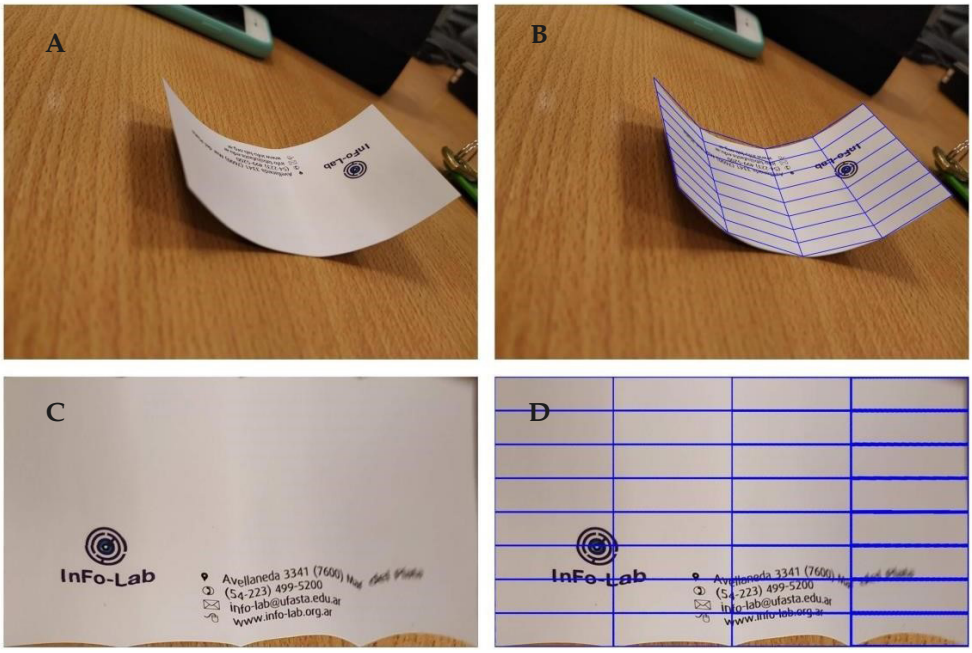


Figura 3. Imagen de referencia para contrastar con Fig 2-C.

En las Figuras 2 y 3 puede verse un ejemplo de esta técnica en acción. Si bien la imagen final en Fig. 2-C cuenta con deformaciones (ocasionadas por la definición de una grilla simple, que no cuenta con la resolución adecuada para el grado de deformación presente en la imagen), la transformación utilizada reúne traslaciones, rotaciones y cambios de perspectiva en una sola operación.

3.3.3 Image stacking, o apilado de imágenes

El stacking es una técnica que permite combinar varias imágenes similares, que deben tener pequeñas variaciones entre ellas, en una sola imagen de mayor calidad. Puede servir para mejorar la resolución espacial de las imágenes, lograr un menor ruido, o mejorar nitidez, entre otras posibilidades.

Es un principio básico de la estadística que la variación propia de un proceso de medición puede reducirse promediando el valor de varias muestras individuales. En el caso del stacking, se aplica este concepto a un conjunto de fotografías de un mismo objeto.

Para poder utilizarlo de manera efectiva, es necesario que las imágenes base no presenten movimiento o cambios de perspectiva entre ellas, o en su defecto, que se encuentren alineadas entre sí.

Se reducen las variaciones cromáticas (producto de la iluminación fluorescente de la escena) y el ruido propio que genera el sensor de la cámara en la fotografía. La imagen final que se obtiene en el caso de no alinear las imágenes base no es nítida y

presenta una distorsión de movimiento. Al contrario, la imagen donde sí se aplicó el alineamiento tiene mejor nitidez, y revela detalles más finos que no se podían distinguir en las imágenes base.

Figura 4. Imagen de base (izq.) comparada con la imagen final luego de aplicar stacking (der.), vista general.

Figura 5. Detalle de la imagen base comparado contra la misma región en la imagen compuesta.

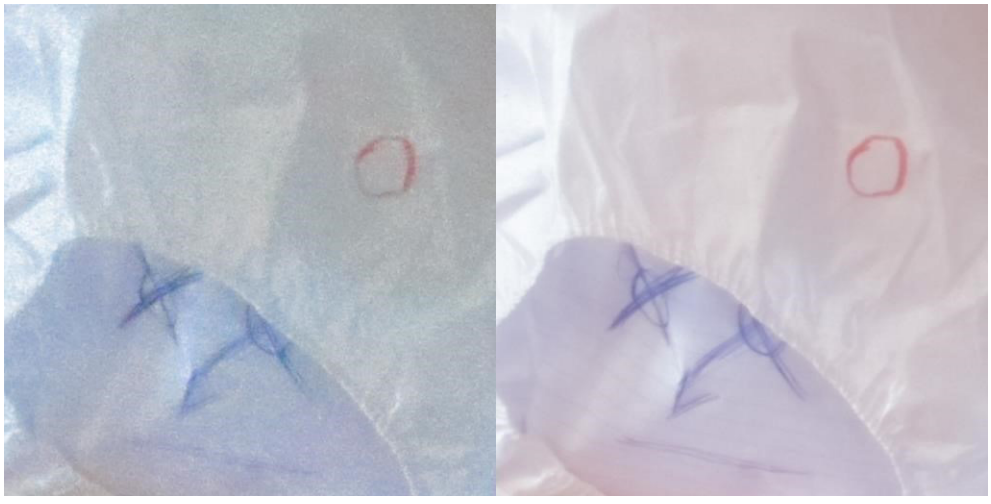


Figura 6. Detalle de la imagen base comparado contra la misma región en la imagen compuesta.

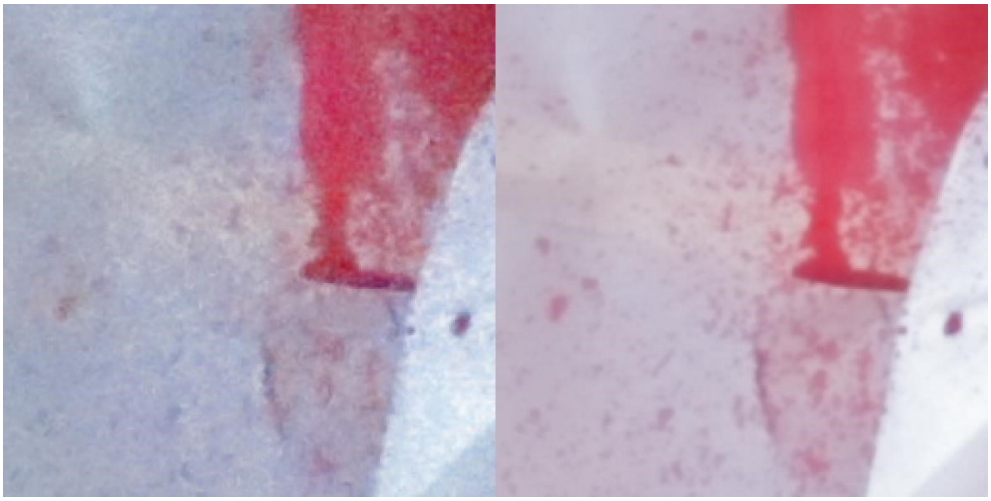


Figura 7. Detalle de la imagen base comparado contra la misma región en la imagen compuesta.

Se realizó una prueba en la que se tomaron 20 fotografías de una escena preparada, con la cámara fotográfica configurada en modo ráfaga y sin utilizar trípode. Las imágenes se alinearon entre sí para compensar el movimiento natural ocasionado por sostener la cámara a mano alzada.

En la Fig. 4 se puede ver la comparación a nivel macroscópico de una de las imágenes base utilizadas, y la imagen final resultante, y en las figuras 5, 6 y 7 detalles sobre las mismas. En general, se puede apreciar la menor cantidad de ruido en la imagen, y también la presencia de detalles más pequeños que se hacen evidentes en la imagen final, es decir, se ha mejorado la resolución espacial.

3.3.4 Desentrelazado

El entrelazado de vídeo es un mecanismo de compresión que, en lugar de guardar cada fotograma completo, almacena en un fotograma las líneas pares de la imagen, y en el siguiente fotograma, las líneas impares de esta. Los algoritmos de desentralazado permiten combinar las líneas pares e impares de una imagen entrelazada (o de dos cuadros de video consecutivos), para recuperar la imagen original.

Se utilizó el algoritmo de desentrelazado "Deinterlace2x" (variante DCCI2x), incluido con GMIC[16], sobre un cuadro de video extraído de una filmación propia. Debido al rápido movimiento, se puede observar en la Fig. 8 deformaciones propias del desentrelazado: un "serrucho" o "peine" en los bordes de la imagen donde hay más movimiento. Además, puede observarse que la patente del automóvil es ilegible producto del mismo. Luego de aplicar el algoritmo de desentrelazado (Fig 9), se aprecia el detalle de imagen recuperado.

Figura 8. Extracción de un cuadro de vídeo

16 G'MIC: GREYC's Magic for Image Computing, https://gmic.eu/.

Figura 9. Imagen reconstruida por el algoritmo de desentrelazado.

3.3.5 Deconvolución

La convolución es una operación matemática sobre señales en la que un *kernel* modifica y deforma la señal original[17]. Dependiendo de este último, la señal se verá afectada en mayor o menor medida. Existe una operación inversa, llamada deconvolución, que permite recuperar la señal latente, que es una aproximación de la señal original.

Al trabajar con imágenes digitales, puede usarse la convolución como modelo de las distorsiones que sufrió la imagen original al ser obtenida.

Para este ejemplo, se tomó la fotografía del culote de una vaina con un tiempo de exposición largo, de manera que la imagen obtenida presente movimiento (Fig. 10). Aplicando la operación de deconvolución con un kernel adecuado (Fig. 11) se logra eliminar gran parte de la distorsión generada por el movimiento de la imagen, y es posible leer el marcaje de la vaina en detalle. Para este proceso se utilizó el software SmartDeblur[18].

17 C. Rafael, Gonzalez, E. Woods Richard, & Masters, B. R. (2009). Digital Image Processing Third Edition. Ed. Pearson Education, Inc. p209-210.

18 Disponible: http://smartdeblur.net/

Tal como se muestra en la imagen, se genera un "fantasma" o residuo de la imagen original. Este proviene del hecho que la imagen latente es una aproximación de la imagen original deformada.

Figura 10. Culote de vaina con presencia de deformación

Figura 11. kernel de deformación que afecta la imagen detectada por SmartDeblur

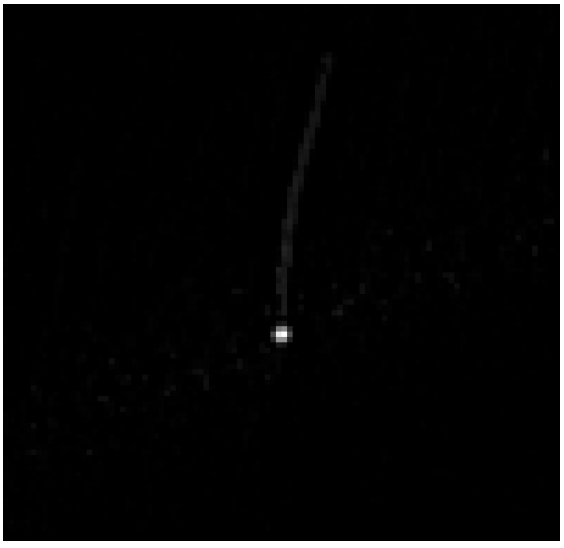


Figura 12. Resultado de la deconvolución presentando la imagen latente

3.3.6 Normalización local y ecualización de histograma

Las técnicas de procesamiento de imágenes que trabajan sobre el histograma permiten modificar la relación entre los valores más oscuros y más brillantes de esta, y así mejorar el contraste percibido. La diferencia entre Ecualización y la Normalización local, es que la Ecualización opera sobre la imagen de manera global, mientras que la Normalización Local opera sobre la imagen buscando el balance óptimo para cada pixel de acuerdo a su entorno local. Por ejemplo, si el rango de intensidad de la imagen es de 50 a 180 y el rango deseado es de 0 a 255, el proceso implica restar 50 a cada píxel de intensidad, lo que hace que el rango sea de 0 a 130. Entonces, cada intensidad de píxel se multiplica por 255/130, haciendo que el rango sea de 0 a 255.

Para realizar la prueba del uso de esta técnica, se tomó una fotografía con iluminación despareja, que presenta elementos muy brillantes y oscuros en el mismo cuadro, producto de la utilización del flash. Al aplicar las herramientas de Normalización y Ecualización de

Histograma[19] se puede recuperar el detalle en las regiones más oscuras. Inicialmente se probó utilizando la herramienta de Ecualización de Histograma Adaptativa

19 C. fael, Gonzalez RaE. Woods Richard, & Masters, B. R. (2009). Digital Image Processing Third Edition.Journal of Biomedical Optics. Ed. Pearson Education, Inc. P 120-128

(una variante del algoritmo general), pero no alcanzó para ver el detalle en las partes más oscuras de la imagen; luego se utilizó la herramienta de Curva de Intensidades, y se realizó el ajuste a mano. Finalmente, se concluyó que era mejor la Ecualización de Histograma, porque, aunque los resultados presentan una ligera distorsión de color, funciona de manera automática.

Figura 13. Imagen original de un escenario del hecho

Figura 14. Curva de Intensidades

Figura 15. Ecualización de Histograma

3.4 Guía de Buenas Prácticas de Fotografía Forense

En Argentina no existe una guía específica en la que se indique cómo tomar una fotografía en la escena del crimen, ni como calibrar el dispositivo. Por esto mismo, se decidió crear una guía que los especialistas puedan consultar antes de arribar a una escena del crimen las mejores prácticas a considerar a la hora de realizar tomas fotográficas que luego puedan ser pruebas válidas.

Recomendaciones a aplicar en la escena:

1. El fotógrafo inicia la inspección y análisis previo de manera general de la escena del crimen, documentando la presencia de las personas en el lugar y alrededores. También debe realizar la preservación de la escena y el acordonamiento de la misma.
2. En la búsqueda y fijación de indicios al fotógrafo le corresponde documentar los indicios encontrados, conforme a las técnicas adecuadas, sin alterar el estado original de los mismos.
3. Se deben colocar en todos los indicios, la regla métrica y la señalización adecuada.
4. Debe captar fotografías panorámicas, de mediana distancia, de detalle y las demás fotografías que a criterio del fiscal a cargo sean necesarias.
5. Todos los indicios allí encontrados y la peritación de los mismos deben ser documentados, en su estado original y luego del peritaje in situ.
6. En caso de que haya un cuerpo, el mismo debe ser fotografiado tal cual se encuentra, antes de que el personal médico lo retire de la escena, registrando fotografías de todos los ángulos posibles.

Recomendaciones con la cámara:

1. Una fotografía está correctamente expuesta cuando el sensor es capaz de capturar la mayor cantidad de información (luz) y tonos (rango dinámico) que su capacidad le permite.
2. Al llegar a la escena analizar el entorno y la cantidad de luz con la que se cuenta en el lugar para determinar las propiedades de la cámara a utilizar.
3. Tomar el dispositivo y seleccionar la opción de fotografiado M (Manual).

4. Ir a la configuración de la cámara.
5. En el menú de la cámara seleccionar el área de medición de la luz en puntual.
6. Calibrar la ISO (sensibilidad de la cámara ante la luz) según el escenario al que se enfrente:
    - Cuanto más iluminada esté la escena, más baja la ISO que se puede utilizar.
    - Bajo luz del sol, se recomienda utilizar ISO 50, 64, 80, o la más baja que permita la cámara.
    - De noche, se recomienda utilizar ISO 1600 o superior. Es importante tener en cuenta que las ISOs más altas generan ruido en la foto, que toma la forma de un puntillado que reduce la resolución efectiva de la imagen.
7. Calibrar la velocidad de exposición:
    - Si no se cuenta con trípode, debe configurarse de 1/80 o más rápida.
    - Si se cuenta con trípode, se pueden usar velocidades de exposición más lentas.
8. Calibrar la apertura de diafragma (entrada de luz al sensor) según al escenario:
    - Si es muy oscuro o si está nublado, debe estar abierto al máximo, en f/2.8 o 4.
    - Si hay mucha iluminación o se encuentra el día muy soleado, debe estar cerrado al máximo, f/16 a f/24 (dependiendo del lente).
    - Para iluminaciones intermedias se utiliza un f/8, u otras aperturas intermedias.
9. Para ajustar el valor de exposición, es preciso realizar una medición del tono más claro de la escena.
10. Calibrar el balance de blancos, para lograr una adecuada representación de los colores. La cámara permite seleccionar la sensibilidad, temperatura de color, tamaño de la imagen y la resolución por imagen de manera individual.

- Es importante configurar estas opciones si la cámara no se utiliza formato RAW, ya que, luego de tomada la fotografía, es difícil de compensarlas.

11. Ajustar la distancia en el área a enfocar.
12. Encuadrar el motivo a través del visor.
13. Capturar la imagen.

Sugerencias:

1. Para técnicas con Luminol/Bluestar se debe dejar la cámara en función "Bulbo", para que pueda estar alrededor de 1 minuto con el obturador abierto, poner el flash en la primera cortina de manera que sea disparado en medio de este tiempo y la fotografía quede correctamente expuesta y visible.
2. En casos donde la iluminación es escasa y la cámara no permite modificar las configuraciones, se debe poner el dispositivo con ISO alta (ej: 1600) y tiempo de exposición muy bajo (ej 1/200), con el objeto de tomar varias fotografías en modo ráfaga y poder combinarlas con la técnica de Stacking.
3. El uso de *stacking* puede ser una herramienta valiosa en situaciones donde no se cuenta con iluminación adecuada y por lo tanto el fotógrafo se ve forzado a utilizar una ISO alta, que introduce ruido en las imágenes obtenidas y reduce la resolución efectiva de las imágenes obtenidas.

    a) Utilizar una ISO alta (1600 a 3200, ISOs superiores solamente logran reducir el rango dinámico final de la imagen).

    b) Usar velocidad de obturación alta, verificando con el fotómetro y el histograma que todavía se puede capturar detalle en la imagen.

    c) Configurar el modo de disparo en "Ráfaga".

    d) Capturar entre 10 y 50 fotografías.

4. Si el usuario toma múltiples imágenes desde diferentes ángulos de la escena del crimen, puede ser de ayuda para el planimétrico a la hora de tomar medidas de la misma.

Acciones de mejora de imagen:

1. Las técnicas de filtrado lineal incluyen afilado, desbarbado, mejora y deconvolución. Estas técnicas, se usan para aumentar el contraste de pequeños detalles en una imagen. Si se usa un bajo grado de mejora, la imagen seguirá siendo igualmente precisa de la representación de la escena.

2. Se puede usar un ajuste de contraste no lineal para resaltar detalles en las áreas sombreadas de una imagen sin afectar las áreas resaltadas.

3. Las técnicas de reducción de ruido aleatorio se usan para reducir el contraste de pequeños detalles en la imagen para suprimir el ruido aleatorio.

4. Las técnicas de medición de la escena sirven para a través de la medida inicial de un objeto conocido y una alineación de la imagen, lograr que pueda conocerse la medida faltante.

5. Las técnicas de desentrelazado sirven para los vídeos de cámaras de seguridad, como vídeos de la escena, para suprimir el "fantasma" o "serrucho" y que puedan mejorarse detalles de la misma.

Se sugiere a continuación una lista de acciones básicas vinculadas a la calibración de la fotografía para maximizar la luz y el rango dinámico, que pueden sintetizarse en:

- Analizar el entorno
- Usar modo manual
- Configurar la cámara
- Calibrar ISO
- Ajustar velocidad de exposición
- Ajustar apertura de diafragma
- Ajustar balance de blancos

Además, es preciso recordar que:

- Los reactivos Luminol y Bluestar necesitan modo bulbo para exposición prolongada.
- Si la iluminación es escasa, es conveniente tomar fotografías adicionales con modo ráfaga y luego mejorar con *stacking*.

- Tomar imágenes de diferentes ángulos es recomendable y puede colaborar con la posterior tarea de planimetría del lugar.

3.5 Conclusiones

La fotografía digital puede realizar un avance significativo en la criminalística. En la actualidad el especialista puede registrar imágenes de la escena del hecho desde diferentes ángulos y perspectivas, tanto generales como particulares, y luego procesarlas con distintas herramientas de software que le permitan extraer información significativa de las mismas.

Mientras que, en otro momento, con las cámaras analógicas esto era prácticamente imposible, ya sea por el alto costo que, del revelado de las fotografías, así como también, por la escasez de imágenes que se podían tomar en una escena determinada.

La Guía propuesta, recomienda un conjunto de actividades básicas que ayuda a los especialistas a prepararse antes de arribar a la escena y según las condiciones en las que se encuentra, calibrar la cámara para adaptarla en el entorno. De esta manera, es posible sacar el mayor provecho al registro, logrando que las imágenes tomadas sean de mejor calidad y reducir la necesidad de procesarlas digitalmente. Y en caso que esto último sea requerido, se sugiere qué herramienta sería útil en cada caso, incluso combinándolas, para la mejora de imagen.

Las técnicas propuestas que son utilizadas sobre las imágenes se basan en algoritmos y procedimientos científicos que dan valor probatorio, logrando resultados valiosos y factibles de ser utilizados en la etapa del juicio oral:

Medición de objetos en imágenes: permite tomar medidas relativas con respecto a la medida de objetos conocidos presentes en la imagen.

- Transformación de grilla: permite mapear una imagen de acuerdo a la relación entre dos grillas.
- Stacking: permite combinar varias imágenes en una sola de mayor resolución y calidad.
- Desentrelazado: permite eliminar distorsiones típicas de cámara vídeo.
- Deconvolución: permite eliminar el movimiento de la cámara al momento de sacar una fotografía e imperfecciones del lente fotográfico.
- Normalización: permite equilibrar el contraste de la imagen de manera automática.

Concluyendo se puede afirmar que estás técnicas se adaptan para lograr en poco tiempo el procesamiento de imágenes y el resaltado de los detalles de interés, logrando que la investigación tenga resultados rápidos y factibles de presentar como medio de prueba en un Juicio.

3.6 Agradecimientos

Queremos agradecer especialmente al Lic. Hernán Gacio, director de la carrera y a la Mg. Eugenia Huinchulef, profesora de la materia Taller de Tesis de la Lic. en Criminalística de la Universidad FASTA, por el aporte realizado para la concreción de este trabajo. También queremos agradecer al InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense, integrado por la Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires, la Municipalidad de General Pueyrredón y la Universidad FASTA, por generar el ambiente propicio para seguir soñando y creando herramientas para los profesionales forenses y los investigadores criminales.

3.7 Referencias Bibliográficas

Arrocha E, Arauz J y Arosemena A. *"Fotografía e infografía"* (Monografía). Facultad de Comunicación Social, Universidad de Panamá, 2013.

Definición de Fotografía. Disponible en:

https://www.definicionabc.com/tecnologia/fotografia.php accedido el 05/02/2019

Fotografía Forense por Andrea Castellón Sossa (Costa Rica). Disponible en:

https://criminologiacr.com/2015/02/24/fotografia-forense/ accedido el 05/02/2019

Guzmán, C. Manual de criminalística. Buenos Aires, Argentina. La Rocca. 2003

Rico, F. G., & Anda, D. (1991). *La fotografía forense en la peritación legal*. Ed. Trillas, México.

Saquiché, Ligia María Sum. *Fotografía forense: Uso de la fotografía digital en las escenas del crimen de delitos contra la vida.* (Tesis de grado). Campus Central Guatemala de la Asunción, 2013.

González Donis, José Carlos. *Características de la fotografía análoga y digital*. Guatemala. 2007. Tesis de Escuela de Ciencias de la Comunicación. Universidad de San Carlos de Guatemala.

Acharya, T., & Ray, A. K. (2005). *Image processing: principles and applications.* Ed. John Wiley & Sons.

C. Rafael, Gonzalez, E. Woods Richard, & Masters, B. R. (2009). *Digital Image Processing Third Edition*. Ed. Pearson Education, Inc.

Parker, J. R. (2010). *Algorithms for image processing and computer vision.* Ed. John Wiley & Sons.

GREYC's Magic for Image Computing. Disponible en: https://gmic.eu/. Accedido el 16/09/2019.

Di Iorio, A. H., Castellote, M. A., Constanzo, B., Curti, H., Waimann, J., Lamperti, S. B.,

… & Greco, F. (2017). El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense.

Procesamiento de Imágenes. Disponible en: https://volaya.github.io/libro- sig/ chapters/Imagenes.html accedido el 10/04/2019

Alineación de Imagen. Disponible en: *https://www.learnopencv.com/image-alignment- ecc-in-opencv-c-python/* accedido el 12/05/2019

Desenrollamiento de un cilindro. Disponible: *https://dsp.stackexchange.com/questions/2406/how-to-flatten-the-image-of-a-label- on-afood-jar* accedido el 20/05/2019

Manual de normas y procedimientos para el Procesamiento de Escenas Crimen, del Ministerio Público, Guatemala, Abril 2009. Resolución 16-2009.

4 La Tecnología y la Informática en el Debate Jurídico-Procesal

Cortes Monsalve Lilia[20]
lilia.cortes@unilibre.edu.co
Bryan Egea Suarez[21]
bryan_cho@hotmail.es
Isabela Conde Campos[15]
isaconk@hotmail.com

Resumen

Este estudio aborda la incidencia de las tecnologías de la comunicación en la mensajería instantánea, como un instrumento que permite probar distintos hechos, cuya relevancia resulta fundamental bajo el enfoque de género, y que en Colombia hay algunos avances de los que hablaremos en este trabajo.

El trabajo desarrolla dos líneas de pensamiento, en primer lugar, se realiza un análisis de la mensajería instantánea como medio de prueba documental en Colombia, en procesos penales. En segundo lugar, se examinó la valoración judicial de la mensajería instantánea en los procesos penales cuando se trata de establecer responsabilidad penal por los delitos que atentan contra la integridad sexual de cualquier individuo en general, y en particular de la mujer por razón de su género.

Palabras clave: mensajería instantánea, debate procesal, prueba documental tecnológica.

---

20 Docente jornada completa investigadora. Categoría Asociada Colciencias convocatoria 2018-Codirectora Grupo Criminalística y Ciencias Forenses Categoría A1 y Sistemas Penitenciarios y Carcelarios categoría A1 convocatoria 2018. Abogada, criminóloga, especialista en Derecho Constitucional, Candidata a Doctor en Derecho. Docente pregrado, Maestría en Derecho Penal Universidad Libre Cali, Bogotá, Barranquilla. Docente Maestría en Ingeniería Civil y geomántica, Facultad de Ingeniería Civil, Arquitectura e Ingeniera Topográfica Universidad del Valle Sede Cali. Líder *Semillero Instituciones Jurídico Penales.*

21 Estudiante 4 año Derecho – integrante *Semillero Instituciones Jurídico Penales* - Universidad Libre Cali [15] Estudiante 4 año Derecho - *Semillero Instituciones Jurídico Penales* - Universidad Libre Cali

4.1 La mensajería instantánea como una nueva modalidad del medio de prueba documental en Colombia

Noción de mensajería instantánea. Los avances tecnológicos han facilitado la comunicación entre las personas, el mundo afronta los efectos deseados y no deseados de la globalización, y en él la mensajería instantánea se ha convertido en una herramienta que ha permitido avanzar y comunicarse en tiempo real con otras personas sin importar el lugar del mundo en donde se encuentren, siempre y cuando estén conectados a internet; un claro ejemplo se ve reflejado a través de WhatsApp y Facebook, plataformas digitales de comunicación que han tenido un importante auge en los últimos años, dinamizado por la redes sociales.

Cabe aseverar que esta nueva forma de comunicación tiene una naturaleza incluyente, ya que su forma de uso es afable para individuos, que presenten algún tipo de limitación real o imaginaria, física o cognitiva o que generen barreras como prejuicio, por ejemplo ancianos, los niños y los discapacitados; en otro orden de ideas, se evidencia que se utiliza este medio de comunicación para tramitar asuntos personales, y también con igual frecuencia y efectividad en varios sectores como el laboral, educativo, en actividades de prestación de servicios y de producción.

En la sociedad actual se vive una inmensa masificación y expansión de las tecnologías de la información y comunicación. Nos encontramos ante un uso de estas nuevas tecnologías totalmente globalizado por parte de cualquier persona con independencia de la edad, de las preferencias, del lugar, entre otras. Desde su aparición por primera vez a mediados del siglo XX han ido calando en cada uno de los diferentes sectores tales como en la industria, economía, comercio, ocio y educación hasta el punto de resultar imprescindibles para la vida cotidiana. (Quiles, 2016, p.6).

Bajo el criterio anterior, se entiende que la mensajería instantánea es un medio de comunicación en donde dos o más personas se envían mensajes (texto, fotografías, audios, videos) a través de dispositivos electrónicos que permitan ejecutar dicha acción de forma instantánea; se diferencia del correo electrónico puesto que la información que brinda el emisor es recibida en tiempo real por su receptor.

Noción de mensajería de datos. A diferencia de la mensajería instantánea, los mensajes de datos son toda aquella información que se envía o se recibe por cualquier medio electrónico sin la particularidad de la inmediatez. Estos surgen con la evolución tecnológica de los medios de comunicación y la aparición del internet, por lo cual guardan una relación estrecha, pero no símil, con la mensajería instantánea, formando parte integral de la mensajería digital por su naturaleza de necesitar un medio electrónico para poder ejecutarse. En Colombia los mensajes de datos se encuentran regulados por la ley 527 de 1999, la cual controla su uso y

aplicación, en ella se definen como: "Artículo 2. Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".

4.2 La mensajería instantánea y los medios de prueba en Colombia

La mensajería instantánea es así definida propiamente como un medio de comunicación por medio del cual dos o más personas naturales, - o jurídicas dentro del ámbito comercial- se envían mensajes (textos, fotografías, audios, videos) a través de dispositivos electrónicos que permitan ejecutar dicha acción de manera instantánea, por lo tanto, es procedente entonces hablar de esta desde el punto de vista de los medios de prueba en los procesos judiciales en Colombia.

La legislación colombiana, en referencia inicial al Código General del Proceso contiene en su normatividad procesal, los diferentes medios de prueba aplicables a todo proceso de naturaleza civil, comercial, de familia y agraria que dentro del ordenamiento jurídico han de llevarse a cabo. Para el caso, la norma consagra de manera general en su artículo 165, en el cual establece que son medios de prueba la declaración de parte, la confesión, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios, los informes y todo aquel otro medio distinto a los anteriores que sea útil para la formación del convencimiento del juez.

Desde el ámbito del derecho penal colombiano, la ley 906 de 2004, consagra en su artículo 382, como medios de prueba, el testimonio, la prueba pericial, la prueba documental, la prueba de inspección, los elementos materiales probatorios, la evidencia física y al igual que en el caso del Código General del Proceso, permite que pueda añadirse cualquier otro medio, técnico o científico, siempre que sea necesario y no contraríe el ordenamiento jurídico.

Las dos alusiones esbozadas por los Códigos mencionados anteriormente dejan al final de su enunciado el camino abierto para todos aquellos otros medios que sean necesarios, independientemente de su naturaleza, siempre y cuando no contraríen al ordenamiento jurídico. En razón a lo anterior podría considerarse que la mensajería instantánea puesta frente a la definición de medio de prueba corresponde en cuanto a características y aplicabilidad en los procesos judiciales, lo que permite su implementación como una nueva modalidad del medio de prueba documental en Colombia.

Los medios de prueba son aquellos métodos a través de los cuales se lleva al convencimiento al juez para la eventual convicción de los hechos objetos de ser probados, sin violación alguna al ordenamiento jurídico particular; y definidos por el maestro Davis Echandía, se clasifican en dos grupos, el primero de ellos dispone de la siguiente manera:

> Se entiende por medio de prueba la actividad del juez o de las partes, que suministra al primero el conocimiento de los hechos del proceso y, por lo tanto, las fuentes de donde se extraen los motivos o argumentos para lograr su convicción sobre los hechos del proceso, es decir, la confesión de la parte, la declaración del testigo, el dictamen del perito, la inspección o percepción del juez, la narración contenida en el documento, la percepción e inducción en la prueba de indicios. (Echandía, pp. 550 - 551).

Y, por otro lado, la segunda de ellas que dispone una concepción de medio de prueba referente a un órgano o instrumento, a diferencia de la primera que dispone sobre una fuente de conocimiento en materia probatoria:

> Desde un segundo punto de vista se entiende por medio de prueba los instrumentos y órganos que suministran al juez ese conocimiento y esas fuentes de prueba, a saber: el testigo, el perito, la parte confesante, el documento, la cosa que sirve de indicio, es decir, los elementos personales y materiales de la prueba. (Echandía, p. 551).

Por los motivos expuestos anteriormente, la prueba documental desde la mensajería instantánea como su nueva modalidad formaría parte del primer grupo de medios de prueba que el maestro Echandía describe, ya que esta clase de medio probatorio puede almacenar dentro de sí mismo, información en diferentes formatos con voz e imágenes, por ejemplo audios, fotográficas, videográficas o documentales, puesto que estas tienen por objetivo, llevar al juez a un estado de certeza y convencimiento respecto de hechos en particular propuestos por una parte dentro del proceso, independientemente de que no hayan sido introducidas por sí mismas como pruebas autónomas, dado que su introducción fue dependiente de un medio de prueba principal y categórico, que para el caso, es el defendido por la actual tesis de este escrito, o sea, la prueba documental, que bien es definida como: "Por prueba documental suele entenderse el conjunto de actividades dirigidas a convencer al juzgador de la certeza, positiva o negativa de unos hechos mediante la apreciación de objetos que incorporan la expresión escrita de pensamientos humanos (De la oliva, Diez-Picazo & Vegas, 2016, p.163).

4.2.2 La Mensajería Instantánea en Investigaciones por Violencia Sexual en Colombia

El postulado inicial de la tesis que defiende este texto, es en suma la implementación de la mensajería instantánea como nueva modalidad del medio de prueba documental, el cual para el caso se correlaciona con el fenómeno de la violencia contra la mujer en Colombia desde el marco de la violencia sexual, dado que en la cotidianeidad, esta problemática antijurídica normalmente toma ocurrencia en ambientes eminentemente privados, por lo cual, resulta realmente difícil encontrar un medio de prueba distinto a la declaración de parte y al testimonio, que logre evidenciar el suceso por el cual una mujer fue lesionada, agredida o ultrajada sexualmente.

Sobre lo expuesto antes, se entiende entonces que las únicas pruebas pertinentes para casos de violencia sexual contra la mujer se limitan a las brindadas por personas externas que vieron, escucharon o dan cuenta sobre el hecho, como se ejemplifica con el testimonio, o, por otro lado, con la misma declaración de la parte afectada, rendida en estrados judiciales. Ahora bien, frente al reconocido fenómeno del uso de las tecnologías de la comunicación que actualmente se evidencia y continua avanzando, resulta propio también reconocer, que el actuar criminal ha evolucionado conforme a los nuevos escenarios y ámbitos de interés de la sociedad.

A través de la mensajería instantánea, definida esta misma como una nueva modalidad del medio de prueba documental que transmite información (videos, fotos, documentos y textos) de manera instantánea, se ha evidenciado el patrón sistemático mediante el cual si bien se transmite información, esta misma no siempre es de carácter legal, ya que en determinados casos, la información que circula tiende a ser lesiva para una persona determinada y vulnera el ordenamiento jurídico que en prima facie, protege los derechos del individuo, y en segundo lugar, en el ámbito punitivo, las conductas llevadas a cabo por medio de aplicaciones como Facebook, WhatsApp y Twitter, facilitan la divulgación de contenido susceptible de ser prueba en un proceso penal por razón de su naturaleza vinculante.

Al hablar de pruebas, resultaría dicotómico no evidenciar la problemática de la mensajería instantánea con relación a la violencia sexual contra la mujer sin un caso que demuestre realmente lo que se está postulando en éste preciso momento, así que, bajo ese entendido, la sentencia SP922-2019[22], evidencia la problemática de la infravaloración de la mensajería instantánea en un proceso penal en donde una mujer es víctima. La jurisprudencia demuestra que la primera y la segunda instancia de igual forma, valoraron las conversaciones que se dieron por medio de mensajería

22 Corte Suprema de Justicia, Sentencia SP922-2019. M.P. Luis Antonio Hernández Barbosa.

instantánea de forma racional; aunque estas hayan sido puestas a valoración del Juez y Magistrados por medio de un testimonio y no cómo una modalidad del medio de prueba documental autónomo e independiente. Para el caso, juega vital importancia esta prueba porqué las conversaciones demuestran que la menor de edad víctima del caso, dio a conocer a su victimario por medio de Facebook una supuesta edad que por cuestiones físicas y psicológicas se podía inferir era superior a los catorce (14) años. Lo anterior en razón de que las relaciones sexuales con menor de 14 años son tipificadas por el artículo 208 del Código Penal Colombiano bajo el tipo de acceso carnal abusivo con menor de catorce años, y, además, quien incurriese en esta conducta, estaría sujeto a enfrentar entre 12 y 20 años de prisión.

Por este motivo, la Corte Suprema de Justicia en Sala de Casación Penal, fue la encargada de analizar la providencia proferida por su *Ad Quem* en la que este reitero la decisión de su *a quo*, ello por medio de recurso de casación. La Corte evidenció que en primera instancia el juez falló condenando al acusado en razón a que el victimario conocía la edad de la víctima, ya que esta misma se la había mencionado por Facebook; por otro lado constató que en segunda instancia se ratificó el fallo en base al claro conocimiento que tenía el victimario sobre la edad de la víctima, sin importar de igual forma, que uno de los argumentos del Tribunal haya aludido una violación indirecta a la ley sustancial por falso raciocinio, al aseverar que por la victima tener falda y uniforme escolar, era menor de edad.

Sin embargo, la Fiscalía General de la Nación, no adjuntó la mensajería instantánea recopilada de Facebook como una nueva modalidad de prueba documental independiente. Para lo cual se valió del testimonio de la hermana de la menor, en el que ella relató lo que se dijo en la conversación que se llevó a cabo por la red social mencionada anteriormente; no obstante, no esperaba la Fiscalía que la menor incurriera en contradicción al ofrecer su testimonio, dejando en entredicho todo aquello que atestiguo en beneficio de la víctima, motivo por el cual la Corte Suprema de Justicia en sala de casación penal decidió fallar con base al *indubio pro reo*, absolviendo a quien fue el victimario por duda razonable.

4.3 Conclusiones

Se concluye de todo lo anterior que la mensajería instantánea es un medio de comunicación a través del cual se envían y reciben mensajes de todo tipo de manera instantánea: que esta ha entrado a representar un papel preponderante dentro de nuestra sociedad, a tal nivel que ha de convertirse en un imperativo considerarla y adoptarla dentro de los procesos judiciales en Colombia, con ocasión a que se ha introducido fuertemente a través de la transnacionalización de bienes y servicios, y del derecho y el continuo avance de las tecnologías de la comunicación debido

a su fácil acceso y uso, en la mayoría de la población sin distinción de edad. De igual forma, la mensajería instantánea deberá ser también implementada como una nueva modalidad dentro del medio de prueba documental, dado que esta permite dar conocimiento al juez sobre los hechos, llevándolo al convencimiento y a la certeza sobre las afirmaciones y negaciones que se den en un pleito jurídico independientemente de su naturaleza en particular.

Subsidiariamente, en el campo penal en específico, la mensajería instantánea es de vital importancia, debido a que para algunos delitos en particular, como en los casos de violencia sexual contra las mujeres por razón de su género y en condición del mismo, las pruebas con que se cuenta normalmente para ser valoradas eventualmente por un Juez, son aquellas que se retrotraen al testimonio y a la declaración de parte, dándole al proceso un camino muy subjetivo, ya que dependería este de una adecuada valoración de los recuerdos y vivencias de otras personas, campo en el cual la pericia no se mide en datos cuantitativos, sino en un criterio de interpretación personal con base a lo que se escucha y analiza.

Por lo anterior, es de común conocimiento que las decisiones que son adoptadas por Tribunales, Juzgados y las mismas altas Cortes, recaen en decisiones fundadas en estándares probatorios apoyados en los diferentes medios de prueba que para cada caso son necesarios. Si se implementara la mensajería instantánea como nueva modalidad del medio de prueba documental para ser adoptada en los casos en que fuere pertinente, esta permitiría mitigar la impunidad, ya que se podrían disminuir las posibilidades de incurrir en una duda razonable o una indebida medición cuantitativa de las probabilidades de que un hecho sea cierto o incierto. Para el caso de la violencia sexual contra la mujer, podría ser significativo en el debate probatorio de ser tenida en cuenta esta nueva modalidad de prueba documental, ya que, dentro de sí misma almacena evidencia distinta a la prueba en sí, como fotos y videos. Se tiene además que la mensajería instantánea no se encontraría sujeta a un análisis de las condiciones personales de quien haya sido participe de la conversación, sino de las posiciones sustentadas en juicio sobre la veracidad de tal interacción digital por una red social. Finalmente, respecto a su impacto en el debate probatorio, sería de gran utilidad no solo en procesos de índole penal sino también en cualquier otro que dentro de la jurisdicción ordinaria tenga lugar y que requiera de una adecuada aplicación de justicia material.

4.4 Referencias Bibliográficas

Bustamante, M.M. (2010). La relación del estándar de prueba de la duda razonable y la presunción de inocencia desde el garantismo procesal en el proceso penal colombiano. Revista Opinión Jurídica. (9). No.17, 71-91. Medellín: Universidad De Medellín. Corte Constitucional. Sentencia T-878/14 M.P. Jorge Iván Palacio Palacio.

Cabezas-Martinez, Núñez-Bermeo, Arteaga Córdoba & Cortes-Monsalve. Análisis crítico del sistema penal colombiano ISBN 978-958-5545-30-4. Impreso y ISBN 978-958-5545-31-

1. Libro digital descargable

Centro Regional de Derechos Humanos y Justicia De Genero: Situación en Colombia de la violencia sexual contra las mujeres. revisado en enero 27 del 2017. Disponible en http://www.humanas.org.co/archivos/Situacion_en_Colombia_de_la_violencia_sexual_con tra_las_mujeres.pdf.

Corte Constitucional. Sentencia T-804/14 M.P. Jorge Iván Palacio Palacio.

Corte Suprema De Justicia. Sentencia Sp-2706-2018 M.P. José Luis Barceló Camacho.

Cortés, E. (2014). Feminización Y Subalternización Del Otro Enemigo. Construcción Y Destrucción De Corporalidades En Contextos De Conflicto Armado Y Violencia Extrema. Revista Colombia Internacional. No. 80. Bogotá: Facultad De Ciencias Sociales, Universidad De Los Andes.

Cortes-Monsalve, Garrido-Ochoa & Rubiano-Medina; (2018). Estándares de enseñanza para la formación en litigación oral en las facultades de Derecho en Colombia. ISBN: 978-95899498-2-5.

De La Oliva, A. Diez-Pícazo, I. Vegas, J. (2016). Curso De Derecho Procesal Civil II: Parte Especial. Madrid, Editorial Centro De Estudios Ramón Aceres, S.A.

Echandia, H. D. (2012). Teoría General De La Prueba Judicial. Bogotá, Editorial Temis S.A.

Ferrajoli, L. (1999). Derechos Y Garantías. La Ley Del Más Débil. Madrid, Editorial Trotta.

Lagos-Enriquez, Meneses-Medina & Cortes-Monsalve. *"El derecho penal del riesgo un instrumento de política criminal"* en libro Legalidad y subjetividad desde la mirada foucaultiana 2017 Editorial UPB. ISBN: 978–958-764-512-9.

Maier, Julio. Derecho Procesal Penal Tomo II. 3ª. Reimpresión 2013. ISBN 978-987-9120-54-5. Buenos Aires.

Melero, N. (2010). Reivindicar La Igualdad De Mujeres Y Hombres En La Sociedad: Una Aproximación Al Concepto De Género. Revista Castellano-Manchega De Ciencias Sociales. No. 11, 73-83.

Pino-Domínguez, Cortes-Monsalve & Salcedo-Cifuentes. (2018). Caracterización De Los Casos De Violencia Sexual Atendidos En Dos Instituciones Prestadoras De Servicios De Salud Del Municipio De Palmira-Valle Del Cauca. Colombia. Rev. Méd. Risaralda 2018; 24 (1): 10 - 13 ISSN:2539-5203 Contacto: Revistamedica@Utp.Edu.Co Https://Doi.Org/10.22517/Issn.2539-5203

Ramos, C. (1997). El Concepto De "Género" Y Su Utilidad Para El Análisis Histórico. Revista La Alfaba, Segunda Época. (2). Bogotá: Facultad De Ciencias Humanas, Universidad Nacional De Colombia. Recuperado De Http://Www.Biblioteca.Unlpam.Edu.Ar/Pubpdf/Aljaba/V02a02ramos.Pdf.

Ruiz, Y. (2007). La Violencia Contra La Mujer En La Sociedad Actual: Análisis Y Propuestas De Prevención. Castellón De La Plana: Universitat Jaume I. Recuperado De Http:// Repositori.Uji.Es/Xmlui/Bitstream/Handle/10234/78453/Forum_2007_18. Pdf?Seque nce=1.

Sánchez J, Alonso C, Horno P, Santos A. Niños y niñas víctimas de abuso sexual y el procedimiento judicial. Revisado en junio 1 del 2015. Disponible en https://www. savethechildren.es/sites/.../violencia_sexual_contra_losninosylasninas.pdf.

Taruffo, M. (2005). Conocimiento Científico Y Estándares De Prueba Judicial.

Boletín Mexicano De Derecho Comparado. No. 114, 1285-1312. Pavía: Universidad De Pavía.

Tabarez-Valencia; Bedoya L., & Cortes-Monsalve Identificación de criterios de orden legal y científico en el derecho probatorio del sistema penal que incidieron en el proferimiento de sentencias de los enjuiciados por delitos sexuales entre el 2009-2010 en dos municipios del Valle del Cauca. Revista Criminalidad ISSN 1794 Vol. 58 Numero 2 mayo-agosto De 2016 Bogotá Colombia.

Tortosa, J. (2009). Feminización De La Pobreza Y Perspectiva De Género. Revista Internacional De Organizaciones (Rio). No. 3, 71-89. Recuperado De Https:// Core.Ac.Uk/Download/Pdf/16367145.Pdf.

Quiles, L. (2016). Las Nuevas Tecnologías Como Medio De Prueba En El Proceso Penal (Tesis De Pregrado). Elche: Facultad De Ciencias Sociales Y Jurídicas De Elche, Universidad Miguel Hernández.

5 Falencias en el Tratamiento de la Memoria Flash USB que Afectan La Validéz Como Evidencia Digital y sus Consecuencias en el Sistema Penal Acusatorio Colombiano

Wilmer Mondragón Restrepo[23]
Jovanne Esteban Ortiz Pérez[24]

Resumen

El permanente progreso tecnológico que experimenta la humanidad, permite evolucionar igualmente a nuevas formas de delinquir a través de sistemas informáticos, las cuales abren la puerta al concepto de evidencia digital como elemento material probatorio y evidencia física en el proceso penal Colombiano, presentándose en algunas ocasiones deficiencias en su procedimiento que afectan la validez como medio probatorio, razón por la cual esta investigación muestra las diferentes fases y las falencias que se presentan en la manipulación de este tipo de elemento especialmente en memorias Flash USB, así mismo algunas consecuencias jurídicas que se pueden presentar en materia procesal penal frente a estos errores detectados; de esta manera se revela la importancia que tiene la evidencia digital por contar con un tratamiento diferenciado respecto de otros medios probatorios, dada su naturaleza volátil por tratarse de información electrónica, así como la necesidad de llevar a cabo el procedimiento de cadena de custodia que garantice la autenticidad y capacidad demostrativa.

23 Abogado Universidad Cooperativa de Colombia. Especialista en Derecho Penal Universidad Libre. E-mail: andres721m@hotmail.com.

24 Abogado Universidad Central del Valle. Especialista en Servicio de Policía de la Escuela de Posgrados Policía Nacional. Especialista en Derecho Procesal Universidad Pontificia Bolivariana. Especialista en Derecho Penal Universidad Libre. E-mail: jovanneortiz@outlook.com

Palabras Claves: Evidencia digital, informática forense, memoria flash, cadena de custodia, prueba, falencia.

Abstract

The permanent technological progress that humanity experiences, also allows new forms of crime to evolve through computer systems, which open the door to the concept of digital evidence as material evidence and physical evidence in the Colombian criminal process, presenting itself on some occasions deficiencies in it´s procedure that affect the validity as a means of evidence, which is why this investigation shows the different phases and the shortcomings that arise in the manipulation of this type of element especially in USB flash drives, as well as some legal consequences that can be present in criminal procedural matters against these errors detected; in this way, the importance of digital evidence is revealed by having a differentiated treatment compared to other evidence, given it´s volatile nature because it is electronic information, as well as the need to carry out the chain of custody procedure that guarantees authenticity and demonstrative capacity.

Key Words: Digital evidence, computer forensics, flash memory, chain of custody, proof, failure.

Introducción

La era digital no solo hace referencia al avance de las innovaciones tecnológicas en la que paulatinamente se reducirá el uso del papel, sino que cada vez será más importante para los individuos proteger su identidad y privacidad, considerando la sociedad en ese universo digital como un entramado comunicativo masivo que diariamente produce información, en él se encuentran conceptos personales y públicos, en un intercambio de información que fluye velozmente, almacenada o trasmitida en formato digital a través de nubes o archivos digitales cargados de megabytes, kilobytes, terabytes, etc.

Las memorias flash USB y otros dispositivos de almacenamiento, son fuentes donde se archiva todo contenido compartido y creado en los medios tecnológicos (celular, computador, tablets, entre otros), en las que se recogen y se registran las actividades, gustos, tendencias, imágenes y escritos de las personas, quedando al descubierto la sensibilidad y fragilidad de la información que pueden llegar a contener los medios digitales, puesto que en el almacenamiento se conserva el registro de archivos personales y públicos.

Avances tecnológicos que no solo han sido de gran utilidad para la modernización de la sociedad, sino que, además, sin proponérselo han permitido que de manera más ágil evolucionen las formas y métodos criminales, al punto que nuestra legislación ha tenido que crear nuevos tipos penales para proteger la información y los datos de atentados contra la confidencialidad, integridad, disponibilidad de los datos y sistemas informáticos.

De allí la trascendencia en el proceso penal, que se realice un adecuado tratamiento de la evidencia digital en cada una de sus fases y por cada uno de los servidores públicos o particulares que puedan entrar en contacto con la misma, para que no se afecte su validez como prueba pericial en el sistema penal acusatorio colombiano.

Es por esto, que la investigación forense digital cumple un papel determinante en el logro de la admisibilidad de la información, almacenada o trasmitida en formato digital como medio de prueba en un juicio penal, advirtiendo que la evidencia digital es algo menos tangible que la mayoría de las pruebas físicas y es considerada en una categoría de pruebas frágiles, siendo esta la relevancia de observar estrictamente un adecuado tratamiento de esta clase de evidencias, desde el momento mismo de la recolección y durante las diferentes fases de su tratamiento, permitiendo de esta manera demostrar que esta no ha sido alterada o modificada, sin embargo, en algunos casos se presentan falencias que afectan su validez probatoria.

Este trabajo aborda un recorrido por las distintas fases que comprende el procedimiento de evidencia digital, desde el aislamiento de la escena, recolección, extracción y análisis de la información, culminando con el informe pericial por parte del perito informático, detectando a partir de algunas sentencias las falencias que se presentan en su tratamiento y que afectan su vocación probatoria para finalmente emitir unas conclusiones al respecto.

Lo anterior nos permite tener como objetivo general, describir de manera detallada algunas falencias presentadas en el tratamiento de la evidencia digital que afectan su validez probatoria, especialmente en memorias flash USB y sus consecuencias jurídicas en el sistema penal acusatorio colombiano, para ello se desarrollaron tres objetivos específicos, a saber:

Detallar el tratamiento de la evidencia digital especialmente de memorias flash USB como elemento material probatorio y su uso en desarrollo de la ley 906 de 2004.

Identificar algunas falencias presentadas en las fases de procedimiento de aislamiento de la escena, recolección, extracción y análisis de la información de la evidencia digital.

Indicar las consecuencias jurídicas generadas por las falencias presentadas en el tratamiento de la evidencia digital, especialmente en memorias flash USB que afectan su validez probatoria como prueba pericial en el sistema penal acusatorio colombiano.

Las fuentes para la presente investigación fueron principalmente teóricas dada la naturaleza del proceso jurídico para ampliar los conocimientos referentes a la validez de la evidencia digital en el proceso penal colombiano, desarrollado en cuatro títulos donde el primero aborda la evidencia digital como medio probatorio en el sistema penal acusatorio colombiano, en el segundo se exponen las fases y falencias presentadas en el tratamiento de la evidencia digital, en el tercero se explican algunas consecuencias jurídicas ante dichas falencias y por último se mencionan las conclusiones de este trabajo de investigación.

5.1 Evidencia Digital Como Medio Probatorio

En la legislación penal colombiana, la práctica de pruebas se surte durante la audiencia de juicio oral con la intervención de las partes, en aras de garantizar los principios generales que rigen la prueba judicial, las cuales tienen como finalidad llevar al conocimiento del juez más allá de toda duda razonable, los hechos y circunstancias materia del juicio para determinar o desvirtuar responsabilidad penal del acusado, como autor o participe de la conducta endilgada que se materializa

a través de una sentencia condenatoria o absolutoria según sea el caso, siempre soportada en las pruebas debatidas durante el juicio.

De forma general, prueba es la actividad que permite conocer un resultado, con base en la realización de un análisis exhaustivo de los hechos para determinar la verdad o su falsedad (Valencia, Ramirez , & Vera , 2016), en consecuencia, dentro de las etapas probatorias en el proceso penal se aplican los principios rectores de la prueba.

Según el código de procedimiento penal (Ley 906, 2004), establece como medios de conocimiento: la prueba testimonial, la prueba pericial, la prueba documental, la prueba de inspección, los elementos materiales probatorios, evidencia física o cualquier otro medio técnico o científico, que no viole el ordenamiento jurídico. A pesar de estar enmarcado en el acápite de práctica de pruebas, el legislador deja abierta la puerta para considerar cualquier otro elemento técnico o científico como medio de prueba, es decir, en atención al principio de libertad probatoria los hechos y circunstancia de interés para la investigación, se podrán probar por cualquier medio que no violente garantías fundamentales.

En nuestro medio se han utilizado indistintamente denominaciones como: prueba, evidencia, indicio, elementos materiales de prueba, y elementos materiales probatorios, sin que con ello se haya conseguido claridad acerca de su significado, por el contrario, el uso indiscriminado de los términos ha llevado a una falta de precisión respecto a lo que se quiere significar, mientras que en la redacción de la ley 600 de 2000, se mencionan los términos de "prueba" y "elementos materiales de prueba" sin distinción alguna, la ley 906 de 2004 por su parte utiliza denominaciones como "elementos materiales probatorios y evidencia física" presentándolos como medios cognoscitivos en la indagación e investigación. (Valdés, 2008, pág. 34)

De manera general se entiende por elemento material probatorio y evidencia física cualquier objeto, instrumento o medio de conocimiento conducente al descubrimiento de la verdad, como son huellas, marcas o rastros de origen físico, químico, biológico o electrónico, perceptible a través de los sentidos o mediante la utilización de tecnología forense, cuyo análisis proporciona las bases científicas o técnicas para encaminar la investigación penal, lograr la identificación del autor o autores, y así confirmar o descartar la comisión de una conducta punible y la reconstrucción de los hechos. (Manual del sistema de cadena de custodia, 2018, pág. 10)

Sin embargo, es importante destacar que a pesar que la legislación colombiana trata como sinónimos estos dos conceptos, la expresión elemento material probatorio solo cobra vida cuando el investigador posee una hipótesis que requiere ser probada, en cambio la expresión evidencia física definida como cualquier elemento tangible que se transfiere durante la comisión de un delito y permite objetivar

las observaciones del investigador y además basar en ellas las posibles hipótesis. (Muriel & Ordoñez, 2017)

La evidencia digital inicialmente es considerada como un elemento material probatorio, teniendo en cuenta que desde el momento de su hallazgo será objeto de varios procedimientos en el aspecto técnico y legal, es decir, deberá ser sometida a cadena de custodia, transporte, análisis, control judicial, entre otros. Una vez el perito informático emita los resultados de su análisis, lo hará a través de un informe pericial, que luego de ser aceptado en la audiencia preparatoria e incorporado en el juicio oral, se podrá tener como prueba pericial para ser valorada por el juez de conocimiento.

Del análisis de los elementos materiales probatorios y evidencia física, entre ellos la evidencia digital, específicamente las memorias flash objeto de la presente investigación, se emite un informe de investigador de laboratorio, que luego de haberse surtido las etapas procesales correspondientes, llega a la audiencia de juicio oral donde el perito informático que rindió el informe pericial, brinda su testimonio respecto de su función pericial durante la etapa de práctica de pruebas, y es en ese momento donde podemos hablar de prueba pericial, la cual será valorada por el juez de conocimiento de acuerdo a las reglas de la sana crítica y las máximas de la experiencia.

Se puede afirmar que el dictamen pericial es un medio de prueba que consiste en la aportación de ciertos elementos técnicos, científicos o artísticos, que la persona versada en la materia de que se trate hace para dilucidar la controversia, aporte que requiere de especiales conocimientos. (Cano, 2010, pág. 93)

El peritaje informático es una disciplina que convierte la información contenida en medios informáticos, aunada al conocimiento poseído por una persona sobre tecnologías de la información, en herramientas valiosas para ofrecer certeza o convencimiento al juez sobre unos hechos determinados, es así que a través del peritaje informático la prueba electrónica obtiene verdadera eficacia (Cano, 2010, pág. 103). Lo anterior, significa que el informe pericial para ser valorado por el juez, debe ir acompañado del elemento material probatorio e incorporado por medio del testimonio del perito, quien será interrogado y contra interrogado por las partes en la audiencia de juicio oral.

El actual código de procedimiento penal en su artículo 408 establece quienes pueden ser peritos en Colombia, en armonía con el artículo 236 de la misma norma (Ley 906, 2004), menciona textualmente a los expertos en informática forense, pero en toda la codificación de la norma adjetiva no existe una definición legal de quien es un experto en informática forense ni tampoco una institución encargada de otorgar este tipo de titulación.

En consecuencia, ante el vacío legal podemos decir que un perito informático es una persona que tiene estudios en ingeniería de sistemas, ingeniería en telecomunicaciones, electrónica, electromecánica, mecatrónica o afines, aunque esos perfiles se acomodan a lo que es un perito en informática, nos podemos preguntar ¿que valida un perito en informática?, la respuesta puede ser la experiencia y capacitaciones que tiene con referencia al tema, entre ellos las certificaciones internacionales en el manejo de herramientas informáticas forenses y demás que validen sus competencias.

5.2 Informática Forense

La informática forense es una ciencia forense que se encarga de la preservación, identificación, extracción, documentación e interpretación de la evidencia digital para luego ésta ser presentada en una Corte de Justicia, (Pino S. , 2017), tomando como referencia este concepto del autor, en Colombia la informática forense cada vez asume nuevos retos en la investigación criminal, en atención a que la delincuencia se sirve del uso de la tecnología para cometer delitos, prueba de ello, es la reforma incorporada al código penal mediante ley 1273 de 2009, la cual incorpora tipos penales como el acceso abusivo a un sistema informático, interceptación de datos informáticos, daño informático, uso de software malicioso, entre otros.

Esas nuevas formas de delinquir obligó igualmente a las Instituciones Estatales encargadas de la investigación penal, crear laboratorios de informática forense dotados de sofisticados equipos y personal altamente capacitado como estrategia para contrarrestar la comisión de los mencionados delitos, es así que la Policía Nacional de Colombia por medio de la Dirección de Investigación Criminal (DIJIN) posee laboratorios de informática forense en las diferentes regiones de Policía a nivel nacional adscritos al Centro Cibernético Policial – CECIP- según lo establece la resolución 5839 del 31 de diciembre de 2015 emanada de la Dirección General de la Policía Nacional, así mismo el Cuerpo Técnico de Investigación (C.T.I) posee sus propios laboratorios, encargados de responder a la demanda de solicitudes que realizan las diferentes autoridades competentes en materia informática.

La realidad que en materia criminal se vive, plantea nuevos escenarios que desbordan los conceptos que hasta ahora se venían considerando para "escena" y "lugar". Según Valdés (2008), el concepto de escena debe ser tan amplio que permita entender que podremos estar frente a un espacio tetradimensional (tres dimensiones espaciales y el tiempo) y a la vez en un espacio virtual. Escena es, entonces, un conjunto de lugares espaciales, corporales o virtuales en donde se desarrolló algún tipo de actividad que guarda relación con la conducta que se investiga.

Lo anterior nos permite precisar que los conceptos básicos, se van adecuando ante las nuevas alternativas que se presentan en el Derecho, por cuanto el término de escena ya no se circunscribe a un espacio físico únicamente, sino que se entiende ampliado a un espacio virtual donde actúa la informática forense dada su especialidad.

5.3 Evidencia Digital

Los avances tecnológicos en el mundo son la realidad que vivimos cada día, la era digital transforma y hace la vida de las personas más práctica, acorta distancias, optimiza el tiempo, es decir, de una u otra forma todos tenemos algo que ver con la información digital, situación ante la cual Colombia no puede ser ajena, por el contrario debe estar a la vanguardia de lo que el mundo virtual ofrece, así mismo la criminalidad o ciberdelincuencia avanza de manera concomitante, siendo la informática forense una valiosa herramienta para ser aplicada a la investigación de las diferentes conductas punibles, tanto en lo referente a delitos informáticos propiamente dichos, como aquellos delitos comunes, por ejemplo homicidios, hurtos y demás, que tienen alguna relación directa o indirecta con una evidencia digital como medio de prueba.

Precisando el concepto de evidencia digital se dice que son campos magnéticos y pulsos electrónicos que pueden recogerse y analizarse, usando técnicas y herramientas especiales. A pesar de ser intangibles, constituyen una evidencia. La evidencia digital: a) se puede duplicar en forma exacta, y la copia puede examinarse como si fuera el original; b) Se puede determinar si la evidencia ha sido modificada o falsificada, comparándola con la original; c) es difícil de destruir, inclusive borrándola, pero puede ser recuperada en un disco.

De esto se encarga el forense informático, que dispone de un método y un procedimiento científico, los cuales tienen por finalidad recopilar y manipular las evidencias, respetando la preservación de ellas. La ciencia informática, por lo tanto, estudia las evidencias digitales. (Angulo, 2016)

5.4 Aspectos Legales de la Evidencia Digital

La Constitución Política de Colombia de 1991 consagra en su artículo 29 la garantía del debido proceso, que plantea que toda persona tiene derecho a presentar pruebas y a controvertir las que se alleguen en su contra, igualmente dice que es nula de pleno derecho la prueba obtenida con violación del debido proceso, situación que también abarca la evidencia digital, pues en materia legal, esta deberá cumplir con

todos los lineamientos procesales determinados para cualquier medio probatorio, como medio de convicción para el juez al momento de resolver el problema jurídico.

La ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones", comúnmente llamada ley de comercio electrónico, no define el término de evidencia digital sino que define el mensaje de datos como: "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), internet, el correo electrónico, el telegrama, el télex o el telefax.", por virtud del principio de la equivalencia funcional equipara el documento electrónico al documento manuscrito y le da el mismo valor probatorio, es decir, que el mensaje de datos se convierte en evidencia digital cuando el mismo es sometido al rigor de un manejo técnico con vocación probatoria dentro de una investigación penal.

Es importante recordar que la norma mencionada establece igualmente los requisitos de validez jurídica de los mensajes de datos, es decir, que sea escrito (art. 6), que tenga una firma (art. 7) y sea original (art. 8) (ley 527, 1999), si se cumplen estos requisitos tienen el valor que más adelante brindan los artículos 10 y 11 que regulan la admisibilidad, fuerza probatoria y también los criterios para valorar probatoriamente los mensajes de datos, en otras palabras se puede decir que el mensaje de datos es tomado como prueba dentro de un proceso judicial cuando se establezca la confiabilidad en la forma como se generó, conservó y de acuerdo a la identificación del autor del mismo.

La ley 1273 de 2009, introdujo nuevos tipos penales a nuestra legislación punitiva, que adolecía de regulación frente a delitos informáticos no consagrados originalmente en el código penal de 2000, buscando regular nuevas conductas como medio de control social y poner freno a la ciberdelincuencia.

Con la expedición de la ley 1928 del 24 de julio de 2018 "Por medio de la cual se aprueba el *Convenio Sobre la Ciberdelincuencia* adoptado el 23 de noviembre de 2001 en Budapest", Colombia incorporó a su legislación interna el llamado convenio de Budapest, al cual se han adherido más de 56 países que buscan edificar una política mundial contra la ciberdelincuencia basada en la cooperación internacional, así mismo fortalece las leyes y regulaciones nacionales contra el ciberdelito de todo nivel.

5.5 Evidencia Digital y su Manipulación Como Material Probatorio en Colombia

En la actualidad el auge de las herramientas informáticas tanto a nivel físico como lógico (hardware y software), convirtieron a este tipo de tecnología no solo en herramientas de apoyo al trabajo, si no en un modo de vida por la necesidad de estar conectada permanentemente en un mundo cada vez más globalizado. En consecuencia, la ocurrencia de los delitos informáticos tanto en las organizaciones como en las personas naturales, no debería ser motivo para que estos se beneficien de todas las bondades que brinda la tecnología, situación que genera nuevos retos profesionales frente a controles que permitan establecer un nivel de seguridad en la información.

Para que este material digital tenga relevancia debe contar con parámetros exigidos ante el sistema penal acusatorio colombiano como: la calidad de la prueba, preservación, legibilidad y relevancia, incentivo para la estructuración de parámetros a considerar en la manipulación de archivos digitales dentro de memorias flash, convirtiéndose en prueba pericial para el apoyo investigativo del caso.

Como se han presentado casos donde la manipulación de este tipo de evidencia no se ejecuta con diligencia, que genera una pérdida de material probatorio o información necesaria en la aclaración de un caso, es en la labor del peritaje la resolución de estas necesidades de conserva y recopilación de material significativo para la labor investigativa.

Por ello, es necesario reconocer dentro del derecho procesal penal la importancia del tema probatorio, enmarcando el correcto manejo de la evidencia digital como una necesidad primaria en el funcionamiento del sistema penal.

La manipulación de material informático y su relevancia presentada en un informe pericial como prueba, aporta a nivel general la necesidad por identificar las falencias en los procedimientos presentados en la recopilación, aseguramiento, análisis y presentación de la evidencia digital de todo tipo de archivo en las memorias flash USB.

Bajo el procedimiento de cadena de custodia, surge la necesidad por establecer bases que garanticen el manejo adecuado de este tipo de elementos probatorios para el sistema penal acusatorio Colombiano, por tal motivo, se requiere develar los procesos actuales ejecutados en Colombia para la disposición de estos elementos informáticos, la manipulación de memorias flash USB como herramientas de almacenamiento de archivos digitales que permiten la conserva de estas evidencias, calificado como análisis forense digital o criminalística informática, procedimiento

de peritaje que compete la investigación de todo material tecnológico encontrado en una escena del crimen.

En consecuencia, es preciso la elaboración y establecimiento de parámetros en los procesos de análisis forense de material informático en nuestro país, situación que ha permitido una evolución en términos jurídicos y procedimentales a beneficio del derecho.

Unidades de Almacenamiento

La unidad de almacenamiento es un dispositivo capaz de leer y escribir información con el propósito de almacenarla permanentemente, en la actualidad contamos con muchas clases y categorías de unidades de almacenamiento, facilitando así, el transporte de información y la distribución de la misma en distintos equipos, además estas unidades sirven como herramienta de almacenamiento de datos de manera segura, también conocidos como back up.

Para el profesor Pino (2009, pág. 186) existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido o memoria sólida (como las memorias flash USB) y los dispositivos ópticos (como los discos compactos y DVD). Existe una gran cantidad de memorias flash USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, compact flash, tarjetas XD, memory stick, etc.

La memoria principal o primaria es un recurso importante de las computadoras, que habitualmente denominamos memoria RAM (Random Access Memory), y debido a una limitación tecnológica esta es volátil, es decir, conserva la información mientras el dispositivo se encuentre encendido, conservándola de manera temporal pero una vez apagado se pierde la información, por esa razón es trascendental hacer la diferenciación con los dispositivos objeto de estudio, refiriéndonos a las memorias flash USB, por cuanto estas últimas usan una memoria sólida como se refirió anteriormente, para almacenar la información de forma constante, es decir, no son volátiles.

El almacenamiento en flash se refiere a cualquier tipo de unidad, repositorio o sistema que utiliza memoria flash para conservar los datos durante un período de tiempo prolongado, es ampliamente utilizada en dispositivos de consumo, los teléfonos inteligentes y reproductores de MP3 han abandonado en gran medida la unidad de disco duro (HDD) mecánica; pues flash proporciona ventajas en cuanto a su capacidad de compactarse y su consumo de energía, en las computadoras portátiles, el almacenamiento flash ofrece la ventaja adicional de ser más resistente a los golpes de aceleración gravitatoria alta y las caídas que estos dispositivos a menudo reciben en su vida móvil.

El Dr. Fujio Masuoka inventó NOR y NAND flash, los dos principales tipos de memoria flash, mientras trabajaba para Toshiba en los años ochenta, en comparación con el lento proceso utilizado por EEPROM, se denomina flash por la capacidad del nuevo formato para ser programado y borrado en bloques grandes. NOR y NAND tienen el nombre por la forma en que están interconectadas las puertas flotantes de las celdas de memoria que contienen datos, en configuraciones que se parecen en cierta medida a una puerta lógica NOR o NAND.

Los principales fabricantes de chips de memoria flash NAND incluyen Intel, Micron Technology, Samsung, SK Hynix, Toshiba y la división SanDisk de Western Digital. Los principales fabricantes de memoria flash NOR incluyen a Cypress Semiconductor, Macronix, Microchip Technology, Micron Technology y Winbond. (Rouse, 2017)

Memorias Flash

La memoria flash es un tipo de almacenamiento portátil constituido por chips en estado sólido sin partes móviles, que tienen la propiedad de conservar los datos cuando se les quita la fuente de alimentación, es decir, cuando se apaga el dispositivo que la usa. Tiene la ventaja de ser muy pequeña y práctica, con resistencia a daños y una gran compatibilidad con equipos portátiles, existen muchos formatos de memoria flash y cada vez podremos disponer de este tipo de almacenamiento con mayor capacidad y en tamaño más reducido.

Las memorias flash se han convertido en algo importante para aquellos productos que necesitan una pequeña cantidad de almacenamiento no volátil para datos y programas.

Las celdas de memoria flash pueden gastarse al cabo de un determinado número de ciclos de escritura, que se cifran generalmente entre 100.000 y un millón, dependiendo del diseño, de la celda y de la precisión del proceso de fabricación. El principal mecanismo de destrucción, lo constituye el daño acumulativo que se produce sobre la puerta de flotación de la celda debido a los elevados voltajes empleados, de forma repetitiva para borrar la celda, la capa de óxido se rompe o los electrones se acumulan en la puerta de flotación.

Los fabricantes de memoria flash tienen en cuenta este fenómeno e incorporan celdas adicionales que pueden sustituir a las gastadas, además, muchos fabricantes de sistemas de memoria flash destinados al almacenamiento de datos utilizan una técnica denominada de nivelación que consiste en desplazar los datos alrededor del chip para que cada celda se "gaste" lo más uniformemente posible. (Hilari, 2006)

Diferencia entre Memoria Nand y Nor

En la memoria Flash NAND, los transistores se conectan en serie entre ellos, este tipo de memoria accede a las direcciones de memoria de las células en el orden de página, palabra y finalmente bit. El hecho de ser un tipo de memoria Flash más sencilla de construir, permite aumentar la densidad de transistores por célula de memoria, por tanto, son capaces de almacenar muchos más datos. Esto también le hace tener una capacidad de grabar datos a una velocidad sensiblemente rápida. También es un tipo de memoria Flash que es más permisiva si una célula de memoria no es completamente perfecta.

Las características inherentes de este tipo de memoria hacen que sea la más utilizada para los dispositivos de almacenamiento sólido en el mercado, ya sean fijos, como los SSD, o portátiles como las tarjetas de memoria y los pendrives USB.

La memoria NOR no tiene tolerancia ninguna con las células defectuosas, por lo que cada célula ha de ser siempre perfecta. A diferencia también de la NAND, para borrar las células de memoria NOR hay que borrar la célula entera, en lugar de poder borrar solo un bloque de la información almacenada, como sí permite la memoria NAND.

Así como la memoria NAND es rápida a la hora de grabar datos, la memoria NOR es rápida a la hora de leerlos. Estas características hacen que la memoria NOR sea aquella que más se emplea en los chips de memoria donde se instala la BIOS (Basic input-output system) de las placas base y de las tarjetas gráficas. (Usera, 2018)

Ventajas y Desventajas de la Memoria Flash USB

Como se mencionó, la memoria flash USB tiene unas características especiales que la diferencian de otras unidades, por el tipo de tecnología utilizada y por el puerto que permite conectar periféricos a una computadora según el significado de sus siglas USB (universal serial bus).

Por lo anterior es importante conocer las ventajas y desventajas que ofrecen las memorias flash USB, y que implicación pueden tener como evidencia digital por la información en elas contenidas.

Ventajas

La gran ventaja de los dispositivos de memoria es su portabilidad.

Una tarjeta de memoria flash no requiere energía para funcionar y no tiene

partes móviles, se puede decir que no hay peligro de perder información.

Las memorias flash USB duran más que otras formas de memorias informáticas.

En caso de una caída accidental probablemente no se tiene ningún efecto en la información contenida en él.

Los cambios de temperatura o presión normalmente no afectan.

La información se puede borrar, añadir o eliminar fácilmente.

Proceso de recolección de basura: El sistema recupera la cantidad de páginas muertas acumuladas, que realiza un erase, operación para que las páginas muertas estén disponibles nuevamente.

Nivelación de desgaste: garantiza que todos los bloques borrados se realicen de manera uniforme para lograr una vida útil más larga de la memoria flash.

Desventajas

Falta de privacidad de los datos, teniendo en cuenta que en caso de olvido o perdida cualquier persona puede acceder a la información.

En cualquier momento puede dejar de funcionar por que ha variado el voltaje mientras estaba conectado.

Usar la memoria flash durante muchos años constantemente.

Se puede perder fácilmente por su tamaño o incluso por olvido dejarla conectada en algún dispositivo.

Como se puede usar en cualquier ordenador, son susceptibles a ataques de virus.

Se puede dañar o perder información, al omitir el procedimiento de expulsar correctamente. Con dispositivos flash, las celdas de memoria solo se pueden escribir en un número limitado de veces, típicamente entre 10,000 y 1,000,000 de veces, después de lo cual se vuelven inestables por desgaste.

Pueden retener los datos un mínimo de 10 años en ausencia de alimentación. Es decir, se puede esperar que después de 10 años sin estar conectado, la memoria flash pueda sufrir un deterioro electromagnético por el cual se difumine la información de las cargas eléctricas.

5.6 Tratamiento de la memoria flash USB como evidencia digital

Si bien es cierto, la evidencia digital debería tener unos protocolos en su tratamiento para que sirva como elemento material probatorio en un proceso penal, en Colombia no se encuentra unificado en las instituciones del Estado dichos protocolos, así las cosas, al hacer remisión puntualmente a las memorias flash USB, se evidencia que en nuestro país tampoco existe un protocolo o guía de mejores prácticas específicamente para este tipo de tecnología.

Un estudio publicado en la séptima conferencia Australiana forense digital, concluyó que hay poca evidencia que se haya llevado a cabo investigación de unidades de memoria flash en beneficio para la Policía de campo, así mismo menciona que se necesita más investigación sobre los mecanismos de lectura flash, utilizados por las herramientas de flasheo para adaptar estos mecanismos para su uso, en la próxima generación de herramientas de adquisición de datos forenses. (Sansurooah, 2009)

Lo anterior evidencia que a pesar de la búsqueda de investigaciones sobre memorias flash USB, es poco o nulo lo que se ha publicado para evitar las falencias que se puedan presentar en el tratamiento de estos dispositivos como evidencia digital, teniendo en cuenta que por su naturaleza o características tecnológicas, su tratamiento deber ser diferente a otros tipos de evidencia digital, debiendo obligatoriamente acudir a las mejores prácticas que en materia de evidencia digital se han publicado de manera general.

Por ello, es importante generar la inquietud para que a futuro se genere un proceso de extracción de la información, basado en un procedimiento exclusivo para las memorias flash USB, teniendo en cuenta las ventajas y desventajas mencionadas anteriormente, así como los software que permitan recuperar integralmente toda la información que se requiere en la investigación penal, por ejemplo, un estudio reflejó que desde el punto de vista forense, el pequeño destello o unidades pueden hacer que la vida de los expertos forenses sea muy problemática cuando sea necesario adquirir y analizar su contenido. Herramientas forenses no siempre permiten la adquisición y recuperación exitosa de todos los datos que se han almacenado en los dispositivos, porque la mayoría de los datos eliminados en el tiempo que podrían ser evidencia útil sobre el delito perpetrado, no puede ser adquirida. La única forma de asegurarse de adquirir todos los datos de una memoria flash, es adquirir los datos en la capa más baja donde se puede esperar evidencia. (Sansurooah, 2009)

Como no existe un procedimiento particular para el tratamiento de las memorias flash USB específicamente, los peritos en informática forense al realizar el análisis de estos elementos materiales probatorios, deben acudir al procedimiento de evidencia digital de manera general para todas las evidencias digitales.

5.7 Procedimiento de Cadena de Custodia

El acto legislativo 03 de 2002 introdujo una modificación al artículo 250 de la Constitución Política de Colombia con el fin de implementar el sistema penal oral acusatorio, mencionando dentro de las funciones de la Fiscalía General de la Nación en su numeral tercero lo referente a la cadena de custodia, así: *"… 3. Asegurar los elementos materiales probatorios, garantizando la cadena de custodia mientras se ejerce su contradicción. …"*.

La cadena de custodia es un mecanismo que tiene como finalidad demostrar la autenticidad de los materiales probatorios y la evidencia física, en este sentido, es concebida como un conjunto de medidas que tienen como fin preservar la identidad o integridad de los elementos materiales probatorios o evidencia física y asegurar el poder demostrativo de la prueba.

En desarrollo del articulo 250 superior, la ley 906 de 2004 dentro del libro II Título I llamado: la indagación y la investigación dispuso el capítulo V al cual denominó "Cadena de Custodia" que comprende los artículos 254 al 266, indicando que la cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente.

5.8 Fases en el Tratamiento de la Evidencia Digital

A continuación, se expone el uso de evidencia digital como material probatorio en procesos penales, de manera breve se hace una explicación de cada fase de acuerdo a los procedimientos estandarizados para su manipulación, sin embargo, se hace una corta referencia al modelo PURI implementado por expertos en Argentina que tienen la misma finalidad en el tratamiento de la evidencia digital.

Modelo "PURI": Es importante referir que en Argentina se desarrolla un modelo denominado PURI "Proceso Unificado de Recuperación de Información", como resultado de proyectos de investigación desarrollado por el Grupo de Investigación en Sistemas Operativos e Informática Forense de la Universidad FASTA y por el INFO-LAB Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense) en Mar del Plata durante los años 2010 al 2016; modelo que consiste en una secuencia iniciando el caso, luego vienen las fases de relevamiento, recolección, adquisición, preparación, extracción y análisis y finalmente la presentación del resultado.

> Las fases iniciales de relevamiento y recolección, son de tipo exploratorio y es esperado que sean ejecutadas por un profesional con perfil orientado a la investigación, donde el técnico tenga un rol de asistencia y asesoramiento. En cambio, las fases subsiguientes, esto es: adquisición, preparación, extracción y análisis, y presentación, son netamente de informática forense, y se espera que las tareas involucradas sean desarrolladas por profesionales especializados en esta temática, con la asistencia que se requiera de los investigadores del caso. (Grupo de investigación en sistemas operativos e informática forense InFo-Lab, 2016, pág. 279)

5.9 Procedimiento Para el Tratamiento de la Evidencia Digital

Por su parte el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC- de Colombia emitió la Guía No. 13 denominada Evidencia Digital, por medio del cual estableció parámetros para el procedimiento de evidencia digital para la correcta ejecución de la recolección, análisis y manipulación de la misma, la cual se divide en cinco fases, así: I. aislamiento de la escena, II. Identificación de fuentes de información, pasos iniciales de adquisición de fuentes de información, III. Recolección y examinación de información, IV. Análisis de la información y V. Reporte, basados en las normas NTC ISO/IEC 27035 vigente, así como también la publicación especial de NIST SP800-86 (National Institute of Standards and Technology – (Guide to Integrating Forensic Techniques into Incident Response). (Ministerio de Tecnología de la Información y las Telecomunicaciones, 2016)

El procedimiento de evidencia digital que versa principalmente sobre la información electrónica, dada su naturaleza de fragilidad y volatilidad, es un procedimiento diferente a los demás en materia criminalística, es decir, no es lo mismo cuando nos encontramos frente a un elementos material probatorio como un cadáver, un arma de fuego u otros, que a pesar de requerirse unas técnicas para su manipulación, el elemento se conserva; no sucede lo mismo con la información, por cuanto una acción en segundos puede borrar la evidencia, tan solo con apagar un equipo de cómputo que estaba prendido o haciendo uso de algún software que la elimine.

Aislamiento de la escena. Esta fase es una de las más importantes dentro del proceso de investigación por ser la primera de ellas, toda vez que dependiendo de la correcta forma en que se lleve a cabo el aislamiento de la escena, así mismo será el posterior éxito en el desarrollo de los pasos siguientes como el análisis y presentación del informe pericial o testimonio del perito.

Aquí se corre el riesgo de una indebida manipulación de la evidencia si no se llevan a cabo los pasos o recomendaciones mencionados en la guía, que nos pueden generar diversas situaciones como perder información volátil de gran utilidad, omitir el registro fotográfico de la escena, apagar dispositivos cuando se encuentren prendidos sin aplicar técnicas determinadas para ello o dado el caso llegar a contaminar de algún modo la evidencia que puede servir de prueba en el juicio.

El paso a seguir de acuerdo a lo dicho precedentemente, es realizar el registro de actuación del primer responsable, posteriormente se hace la fijación y documentación del lugar del hecho a cargo del personal de Policía Judicial, seguidamente la recolección, embalaje y rotulado de los elementos materiales probatorios y evidencia física, e iniciar el procedimiento de cadena de custodia aplicando las técnicas y disposiciones del manual del sistema de cadena de custodia, para su posterior análisis en el laboratorio de informática forense.

El éxito de los hallazgos presentados de la evidencia solo es proporcional al cuidado y seguimiento que se le da a ésta, documentando cada acción, traslado, acceso a la información y en el momento de ser dispuesto en juicio, tendiendo claridad sobre el responsable de cada movimiento, gestión o manipulación de la evidencia. En consecuencia, la Fiscalía dispone de un formato estándar para el seguimiento de la cadena de custodia, que debe ser diligenciado en su totalidad sin errores por las personas involucradas en la investigación con veracidad, este documento no admite errores, tachones ni enmendaduras, de ser diligenciada de forma incorrecta, el análisis investigativo sobre la evidencia, por más documentado que se encuentre, podría perder peso ante el estrado. (Vanegas, 2015)

Identificación de fuentes de información. En esta fase le corresponde al técnico identificar fuentes potenciales de información de donde se puedan extraer datos para soportar el proceso de evidencia digital.

Recolección y examinación de información. Esta secuencia requiere especialmente que el experto en informática forense realice el análisis sobre la copia de la imagen de datos, con el fin de conservar la evidencia original que se encuentra sometida al procedimiento de cadena de custodia desde el inicio.

Para llevar a cabo esa copia de la imagen original de manera idéntica, la Fiscalía General de la Nación emitió el "*Instructivo para el hallazgo, identificación, embalaje de la evidencia de tipo digital" y el "Instructivo para extracción de la huella digital a través del HASH MD5"* que consiste en extraer la huella digital del documento electrónico, la cual podríamos decir que se asimila al documento de identificación de las personas, se dice que para que un archivo generado en el día de hoy se parezca a otro en el futuro deben ocurrir 640 elevado a la 128, es decir, tienen que ocurrir 340 billones de billones de billones de billones de ocurrencias.

En esta fase también es importante mencionar que la Policía Nacional de Colombia tiene documentado un proceso denominado: *realizar imágenes forenses*, identificado con el código

2DC-PR-0033 que tiene como objetivo obtener una copia física (bit a bit) de dispositivos de almacenamiento digital vinculados en un proceso investigativo para obtener la réplica original del dispositivo a analizar.

Así mismo tiene documentado otro proceso denominado: *tratamiento y análisis de la evidencia digital*, identificado con el código 2DC-PR-0002 que tiene como objetivo establecer los pasos necesarios para tratar, analizar, identificar, preservar y presentar la evidencia digital de manera que ésta sea legalmente aceptable.

Análisis de la información. Una vez se cumpla las fases anteriores, se procede a realizar un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada.

Reporte. Es la última fase del proceso que condensa toda la información y evidencia obtenida en la fase de análisis, en términos generales contiene el resultado obtenido del trabajo realizado, cómo y porqué fueron utilizados las diferentes herramientas y procedimientos para recolectar y analizar la información, entre otras, que finalmente se materializa en un informe pericial para que surta los efectos jurídicos correspondientes en el proceso penal.

5.10 Falencias Presentadas en el Tratamiento de la Evidencia Digital

En la fase de aislamiento de la escena se pueden cometer muchos errores, que pueden llegar a invalidar la evidencia a futuro dependiendo de la gravedad o magnitud de la falencia y el impacto generado sobre el elemento material probatorio, bien sea en el ámbito técnico o legal.

Podemos tomar como ejemplo práctico un caso de público conocimiento a nivel nacional, como fue la muerte del comandante guerrillero de las FARC, Luis Edgar Devia Silva conocido con el Alias de Raúl Reyes, en desarrollo de la operación FENIX, que para el tema que nos ocupa en la fase I de aislamiento de la escena, se identificaron dos falencias cometidas por personal de policía Judicial en el manejo de la evidencia encontrada en el campamento guerrillero, una de ellas es el hecho de haber recolectado evidencias en otro país (Ecuador) sin tener la autorización para ello y el otro hecho es haber realizado copia de archivos sin haber dejado constancia en las actas, como lo refirió la sentencia de la Corte Suprema de Justicia en radicado 29.877.

Así las cosas, el órgano de cierre en materia penal en Colombia, determinó que dichos elementos materiales probatorios no podían tenerse en cuenta porque estaban viciados, en consecuencia, fueron excluidos de cualquier proceso, en atención al desconocimiento de las normas de cooperación internacional por el indebido procedimiento de recolección y manipulación de personas inexpertas como son los funcionarios de la policía judicial antes de ser enviados al laboratorio correspondiente.

Una de las falencias que más se presenta en la fase de aislamiento de la escena, es la incorrecta manipulación de la evidencia digital, en la mayoría de los casos por desconocimiento ante la falta de capacitación de los funcionarios tanto Policías como de investigadores que llegan al lugar de los hechos.

Otro caso documentado como soporte de las falencias que se presentan en la manipulación de la evidencia digital, es lo concerniente a la cadena de custodia, según providencia emitida por la sala penal del Tribunal Superior de Bogotá dentro de expediente 110012204000200700818 cuando en desarrollo de operaciones militares en enfrentamiento con guerrilleros de las FARC en la Uribe Meta y Ataco –Tolima, los registros de cadena de custodia tenían todos los defectos que pretenden evitar los manuales expedidos para el efecto, porque la documentación presentaba graves modificaciones o alteraciones que permitieron advertir borrado, tachaduras, enmiendas y retoques.

En este caso también el Tribunal determinó al resolver el recurso de apelación, que debía excluirse toda la prueba derivada de los discos duros aportados por la Fiscalía, situación que afectó el normal desarrollo de la investigación, al dejar sin efecto jurídico o validez probatoria una evidencia con capacidad demostrativa de una conducta punible.

La afectación procesal del elemento material probatorio inicia desde el momento de la recolección del mismo, por el mal procedimiento de cadena de custodia, desde ahí parten las falencias porque en ocasiones no se hace la adecuada recolección de la evidencia digital y cuando llegan los elementos al laboratorio presentan problemas, por ejemplo: una memoria flash a la que no se le haya hecho la debida recolección, porque no fue dejada fuera del alcance de la energía estática, un imán, un Garrett o similares, y si alcanza a tener contacto con él, puede llegar al laboratorio sin utilidad para realizar un análisis forense.

Otra falencia especialmente en la fase de recolección y análisis de la información donde actúan directamente los peritos informáticos, se pudo evidenciar en el caso tratado en sentencia 45.375 emanada de la Sala de Casación Penal de la Corte Suprema de Justicia, porque no se realizó la audiencia de control de legalidad posterior que ordena el artículo 237 de la ley 906 de 2004.

Para el Tribunal Superior de Bogotá quien conoció el caso por vía de apelación encontró ilegal la labor del perito, quien fue el encargado de obtener la imagen forense del medio de almacenamiento y extraer de allí información incriminante contra el procesado, porque no apareció acreditado adecuadamente que dichas labores de registro hubieran sido llevadas para su control posterior ante un juez de control de garantías.

Si bien es cierto dicha falencia no obedece a la manipulación de la evidencia digital propiamente dicha, el error se tornó en un tema legal por la omisión de realizar el control judicial, del cual se debe acompañar el procedimiento técnico, porque no debemos olvidar que, a pesar de estar frente a conductas punibles, los presuntos responsables gozan en esa etapa del principio de presunción de inocencia, debido proceso y otras garantías constitucionales que no se deben desconocer.

Otro caso resuelto por el juzgado 46 penal del circuito con funciones de conocimiento de Bogotá dentro del radicado 110016000050201631680 adelantado por el delito de ocultamiento, alteración o destrucción de elemento material probatorio y otro, emitió sentencia absolutoria a favor de los procesados, donde el juez tuvo como prueba para su valoración, informes periciales basados en evidencia digital.

La sentencia, refirió que un perito aportado por la defensa, concluyó que el equipo pericial de informática forense que abordó el análisis de la evidencia digital extraída de los dispositivos de telefonía celular, desarrolló su labor pericial a partir de los reportes de extracción y no desde la extracción total obtenida por la agencia ICE, lo anterior llevó a generarse una duda en el convencimiento del juez.

En el caso mencionado, independientemente de la decisión tomada por el juez, se puede observar que la evidencia digital jugó un papel protagónico en la resolución del caso, porque desde el inició de la investigación los elementos materiales probatorios fundamentales, eran los equipos electrónicos de los investigados.

La falencia identificada frente al caso concreto, lo advirtió el perito de la defensa al manifestar que el análisis en el laboratorio por parte de la Fiscalía se realizó a partir de los reportes de extracción y no desde la extracción total, es decir, al parecer se hizo de manera incompleta, lo que generó duda razonable y aplicación del principio de indubio pro reo.

Por ser la evidencia digital una temática relativamente nueva para muchas personas que intervienen en el sistema penal oral acusatorio, de los casos referenciados y muchos más que se han tramitado en los estrados judiciales, se observa una constante en los errores cometidos y es el desconocimiento de la técnicas establecidas para este tipo de elementos digitales.

Si bien es cierto, la Policía Nacional de Colombia a través de la Dirección Nacional de Escuelas (DINAE) por medio de la Facultad de Investigación Criminal, tiene en su oferta educativa para los funcionarios que ejercen funciones permanentes de Policía judicial, el diplomado en Informática Forense y un seminario en Procesamiento de Evidencia Digital, así mismo la Escuela Judicial Rodrigo Lara Bonilla perteneciente a la rama judicial, tiene a su disposición varios cursos para sus empleados, por ejemplo: taller de uso de herramientas de informática, curso de la prueba penal y las nuevas tecnologías, curso sobre tecnologías de la información y las comunicaciones en la gestión judicial, ello no ha sido suficiente para que todos los funcionarios tengan un mínimo de capacitación frente a estas temáticas.

Es evidente entonces, que los funcionarios que intervienen en el tratamiento de la evidencia digital tanto en la parte técnica como legal, refiriéndonos a los investigadores, peritos, jueces, fiscales y defensa, en algunas ocasiones no están lo suficientemente capacitados en temas digitales.

La ausencia de las habilidades más básicas y fundamentales para la investigación de los crímenes de alta tecnología impide su apropiado juzgamiento. Sin un nivel de educación y entrenamiento adecuado los jueces podrían pasar por alto o malinterpretar evidencia crítica para la resolución de un caso que involucre sistemas informáticos. (Cano, 2010, pág. 222)

5.11 Consecuencias Jurídicas Ante las Falencias en el Tratamiento de la Evidencia Digital

Desde el punto de vista legal, las falencias que se presenten en el tratamiento de la evidencia digital, trae consigo consecuencias jurídicas que afectan el debido proceso en detrimento de los intereses de las partes, tanto defensa como fiscalía, incluyendo además a las víctimas, es por ello que se mencionan las consecuencias que se pueden presentar en materia procesal penal, entre ellas la exclusión, inadmisión, rechazo de la prueba y la nulidad.

Exclusión de la Prueba. Como se mencionó inicialmente, la Constitución Política en su artículo 29 que trata sobre el debido proceso establece que es nula toda prueba obtenida con violación del debido proceso, desarrollado como principio rector por el artículo 23 de la ley 906 de 2004.

La prueba ilegal es aquella que se obtiene con la ausencia de algún requisito formal dispuesto en la ley y por su parte la prueba ilícita es la que se obtiene con violación de las garantías constitucionales, las cuales sufren la misma consecuencia procesal en caso de configurarse alguna de ellas, esto es, que por parte del juez se decrete su exclusión.

Es importante resaltar que existen excepciones a la regla de exclusión probatoria en materia penal, correspondiéndole al juez verificar que la prueba de la que solicitan exclusión, pese a su relación con una prueba ilícita o ilegal, la prueba que se derive de ella pueda ser tenida en cuenta bajo tres factores que son el vínculo atenuado, fuente independiente o descubrimiento inevitable, explicando la Corte Constitucional que por **vínculo atenuado** se ha entendido que si el nexo existente entre la prueba ilícita y la derivada es tenue, entonces la segunda es admisible atendiendo al principio de la buena fe, como quiera que el vínculo entre ambas pruebas resulta ser tan tenue que casi se diluye el nexo de causalidad; la **fuente independiente**, según el cual si determinada evidencia tiene un origen diferente de la prueba ilegalmente obtenida, no se aplica la teoría de los frutos del árbol ponzoñoso; y el **descubrimiento inevitable**, consistente en que la prueba derivada es admisible si el órgano de acusación logra demostrar que aquélla habría sido de todas formas obtenidas por un medio lícito. (Sent. C-591, 2005)

El código de procedimiento penal dispone que el juez excluirá la práctica o aducción de medios de prueba ilegales, incluyendo las que se han practicado, aducido o conseguido con violación de los requisitos formales, esto quiere decir, puntualizando sobre la evidencia digital, que aquella prueba que fue obtenida bajo criterios de ilicitud o ilegalidad, van a ser excluidos del proceso y no podrán ser tenidas en cuenta para que el juez las considere en su valoración probatoria en la sentencia.

Como se expuso en los casos prácticos, el desconocimiento de las normas de cooperación internacional por el indebido procedimiento de recolección de la evidencia digital, la indebida manipulación por personas inexpertas de policía judicial antes de ser enviados los elementos materiales probatorios al laboratorio correspondiente, la omisión o indebida aplicación del procedimiento de cadena de custodia, entre otras malas prácticas realizadas en las distintas fases del procedimiento de evidencia digital, a pesar de los esfuerzos de los funcionarios de Policía judicial y Fiscales para hacer valer los elementos materiales probatorios o evidencia digital como prueba dentro del proceso penal, no es suficiente ante la declaratoria de exclusión probatoria por parte del juez.

La exclusión probatoria es una infortunada consecuencia en la parte procesal, toda vez que, si el fiscal hasta la audiencia preparatoria cuenta con pocos elementos materiales probatorios para sustentar su teoría del caso, o en algunos casos puede pasar que la evidencia digital se convierte en el único medio para demostrar determinada conducta, se verá entonces frustrada de esta manera la administración de justicia.

Rechazo de la Prueba. Los elementos materiales probatorios y evidencia física que debían descubrirse y no lo fueron, no podrán ser aducidos al proceso ni convertirse en prueba, ni practicarse durante el juicio, toda vez que el juez está obligado a rechazarlos, es decir, para el caso de la evidencia digital, es importante tener en cuenta que a pesar de realizar un correcto procedimiento de evidencia digital en su parte técnica, no es suficiente si el fiscal del caso omite realizar el correspondiente descubrimiento a partir de la audiencia de Acusación y así mismo para la defensa su obligación nace a partir de la audiencia preparatoria.

Esta omisión en el descubrimiento probatorio que afecta la igualdad de armas, salvo que se acredite que su descubrimiento se haya omitido por causas no imputables a la parte afectada, genera como consecuencia el rechazo de la evidencia digital, que también puede catalogarse como una falencia posterior, pero de igual manera afecta su validez y no será tenida en cuenta por el juez.

*Inadmisión de la Prueba***.** Para la práctica de pruebas durante la audiencia de juicio oral es importante conocer que las que se practiquen deben ser pertinentes, conducentes, útiles y racionales, como lo expresó la Corte Suprema de Justicia en sentencia de Casación Penal radicado 41.741, lo anterior quiere decir, que si los medios de prueba no cuentan con estos atributos, correrá con la consecuencia jurídica para este tipo de situación que es la inadmisión.

En ocasiones, a pesar de encontrarnos frente a una prueba pertinente, puede ser inadmitida siempre y cuando, (i) exista peligro de causar grave perjuicio indebido, (ii) exista probabilidad que genere confusión en lugar de mayor claridad al asunto o exhiba escaso valor probatorio y (iii) que sea injustamente dilatoria del procedimiento.

Aquí es importante resaltar que la inadmisión por temas de conducencia o pertinencia, no es atribuible directamente al tratamiento que se le haya dado a la evidencia digital, sin embargo, la inadmisión decretada por parte del juez, porque, por ejemplo, tenga un escaso valor probatorio o no guarde relación con el hecho, dejara por fuera dicho medio de prueba de la valoración probatoria que le corresponda hacer al juez.

El proceso penal es una dinámica interesante para cada una de las partes, es por ello que, durante un juicio, los Abogados tienen que objetar cada vez que el juez permite la introducción de alguna evidencia que pueda resultar impropia, y, por otra parte, tienen que objetar también cada vez que el juez deniega la admisión de una evidencia considerada propia o factible. (Fierro, 2012, pág. 1037)

Nulidad. La legislación procesal penal oral acusatoria Colombina establece que se puede generar la nulidad bajo tres vértices, nulidad derivada de la prueba

ilícita, nulidad por incompetencia del juez y nulidad por violación a garantías fundamentales, las cuales a la luz del principio de taxatividad, no le es posible al juez decretar ninguna nulidad por causal diferente a las mencionadas.

Según la Corte Suprema de Justicia en sentencia 30.960, la declaratoria de nulidad es sin lugar a dudas una medida de excepcional carácter, de mayúscula trascendencia en el proceso judicial, teniendo en cuenta que la anulación es el mayor castigo a la actuación, tanto que obliga a rehacerla; luego, una determinación de dicha magnitud sólo procede cuando la irregularidad que se detecta afecta realmente garantías de los sujetos procesales, ora porque se desconocen las bases fundamentales del debido proceso (instrucción – juzgamiento) ya porque se desconocen garantías defensivas. (Corte Suprema de Justicia, 2010).

A pesar de lo anterior, se ha dicho jurisprudencialmente que cualquier irregularidad nimia, intrascendente o irrelevante no es causal de nulidad en el proceso penal, atendiendo los principios rectores de las nulidades.

Es importante hacer la claridad entre nulidad y exclusión, en el entendido que la vulneración de las garantías en el procedimiento investigativo no genera nulidad, genera exclusión del elemento material probatorio o de la evidencia física.

Frente a la declaración de prueba ilícita o de prueba ilegal, la consecuencia no es la nulidad del proceso, sino la exclusión del medio, pues la nulidad de pleno derecho se predica de las pruebas, de conformidad con el artículo 29 de la Constitución Nacional. (Corte Suprema de Justicia, 2014)

5.12 Conclusiones

En el ámbito legal la normatividad Colombiana ha venido nutriéndose cada vez más, no en vano cuenta con leyes importantes y progresivas en materia informática como la ley 527 de 1999 conocida como ley de comercio electrónico, la ley 1273 de 2009 que incorporó nuevos tipos penales y recientemente la ley 1928 de 2018, esta última por medio de la cual se adoptó el convenio de Budapest, que busca edificar una política mundial contra la ciberdelincuencia basada en la cooperación internacional, así mismo fortalece las leyes y regulaciones nacionales contra el ciberdelito de todo nivel.

No existe un procedimiento particular para el tratamiento de las memorias flash USB específicamente, los peritos en informática forense al realizar el análisis de estos elementos materiales probatorios, deben acudir al procedimiento de manera general para todas las evidencias digitales, teniendo en cuenta que forma de asegurarse de recuperar la información de una memoria flash, es adquirir los datos en la capa más baja donde se puede esperar evidencia.

No existe un manual o protocolo único en el manejo de la evidencia digital en Colombia para todos los funcionarios y laboratorios de informática forense, que determine el paso a paso en todas las fases del procedimiento de evidencia digital, como si lo hay para el procedimiento de cadena de custodia denominado "Manual del Sistema de Custodia" y el "Manual Único de Policía Judicial" actualizados recientemente por el Consejo Nacional de Policía Judicial, aplicables a todas las entidades y funcionarios que cumplen funciones de Policía Judicial, sin embargo, cada entidad y laboratorio de informática forense se ciñe a los estándares internacionales.

Se hace necesario que el Consejo Nacional de Policía Judicial, dentro de sus competencias emita un manual único de evidencia digital, que cubra todas las fases del procedimiento de evidencia digital, y sea aplicable a todas las personas y entidades que actúan dentro del proceso penal, así mismo, se deberá incluir dentro de este, un procedimiento especial para el tratamiento de la memoria flash USB.

A pesar de estar documentado el procedimiento de evidencia digital, desde el hallazgo del elemento material probatorio y evidencia física hasta la presentación del informe pericial por parte del informático forense, se comenten errores o falencias en su tratamiento, pero se descubrió como resultado de la presente investigación, que la debilidad más grande se presenta en la fase inicial, es decir, durante la actividad de aislamiento de la escena y recolección de los elementos materiales probatorios, incluyendo el procedimiento de cadena de custodia; pero respecto de las demás fases, se puede decir que los peritos se remiten a los protocolos y procesos de buenas prácticas estandarizados a nivel internacional, en materia de evidencia digital para la extracción y análisis de la información, lo que minimiza enormemente el margen de error en sus procedimientos forenses.

Respecto de los peritos en informática forense, se concluyó que en Colombia, un perito informático forense es un experto en el área de las tecnologías de la información con capacidad y conocimiento técnico-científico en técnicas, herramientas informáticas y protocolos que deben tener una validación científica y producir un resultado preciso y demostrable, ese conocimiento lo adquiere por sus estudios en ingeniería de sistemas y área afines y por su experiencia, sin embargo, no existe una institución en el país que otorgue el título de perito informático.

Se hace necesario que el órgano legislativo tramite una ley, donde fije los parámetros y se determine las competencias que deben tener los peritos en informática forense, así mismo que entidades pueden otorgar el título de perito informático.

En muchos casos las falencias que se presentan obedecen también a la falta de capacitación de los funcionarios que actúan dentro del proceso penal, tanto investigadores, peritos, jueces, fiscales y defensa, que no cuentan con el conocimiento en el manejo de la evidencia digital, pensando que este tipo de evidencia se trata como cualquier otro elemento material probatorio, si tener en cuenta su especialidad, en cuanto a la volatilidad de la información o respecto de las unidades de almacenamiento externo, porque se debe actuar con el debido cuidado.

Es importante que todos los funcionarios de la Policía Nacional, sean capacitados en cursos de evidencia digital, teniendo en cuenta que, por su misión Constitucional de convivencia ciudadana, en la mayoría de los casos son la primera autoridad que tiene contacto con la escena y elementos materiales probatorios, es decir, actúan como primer responsable en escenarios que involucran evidencia digital.

En el mismo campo de la capacitación, es sumamente necesario que los funcionarios tanto fiscales como jueces, sean formados en temas de evidencia digital frente al proceso penal, para que no se generen consecuencias jurídicas adversas al proceso, en detrimento de los intereses de las partes, por desconocimiento en los procedimientos y protocolos en esta área.

El procedimiento de evidencia digital en sus diferentes fases, que culmina con un informe de investigador de laboratorio emitido por el perito en informática forense, debe siempre contar con formalidades legales que no afecten derechos fundamentales, por cuanto la declaratoria por parte del juez como prueba ilegal o ilícita, genera la exclusión del elemento material probatorio del proceso penal.

Tanto la exclusión, rechazo, inadmisión de la prueba o la nulidad decretada por el juez, cada una dependiendo la causal que la genere, afectan la validez del medio probatorio y las garantías procesales de las partes intervinientes, tanto defensa como fiscalía y a las víctimas.

5.13 Referencias Bibliográficas

Adalid Segurity, legal & forensic corporation. (2016). *Manual Básico de Evidencia Digital para Abogados.* Recuperado el 9 de julio de 2019, de https://www.adalid.com/alumnos-adalid/

Angulo, R. (2016). *Cadena de custodia en criminalística* (Cuarta ed.). Bogotá, Colombia: Ediciones Doctrina y Ley.

Bedoya, L. (2008). *La prueba en el proceso penal colombiano.* Bogotá, Colombia: Fiscalía General de la Nación.

Cano, J. J. (2010). *El peritaje informático y la evidencia digital en Colombia.* Bogotá, Colombia: Uniandes.

Constitución Politica de Colombia. (20 de 07 de 1991). Gaceta Constitucional 116. Bogotá, Colombia: Secretaría Senado .

Corte Constitucional. (8 de agosto de 2001). Sent. C-831. Bogotá, Colombia: M.P. Alvaro Tafur Galvis.

Corte Constitucional. (9 de junio de 2005). Sent. C-591. Bogotá, Colombia: M.P. Clara Inés Vargas Hernandez.

Corte Constitucional. (05 de agosto de 2015). sent. C-496. Bogotá, Colombia: M.P.Jorge Ignacio Pretelt Chaljub .

Corte Suprema de Justicia . (18 de julio de 2017). Casación Penal. *Sent. 49.140*. Bogotá, Colombia: M.P. José Francisco Acuña Vizcaya.

Corte Suprema de Justicia. (21 de febrero de 2007). Casación Penal. *Sent. 25.920*. Bogotá, Colombia: M.P. Javier Zapata Ortiz.

Corte Suprema de Justicia. (19 de febrero de 2009). Casación Penal. *Sent. 30.598*. Bogotá, Colombia: M.P. Maria del Rosario Gonzalez de Lemos.

Corte Suprema de Justicia. (14 de abril de 2010). Casación Penal. *Sent. 30.960*. Bogotá, Colombia: M.P. Alfredo Gomez Quintero.

Corte Suprema de Justicia. (18 de mayo de 2011). Casación Penal. *Sent. 29.877*. Bogotá, Colombia: M.P. Javier zapata Ortiz.

Corte Suprema de Justicia. (17 de marzo de 2014). Casación Penal. *Sent. 41.741*. Bogotá, Colombia: M.P. Eyder Patiño Cabrera.

Corte Suprema de Justicia. (19 de 03 de 2014). Casación Penal. *Sent. 41.357*. Bogotá, Colombia: M.P. Gustavo Enrique Malo Fernandez.

Corte Suprema de Justicia. (28 de octubre de 2015). Casación Penal. *Sent. 45.375*. Bogotá, Colombia: M.P. Jose Luis Barceló Camacho.

Decreto 786. (17 de abril de 1990). Diario oficial 39.300. Bogotá , Colombia: Secretaria Congreso.

Fierro, H. (2012). *La nulidad del proceso penal* . Bogotá : Doctrina y Ley.

Fiscalia General de la Nación. (2018). Manual del sistema de cadena de custodia. *4*. Bogotá, Colombia.

Fiscalía General de la Nación. (2018). Manual Unico de Policia Judicial. Bogotá, Colombia.

Fiscalia General de la Nación. (s.f.). Instructivo Para el hallazgo, identificación, embalaje de la evidencia de tipo digital. Bogotá, Colombia.

Fiscalia General de la Nación. (s.f.). Instructivo para extracción de la huella digital a través del HASH MD5. Bogotá, Colombia.

Forensic Investigation Tool. (s.f.). *geekflare.com*. Recuperado el 18 de julio de 2019, de https://geekflare.com/forensic-investigation-tools/

Grupo de investigación en sistemas operativos e informática forense InFo-Lab. (2016). *el rastro digital del delito* (1 ed.). Mar del Plata, Argentina: Universidad FASTA.

Hilari, S. F. (2006). *Revistas Bolivarianas*. Recuperado el 8 de julio de 2019, de http://www.revistasbolivianas.org.bo/scielo.php?pid=S2078-533X2006000100012&script=sci_arttext&tlng=es

Instituto Nacional de Ciberseguridad. (s.f.). *incibe.es*. Recuperado el 10 de julio de 2019, de https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listadosoluciones/encaser-forensic

Juzgado 46 penal del Circuito. (9 de agosto de 2019). *Sent. 11001600005020163168O*. Bogotá, Colombia.

ley 1273. (5 de enero de 2009). Diario Oficial No. 47.223. Bogotá, Colombia: Secretaría Congreso.

Ley 1928. (24 de julio de 2018). Diario Oficial No. 50.664. Bogotá, Colombia: Secretaría

Congreso. ley 527. (18 de agosto de 1999). Diario Oficial No 43.673. Bogota, Colombia: Secretaría Congreso.

Ley 599. (24 de julio de 2000). Diario Oficial No. 44.097. Bogotá, Colombia: Secretaría Congreso.

Ley 600. (24 de julio de 2000). Diario Oficial No. 44.097. Bogotá, Colombia: Secretaría Congreso.

Ley 906. (01 de septiembre de 2004). Diario Oficial No. 45.658. Bogotá, Colombia:Secretaría Congreso.

López, P. (2008). *Investigación Criminal y Criminalística* (3 ed.). Bogotá: Temis.

López, P., & silva, p. (2003). *Investigación Criminal y Criminalística* (Segunda ed.). Bogotá, Colombia: Temis.

Ministerio de Tecnología de la Información y las Telecomunicaciones. (2016). *Guía Evidencia Digital*. Recuperado el 22 de junio de 2019, de www.mintic.gov.co: https://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

Muriel, M., & Ordoñez, H. (2017). *Exclusión de evidencias* (Primera ed.). (U. Libre, Ed.) Cali, Colombia: Poemita.

Perona, E. (10 de febrero de 2016). *SECURITY A(r) TWORK*. Recuperado el 30 de 06 de 2019, de https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-decustodia-de-la-evidencia-digital/

Pino, S. (16 de mayo de 2017). *Derecho Penal Informático.* Recuperado el 17 de junio de 2019, de https://www.academia.edu/33039698/Derecho_Penal_Inform%C3%A1tico_Segund a_Edici%C3%B3n_2017

Pino, S. A. (diciembre de 2009). Recuperado el 05 de julio de 2019, de http://www.criptored.upm.es/guiateoria/gt_m592e.htm

Policia Nacional de Colombia. (31 de diciembre de 2015). Resolución 5839. Bogotá, Colombia.

Prieto, D., & Peña , C. (2007). Evidencia Digital en Colombia: Una reflexión en la práctica. *EJUS*, 12.

Restrepo, J. (2014). *Criminología* (4 ed.). Bogotá: Temis.

Ríos, J. (2017). Las reglas de la cadena de custodia. *Auditool*., 5.

Rouse, M. (julio de 2017). *techtarget*. Recuperado el 30 de agosto de 2019, de https://searchdatacenter.techtarget.com/es/definicion/Almacenamiento-flash

Rousseau, J. J. (1762). *Biblioteca Digital de ILCE.* Recuperado el 30 de 04 de 2019, de http://bibliotecadigital.ilce.edu.mx/Colecciones/ObrasClasicas/_docs/ContratoSocial.pdf

Sansurooah, K. (03 de 12 de 2009). *edith cowan university.* Recuperado el 29 de agosto de 2019, de https://ro.ecu.edu.au/cgi/viewcontent.cgi?referer=https://scholar.google.es/&httpsre dir=1&article=1069&context=adf

Saray, N. (2016). *Procedimiento Penal Acusatorio* (1 ed.). Bogotá: Leyer.

Tribunal Superior de Bogotá . (20 de noviembre de 2008). Sala Penal. *Sent. 11001220400020070081800*. Bogotá, Colombia: M.P. Alberto Poveda Perdomo .

Usera, J. D. (27 de 10 de 2018). *Hardzone*. Recuperado el 30 de 08 de 2019, de https://hardzone.es/2018/10/27/memoria-flash-nand-nor/

Valdés, C. (2008). *Lugar de la conducta punible* (Primera ed.). Bogotá, Colombia: Fiscalia General de la Nación.

Valencia, M., Ramirez , A., & Vera , G. (2016). Admisibilidad de la Prueba novel en el proceso penal colombiano. *La Prueba Pericial*, 83-95.

Vanegas, J. P. (2015). Evidencia Digital y Cadena de Custodia. *Polux*, 4.

6 Tratamiento de los Delitos Electrónicos en Colombia.

El delito de estafa electrónica y su dinámica criminal

Oscar Vergara Taborda,
Gerardo Elías Cortes Buitrago

Resumen

Los avances de las nuevas tecnologías ha hecho que cada día la conducta humana, personas inescrupulosas y delincuentes utilicen la misma ciencia para alcanzar sus propósitos, así aparecen nuevos comportamientos que configuran en nuevos delitos, por su potencialidad de ocasionar daño y vulnerar bienes jurídicos; ya que estas conductas señaladas como punibles, al ser tipificadas, afectan a personas naturales y jurídicas. Esta circunstancia motiva que el Congreso legisle sobre conductas que impactan la económica social e individual, sector productivo y financiero, como por ejemplo, el ofrecimiento engañoso de productos y servicios, el pánico económico, el lavado de activos y la omisión de control, el daño informático, la extorsión informática, sabotaje informático, espionaje informático, acceso no autorizado a sistema de procesamiento de datos, abuso de confianza informática, hurto informático, falsedad informática, estafa informática, corrupción de menores vía informática, entre otros.

Palabras clave: estafa electrónica, delito informático.

Introducción

El Estado Colombiano ha realizado muchas modificaciones al Código Penal (Ley 599 de 2000), creando leyes que se adecuen a las circunstancias de tiempo, modo y lugar, atendiendo las diversas modalidades en que se pueden cometer conductas punibles a través de los medios electrónicos, por consiguiente referente al tema del delito de la *estafa electrónica*, tipo penal que protege el bien jurídico contra el patrimonio económico, el legislador se vio en la necesidad de introducir una reforma a nuestro código penal sustantivo, creando leyes y decretos, entre ellas la ley 1273 de 2009, cuya finalidad es la protección de la información y datos personales. Reconoce la norma como bien jurídico tutelado, una serie de conductas penales entre ellos: obstaculización ilegitima de sistema informático o red de telecomunicaciones; intercepción de datos informáticos, daño informático; uso de software malicioso; violación de datos personales, y suplantación de sitios web para capturar datos personales. De la misma manera se incluye un delito tradicional como el hurto cuando es cometido por medio informático.

Frecuentemente se conoce a través de los medios de comunicación masiva la ocurrencia de defraudaciones, falsedades, hurtos y otras conductas indebidas, que tienen de particular el hecho de que, para su consumación se utilizó tecnología informática o telemática, configurándose el llamado "delito informático"; También es común enterarse del crecimiento de la actividad de piratería de música, video y software.

Se trata, en suma, de la denominada criminalidad informática, genero por lo cual se puede distinguir dos especies: en la primera se ubican los delitos de que – como las primeras a que nos referimos en el párrafo anterior, se cometen a través de medios informáticos, en el segundo los que se cometen sobre elementos informáticos. Como todos los esquemas, este tiene carácter meramente indicativo, pues obviamente es posible que, por ejemplo, a través de medios informáticos se altere información contenida en registros informatizados.

Esta investigación pretende establecer a partir de otros análisis, cómo Colombia ha evolucionado en el tratamiento de la criminalidad que se ha producido por impacto de las TIC (Tecnología de la Información y la Comunicación). Y que, entonces, el derecho penal también ha experimentado una necesidad de reconocer nuevas conductas delictivas para ajustar sus elementos conceptuales por tradición las nuevas realidades.

La criminología, que se ocupa de estudiar el delito como fenómeno social, así como de determinar sus posibles factores etiológicos y de evaluar la respuesta punitiva del Estado, y con base en ello formular la política anticriminal, presenta interesantes líneas de investigación, para amplificar, a las características subjetivas

del delincuente informático[25], a las motivaciones de su actuar[26], a su posición respecto a las víctimas[27], y a la tipología de los delitos informáticos[22].

La criminalística, conjunto de técnicas de investigación policial del delito, se ve abocada a dar un gran salto para hacer frente a la delincuencia informática. Aquí resultan inofensivas las técnicas que tradicionalmente usadas en la investigación penal, como la grafología, documentoscopia[23], lofoscopia[28], entre otros.

En Colombia, el 5 de enero de 2009, el Congreso de la República promulgó la Ley 1273, la cual modificó el código penal adicionando nuevas sanciones en casos relacionados con los delitos informáticos, buscando proteger la información y preservar los sistemas de tecnologías de información y comunicaciones. Esta ley contempla dos capítulos: 1. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, y, 2. De los atentados informáticos y otras infracciones. (CALDERON GARCIA, 2000)

De acuerdo a lo anterior, el delito informático en Colombia se sanciona mediante la Ley 1273 de 2009, y, en ella se contemplan 10 delitos sancionados que son: 1. Acceso abusivo a un sistema informático (modificado del Código Penal); 2. Obstaculización ilegítima del sistema informático o red de telecomunicación; 3. Interceptación de datos informáticos; 4. Daño informático; 5. Uso de software malicioso; 6. Hurto por medios informáticos y semejantes; 7. Violación de datos personales; 8. Suplantación de sitios web para capturar datos personales, 9. Circunstancias de agravación punitiva, y, 10. Transferencia no consentida de activos.

---

25 Intentado precisar un perfil social y psicológico y unas tipologías: hackers, crackers, etc.

26 Lúdica, lucro, inconformidad laboral política.

27 Considerando, por ejemplo, su pertenencia a la empresa agraviada: outsider, insiders.104 Fraudes informáticos-a través de, digamos, "caballo de Troya"-, falsedad en información digitalizada, obtenciones fraudulentas de datos, sabotaje de equipos o de datos ("bombas lógicas"), espionaje informático, etc. [22] Fraudes Informáticos, a través de, digamos, "caballo de Troya", falseada en información digitalizada, obtención fraudulenta de datos, sabotaje de equipos o de datos ("bombas lógicas"), espionaje informático, etc. [23] Es el estudio que se realiza en forma integral del documento en cuestión, con el objetivo de hallar en él las respuestas apropiadas a los interrogantes planteados de pericia mediante métodos, procedimientos y técnicas adecuadas. Es el examen total y pormenorizado del documento, abarcando tanto las detecciones de adulteraciones y falsificaciones que pueden ser de orden química o física, como el examen comparativo para determinar la identidad escritural.

28 La lafoscopia es el estudio de los dibujos lineales que se presentan en las caras y en los bordes de las manos y los pies de todo ser humano. Estos dibujos o rugosidades también son conocidos como crestas papilares. No existen dos crestas papilares iguales, por lo tanto, cada individuo tiene unos dibujos particulares diferentes a los de cada ser humano.

6.1 Tratamiento Jurídico de los delitos Informáticos en Colombia

Ley 1273 de 2009 (Carvajal Avellaneda, 2015)

LEY 1273 DE 2009 (enero 05) 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	
Tipo penal	Descripción normativa y sanción penal
Artículo 269A: Acceso abusivo a un sistema informático	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Artículo 269B: Obstaculización ilegítima de sistema	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

informático o red de telecomunicación.	(48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor. Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
Artículo 269C: Interceptación de datos informáticos.	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Artículo 269D: Daño Informático.	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y
	seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
Artículo 269F: Violación de datos personales.	El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes

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

Artículo 269H: Circunstancias agravación punitiva:	Las penas imponibles de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. Por servidor público en ejercicio de sus funciones. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. Revelando o dando a conocer el contenido de la información en perjuicio de otro. Obteniendo provecho para sí o para un tercero. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. Utilizando como instrumento a un tercero de buena fe. 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.
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 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	Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca,

	posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. Artículo 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.
Pornografía infantil	Artículo 187. La inducción, promoción, favorecimiento o facilitación de la prostitución de una persona menor de edad o incapaz. Artículo 189. La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. La facilitación de las conductas anteriores (El que facilitare la producción, venta, distribución, exhibición...). La posesión de dicho material para la realización de dichas conductas.

Fuente: Carvajal Avellaneda, Mary Angélica, Rangel Ruíz Nataly.

6.2 El Delito electrónico de estafa en el Derecho Penal colombiano

Definición. Se entender el delito de estafa, de acuerdo a Antón Oneca (1958) como *la conducta engañosa, con ánimo de lucro injusto, propio o ajeno, que determinando un error en una o varias personas, les induce a realizar un acto de disposición, a consecuencia del cual se produce un perjuicio en su patrimonio o en el de un tercero*", para lo cual nuestro código penal plantea que debe darse una serie de requisitos para que se configure el delito de Estafa.

En ese sentido, entonces no hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de la clonación de tarjetas bancarias, compra, venta de bienes y servicios, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos entre otras son conductas cada vez más usuales en todas partes del mundo.

De ahí la importancia de la ley 1273 de 2009 que se adiciona al código penal colombiano Titulo VII Bis denominado: "De la protección de la información y de los datos que se divide en dos capítulos a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".

Como se puede apreciar, la ley 1273 de 2009, es un paso significativo en la lucha contra los delitos informáticos en Colombia por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

Pero más allá de ese importante factor con la promulgación de esta ley se obtiene una herramienta específica para denunciar los hechos delictivos a los que se puede ver afectada una persona o una empresa, por tanto es trascendente que se tenga en cuenta que esta ley nace para proteger bienes jurídicos que anteriormente no se enunciaban por cuanto no estaban tipificados como delitos pues ahora ya se ha legislado sobre este aspecto en particular, para que ese tipo de conductas sean sancionadas penalmente y no queden en la impunidad. Una vez estructurados los elementos de la conducta punible de los delitos electrónicos, nos demarca si efectivamente estamos frente a un delito electrónico en particular el delito de Estafa.

El auge del comercio electrónico evidencia en los tiempos actuales que constituye un instrumento cuyo crecimiento es impresionante, sobre los cuales en necesario ejercer control que resguarde el desarrollo de la actividad comercial efectuada. El interés que surja y se establezcan parámetros controladores en beneficio de quienes forman parte de la actividad, es decir tanto demandantes como comerciantes de bienes y servicios.

En la actualidad operan comercialmente a través de este medio un gran número de fraudes que van en detrimento de quienes manipulan comercialmente, aun cuando el espacio, de la operación virtual, los delitos o fraudes que ocurren en el son reales. Los daños, perjuicios, desilusiones y otras consecuencias que puede generar los hechos que representan los engaños producidos en la internet pueden ser incuantificables y ruinosos para quienes sean defraudados. Lo mismo ocurre con otras conductas que aun cuando no son defraudatorias constituyen una amenaza a la seguridad y confianza con las cuales deben hacerse las comunicaciones y transacciones entre las personas.

Las ventajas que producen el anonimato, la velocidad de las comunicaciones y la ansiedad de los mercados, en un hecho que favorece a quienes operan la red en busca de incautos y vulnerables internautas, la indefensión legal de las víctimas se presenta en abundantes modalidades para cometer el delito económico y otras variedades de conductas ilícitas.

Por otra parte, los bajos índices de judicialización y condena de los responsables, ha estimulado el abuso de la tecnología cibernética por causa de la acción de terroristas, piratas, fanáticos, alucinados, traficantes de drogas y productos prohibidos, lavadores de dinero, el crimen organizado y todo género de personas con diversos intereses ilegítimos. Ello perjudica sensiblemente el sano intercambio de quienes, si quieren hacer cosas constructivas, productivas y de buena fe.

La sofisticación del medio cibernético obliga a pensar seriamente acerca del papel que puede desempeñar el Derecho Penal, a los fines de tutelar los bienes jurídicos que representan las interacciones en la internet y con ello, devolver la confianza y la tranquilidad a quienes desean realizar transacciones productivas y hasta placenteras, sin el riesgo de verse despojados, aterrorizados o afectados en sus derechos e intereses impunemente.

Es así como el elemento neurálgico y central del delito de estafa es el engaño o conducta engañosa, que según la redacción del tipo básico debe ser bastante, es decir, competente – tanto desde un prisma objetivo como subjetivo– para producir error a otra u otras personas. El siguiente eslabón de la cadena típica y lógica del delito de estafa lo constituye el error, situación de discordancia entre la representación de la realidad por parte de quien sufre el engaño y los hechos efectivos del mundo exterior, provocada por el sujeto activo mediante la conducta engañosa.

6.3 Características de los delitos electrónicos

Resulta importante describir las características de los delitos electrónicos, a fin de determinar su estructura y adecuarlos a nuestro ordenamiento penal sustantivo, respetando las garantías procesales, como el debido proceso, consagrado en el artículo 29 de nuestra Carta Política, desprendiéndose de este los principios rectores como el de legalidad, presunción de inocencia, favorabilidad y otros. Para Rovira del Canto, otra serie de características para los delitos informáticos que llevan a su identificación clara para posterior adecuación típica, antijurídica y culpable. Y no solo dentro de la dogmática penal, sino también dentro de los aspectos sociológicos y económicos del delito, así: Efectivamente, la incidencia de la posibilidad de repetición de una actuación ilícita en el ámbito informático favorece su nueva comisión, incluso en múltiples ocasiones, derivando en la práctica a que en un alto porcentaje de los supuestos conocidos y enjuiciados de ilícitos informáticos la conducta de los autores no se ha limitado a una única acción delictual, sino a una reiteración continua de la misma. Ello, desde el punto de vista penal sustantivo, se plasma en lo que Alastuey Dobon (2002) denomina como «efecto continuado» propio de esta delincuencia, y el que por la jurisprudencia se aprecie en un alto porcentaje de ocasiones la figura del delito continuado para la sanción de tales comportamientos.

Como instrumento o medio: En esta categoría se encuentran conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, como, por ejemplo: Falsificación de documentos vía computarizada.

- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (hurtos, homicidios, fraudes o estafas, etc.).
- Lectura, sustracción o copiado de información confidencial. · Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.

- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Accesos a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleprocesos.

Como un fin u objetivo: en esta categoría se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como, por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la maquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje, pago de rescate, etc.).

6.4 La estafa electrónica y su modus operandi

Para Sánchez Bernal, el phishing se establece como una de las conductas fraudulentas con más repercusión en la actualidad. Se trata de una práctica encuadrada en el campo de la estafa, que consiste en la adquisición de información confidencial (de carácter económico, personal, o de cualquier otra índole) de forma ilícita, sin consentimiento de su titular; mediante el uso de ingeniería social[29].

29 En seguridad informática, la "ingeniería social" es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Se trata de obtener datos, acceso o privilegios en los sistemas de

El infractor, conocido como phisher, puede simular ser una persona o empresa de confianza, cometiendo el hecho ilícito mediante una comunicación electrónica aparentemente normal (correo electrónico, mensajería instantánea) o incluso, mediante una llamada telefónica. La persona que lleva a cabo esta actividad delictiva suele camuflarse bajo el nombre de la entidad bancaria habitual u otros servicios contratados por el sujeto engañado con el fin de conseguir códigos, contraseñas, números de tarjetas de crédito u otro tipo de información, especialmente bancaria.

La consideración del Derecho penal como última ratio a la hora de solucionar un problema jurídico, impone la necesidad de tener bien claras las razones por las que se debe justificar la intervención coercitiva del Estado. hoy en día, esta "legalidad del Derecho penal" se ve reforzada por la una nimiedad de la doctrina, que resalta por encima de cualquier otra cosa, la función protectora de bienes jurídicos que posee la norma penal (Conde, 1989). Se trata, por tanto, de encontrar el interés socialmente protegido o valor relevante, cuya infracción va a motivar que se ponga en marcha la maquinaria estatal con su mayor arma: el derecho a castigar (ius puniendi). Así, el bien jurídico protegido va a legitimar la norma penal, siguiendo criterios constitucionalmente sustanciales, como la proporcionalidad, la legalidad o el principio de intervención mínima.

El debate en torno al bien jurídico protegido no es baladí, puesto que su determinación y delimitación (su naturaleza, su extensión y límites, o su necesidad y alcance de protección) van a resultar decisivos en los efectos que van a desplegar las específicas figuras contenidas en la parte especial del Derecho penal; llegando a decidir, por ejemplo, la tipicidad o atipicidad de una determinada conducta o la interposición de penas y otras consecuencias jurídicas bien distintas entre sí. Por ello, la toma de postura en la discusión que nos ocupa puede tener una relevancia ineludible, debido a que puede conllevar la vulneración de derechos y facultades individuales igualmente protegidos, estando amparados en la norma penal. Se circunscribe esta discusión, además, en la función preventiva especial de la pena, como resocializadora del individuo, que hace más intensa la necesidad de encontrar un elemento a proteger que justifique la intervención de la jurisdicción penal. no podemos olvidar la paradoja que se produce con la intervención del Estado, al enfrentarse, por un lado, su función como garante de la seguridad y, por lo tanto, asegurador de la libertad y, por la

información, que permitan realizar un acto perjudicial para un sujeto, o que lo exponga a un riesgo o abuso. Engloba, por tanto, cualquier manipulación para conseguir información privilegiada.

otra, el temor que inspira, como amenazador y limitador de dicha libertad por el uso del ius puniendi (Sánchez Bernal, s.f.)[30].

El derecho penal como instrumento de control social, no podía permanecer indiferente ante los daños que se venían causando por el aumento masivo de la utilización de los modernos sistemas informáticos en medios sociales que tradicionalmente habían gozado de una debida protección. La informática se ha utilizado no solo como importante e imprescindible herramienta de trabajo en la sociedad moderna sino también como medio para la realización de delitos tradicionales y otras formas de la nueva delincuencia que ha venido acosando a la sociedad.

Frente al auge de las manipulaciones fraudulentas para obtener provecho patrimonial en perjuicio de otros, surge la preocupación compartida entre la doctrina y el legislador por lograr la elaboración de un nuevo tipo penal al cual pudieren ser reconducidas tales conductas que se concretó en la creación del delito electrónico de estafa, que habría de constituirse en una norma de control social encaminada a fijar unas precisas pautas de convivencia en el ámbito de las relaciones sociales patrimoniales que se llevan a cabo a través de sistemas informáticos (MUÑOZ., 2005, pág. 183).

En el ordenamiento jurídico penal colombiano, la estafa consiste en la obtención, para el agente o para un tercero, de un beneficio sin causa jurídica, con perjuicio patrimonial ajeno y correlativo, logrado mediante artimañas que inducen en error a la víctima y la determinan a entregar el bien o a realizar una prestación, con aparente voluntad, pero con consentimiento sustancialmente viciado por el engaño. Sus requisitos son: a) el perjuicio patrimonial logrado o intentado, b) el ánimo de lucro, c) el engaño fraudulento.

Este último es el característico de las estafas, y lo que separa este tipo de infracción de las formas violentas, como el hurto. El engaño supone una ilusión, es decir, el ejemplo del error provocado o mantenido por el agente se requiere que sea fraudulenta; es decir resultante de la presentación de hechos erróneos o del disfraz o disimulo de hechos exactos. El más típico elemento de la estafa radica en que el engaño sea el medio de obtener la entrega de la suma o de la cosa que se logra. Es decir, que el propio poseedor es el que, en virtud del engaño, toma la medida que disminuye su patrimonio, o mejor, que es el mismo quien entrega la cantidad de dinero, movido en aquel instante por la ilusión errónea que el agente suscita, pero es claro que no se excluye la hipótesis de que el autor se valga en sus maniobrar de una tercera persona.

---

30 Javier Sánchez Bernal es estudiante de quinto de Derecho en la universidad de Salamanca y Becario de Colaboración en el departamento de Derecho Público General, por el Ministerio de Educación, Política Social y Deporte.

Entrando en el caso concreto en particular, plantea Suarez que "en la estafa informática hay que precisar si se trata de uno de naturaleza solo individual o de naturaleza compleja (individual o colectiva), que tendría no solo la misión de la de tutelar otro bien jurídico de característica supra individual o colectiva, demarcado por el interés social que se tiene en la seguridad del tráfico de activos por medios informáticos.

Con el propósito de tener claridad conceptual sobre el hecho punible denominado Estafa Informática, se debe expresar que no está regulada como un tipo especial en la legislación colombiana, tal como lo manifiesta el tratadista Alberto Suarez Sánchez, al decir que:

> La legislación penal colombiana no regula de manera expresa la denominada estafa informática, pues se echa de menos un tipo especial que recoja la conducta de quien a través de manipulaciones informáticas realice transferencias patrimoniales en perjuicio de un tercero (SUAREZ SÁNCHEZ, 2009, pág. 321) .

En la legislación colombiana no se expresa en forma taxativa los medios que puede utilizar el sujeto activo del hecho punible de estafa, debido a las dificultades de enmarcarlos en una formula descriptiva, que estructure dicho ilícito. En eventos de esta naturaleza se pone de manifiesto el ingenio del delincuente, que puede superar el conocimiento y precisión del legislador, e incluso ir más lejos; y unido a esto, el interés y deseo de incrementar en forma rápida y fácil el patrimonio por parte de la víctima, situación está que aprovecha el victimario para alcanzar sus propósitos. En este orden de ideas para engañar, si la consecuencia final de las mismas se materializa en la ejecución de un acto de disposición patrimonial beneficioso para el sujeto activo y perjudicial para la víctima.

No obstante, para que se tipifique el artificio o engaño, no es suficiente la existencia objetiva de la simulación, en razón a que se requiere que el sujeto activo haya realizado de forma internacional la manipulación destinada a generar un juicio falso.

El engaño comporta de manera implícita en elemento subjetivo, debido a que el medio utilizado de haber sido realizado en forma intencional orientado al resultado o meta del engaño. Al respecto, el profesor Alberto Suarez Sánchez, dice:

> El engaño debe ser directo y eficaz: directo, porque la relación entre el timador y el engaño ha de ser personal e inmediata, sin intermediario alguno, y eficaz, en el sentido de que debe ser de tal entidad que mueva la voluntad del engañado a hacer la disposición patrimonial (2009).

Se debe advertir que un número elevado de manipulaciones informáticas cuando afectan los sistemas automatizados para la toma de decisiones, en los eventos en que no existe detrás hombre alguno para vigilar la salida de datos ni para la realización de un acto de disposición, no puede expresarse de la existencia de un error que necesariamente recaiga en una persona. En estos eventos no hay una persona inducida o mantenida en el error por la acción fraudulenta dirigida a lograr la realización de la disposición patrimonial perjudicial. En este orden las ideas, el profesor mencionado Alberto Suarez Sánchez, manifiestan:

> El error que puede ser personal, (el juicio falso recae sobre una persona o seis cualidades), real (el juicio falso recae sobre la cosa o una cualidad de la misma) o sobre la naturaleza de un acto (cuando se cree realizar un acto jurídico distinto al real), únicamente puede ser humano dado que solo se puede mantener o inducir a un error a una persona ("induciendo o manteniendo a otro en error"), luego no es posible engañar a una maquina o artefacto[31].

Se dijo antes que cuando una persona logra obtener un producto introduciendo una moneda falsa o un objeto que simule ser una moneda en una máquina expendedora de artículos, no se tipifica el delito de estafa, en virtud de no haber engañado a una persona; y en consecuencia, el delito será el de hurto.

El referido a la disposición que se materializa en un aprovechamiento al margen de la ley y el correlativo perjuicio que sufre el sujeto pasivo de hecho punible debe ser ejecutado por una persona, que en este caso es la persona engañada, de tal suerte, que no es posible una disposición con dichas características por l acción de una máquina.

Los anteriores argumentos sirven para que la doctrina dominante no acepte que las manipulaciones informáticas que den lugar a transferencias patrimoniales que van en detrimento del patrimonio ajeno al tipo de ilícito de estafa común; y en consecuencia, ante la ausencia de un tipo que recoja tales conductas, son partidarios de la creación de la respectiva norma por el legislador.

A pesar de lo expresado, existen autores que manifiestan que las defraudaciones por medios informáticos son estafas que pueden ser cobijadas por el tipo básico de la misma, al no referirse tal maquinación a una autentica estafa, en razón a que el mismo legislador, como se establece en el Código Penal español, que en el artículo 248, empieza diciendo: "También se consideran reos de estafa", para recoger en dicho precepto conductas que en realidad no son estafas razón por la que se denomina "tipo de estafa peculiar", "estafa específica", o "tipo específico de estafa",

31 Ibid.

mientras que hay autores que sostienen que no es una modalidad de estafa a pesar de reconocerle una naturaleza defraudadora.

De otra parte, se debe advertir que no se debe asimilar la conducta de la persona que por medio de manipulaciones informáticas obtenga incremento patrimonial en perjuicio de otra, a la de un comportamiento similar, por medio de la inducción o manteniendo en el error a otra persona, sin la existencia de una norma que de manera expresa tenga a aquel como autor de dicho hecho punible, lo que equivale a una violación al principio de la legalidad penal; puesto que, tal interpretación implicaría la aplicación de una analogía inaceptable, improcedente, o que podría entenderse como una interpretación extensiva de una disposición restrictiva, aspecto este que va en contravía del valor superior de la seguridad jurídica, siendo este postulado uno de los fundamentos del Estado de Derecho.

Frente al delito de estafa se debe reiterar que su característica fundamental consiste en que el agente autor de la conducta utiliza como instrumento a la misma víctima; lo que significa que en el fondo hace referencia a una teoría mediata para alcanzar un bien servicio que genera al engañado o a un tercero, situación que no se presenta cuando el agente de la manipulación informática obtiene la transferencia del activo patrimonial perjudicial, en razón a que emplea como instrumento a la misma máquina que acciona.

En el orden de ideas expuestas, se debe recordar que en realidad se refiere a un delito de defraudación patrimonial independiente con sus propios elementos que lo estructuran, pero que en términos estrictos no tipifica una modalidad de estafa genérica, y solo equiparable a la misma en el evento de que exista una norma que de manera expresa así lo consagre, en cuyo precepto el bien jurídico tutelado es el interés patrimonial individual. "Se aleja la posibilidad de atribuirle a esta figura penal la naturaleza del delito informático y de la información (CANTO, 2002)", que la nueva era de la informática reclama para una real protección[32].

Se ha manifestado que actualmente con el uso de tecnologías tan avanzadas en el mundo de los negocios económicos, se establecen relaciones e interacciones de múltiple índole entre personas naturales y jurídicas que posibilitan diversas formas de engañar, lo que obliga al legislador a pensar, y, repensar y revaluar el concepto jurídico que se ha tenido de engañar, pues, no es necesaria a la conducta engañosa, el concepto de una relación física, personal e inmediata, por lo menos entre el victimario y la victima para tipificar un hecho punible de la naturaleza que nos ocupa.

32 Ibid.

Ahora es conveniente expresar que si la ley establece que es autor del delito de estafa "quien induce o mantiene en error a otro", el sujeto de dicha conducta ilícita no puede ser una casa, una máquina, un computador, un banco de datos, etc., sino una persona, a quien se utiliza como instrumento para que haga la disposición patrimonial nociva (SUAREZ SÁNCHEZ, 2009).

En consecuencia, frente a la legislación colombiana no es procedente expresarse que no se requiere la adopción de tipos penales especiales, para sancionar las defraudaciones mencionadas como lesivas del patrimonio económico, con el argumento de que, si bien es cierto que no se engaña a una persona en el momento de hacerse la manipulación informática, también lo es que al final el engañado es una persona.

Lo anterior nos indica que en nuestra legislación se debe crear un tipo autónomo o adicionar al tipo básico o general de la estafa, en razón a que un tipo de la naturaleza indica requiere como uno de sus elementos la "inducción" o el mantenimiento en error a otro, mediante el empleo de artificio o engaño, siendo indispensable instrumentalizar a la persona que ejecuta la acción de disposición patrimonial perjudicial para el mismo o un tercero.

Se ha podido constatar en este estudio que en el evento de defraudaciones por medio de manipulaciones informáticas no se emplea a una persona como instrumento, sino que, por el contrario, se acciona a una maquina; pero, además, que a la persona inducida al error o engaño efectué la disposición, cuya defraudación patrimonial se obtiene por medio de la manipulación del computador. Esto nos indica que si no existe el tipo penal que recoja la conducta descrita, la misma queda impune.

En este orden de ideas, es conveniente manifestar que si en nuestro país se pretendiera sancionar el comportamiento expresado, que se considera como una necesidad, en razón a que amerita una pena, y ante dicha situación se deben adoptar soluciones viables para enfrentar el flagelo de las defraudaciones patrimoniales por medio de manipulaciones informáticas, en donde se obtiene provecho patrimonial en forma ilícita, sin que sea necesario mantener en el error o engaño a las personas víctimas de dicho hecho punible y desde luego, obteniendo su disposición patrimonial, cuyos dos elementos son indispensable para poder tipificarse el delito de estafa, tal como está consagrado en la legislación colombiana.

Es imprescindible fijar si el delito de estafa electrónica debe ser configurado como uno de característica evidentemente patrimonial o como un verdadero delito económico, lo que a su turno es determinante para delimitar el injusto típico de este delito, por su incidencia en la interpretación de algunos de los elementos que lo configuran.

Por su parte Tiedemann en cita de Galán Muñoz, (2005) , al analizar el delito de esta estafa informática, y según el mismo Sánchez se apartaba de la postura que le asignaba una naturaleza a la estafa común, pues afirmaba que en dicho delito, además del patrimonio se protegían otros bienes de carácter colectivo o supra individual dado que la ejecución de tal hecho punible no solo produciría efectos sobre el patrimonio individual sino también sobre los fundamentos del propio sistema informático.

Esta interpretación dual (individual y colectiva) del bien jurídico conduciría admitir que la comisión de un delito de estafa informática conduciría además de la pérdida patrimonial para un individuo, la lesión de la seguridad y la confianza que os ciudadanos deben tener en esta clase de tráfico comercial.

Según este planteamiento para que se configure la estafa electrónica se tendría que presentar la puesta en peligro del bien jurídico individual, o sea el patrimonio, y se exigiría también que el hecho causase al menos la puesta en peligro de un bien jurídico de carácter colectivo, que en este caso sería el señalado por la seguridad del tráfico económico representado por los medios informáticos.

Se incardina así, tal delito en los denominados delitos económicos, porque a través de la protección que se brinda a un bien jurídico individual (el patrimonio) se busca tutelar también a los agentes comerciales y al estado, y de esta manera al propio orden económico a su integridad.

En tales condiciones, se admitía que el delito de estafa informática tutela un bien jurídico que a pesar de no pertenecer a los intereses jurídicos del Estado, tampoco podía hacerse coincidir con los intereses económicos del individuo, lo cual abre el camino para la discusión acerca de si se trata de los denominados bienes jurídicos intermedios, como lo entendía Tiedemann, quien señala como ejemplo de tales intereses el tutelado en el delito de estafa informática, que estaría constituido por el correcto procesamiento de los datos electrónicos, que es tenido como un instrumento imprescindible de la vida económica moderna (Tiedemañ, 1993).

Sin duda, la aceptación de este bien jurídico intermedio (Luzon Peña, 2017)[33] tendría una gran incidencia en la delimitación e interpretación del injusto típico del delito de estafa informática. En efecto, si los delitos protectores de un bien jurídico intermedio se caracteriza frente a los simples delitos-pluriofensivos de peligro por el hecho de que para su consumación se exige lesión de uno de los dos valores que lo conformen, el colectivo o el individual (De la Mata Barranco & De la Cuesta Arismendi, 2010), para poder clasificar al delito de estafa informática como protector de un bien jurídico intermedio, hay que aceptar que la conducta típica se dirige

33 p. 314) afirma que junto a los tipos sólo de peligro, a veces se configuran delitos de lesión y peligro, que implican lesión de un bien jurídico en peligro para otro, como el incendio, por ejemplo.

a lesionar de manera inmediata un bien jurídico individual, al mismo tiempo que provoca dicha lesión la mediata puesta en peligro de otro valor de índole diversa a la del primero (Muñoz, 2005). El delito de estafa en la ley colombiana se consuma cuando se obtiene provecho patrimonial ilícito para sí o para otro. La Corte Suprema de Justicia ha señalado que:

> (…) la estafa se consuma en el propio instante en que debido a la inducción en error, el sujeto activo incorpora a su haber patrimonial bienes o derechos que hasta ese momento pertenecían a la víctima o a un tercero, y de los cuales el estado se desprende, no por expresión de su libre voluntad, sino de su distorsionada comprensión de la realidad, situación a la que se llega a través del ardid, el engaño, las palabras o los hechos fingidos" (Sentencia, 1999).

Igualmente, que la estafa, básicamente, consiste en obtener un provecho ilícito para sí o para un tercero, lo que implica un incremento del patrimonio del actor y el correlativo detrimento del perteneciente a la víctima. Por tanto, la consumación de la conducta se pone de manifiesto a partir de ese efecto, porque coincide con la lesión al bien jurídicamente protegido; de ahí que para establecer el momento consumativo de la conducta deba tomarse como punto de referencia aquel en el cual se produce esa transferencia que implica el crecimiento de un patrimonio en perjuicio de otro (Sentencia, 2002).

El perjuicio ajeno debe darse de modo correlativo con la ilícita utilidad. No todo provecho obtenido con artificio trae dispuesto el perjuicio para otro, como lo señala el Dr. Suarez en su ejemplo si A, sin ser arquitecto, se hace pasar como tal y logra que otro contrate sus servicios para la ejecución de una obra, que es desarrollada en su totalidad con buena calidad por el impostor, no se da la estafa a pesar de que hubo el ardí y el provecho, ya que no se causó perjuicio, dado que la obra habría sido construida en las mismas condiciones si el engañado hubiera contratado con un verdadero arquitecto.

6.5 Elementos del tipo penal de la estafa

De la descripción típica del delito de estafa se ha de concluir que son los elementos de esta:

- La conducta del sujeto activo del delito debe estar orientada a la obtención de un provecho ilícito de carácter patrimonial que consecuentemente debe traducirse en un daño de la misma naturaleza al sujeto pasivo el delito, que se obtiene como consecuencia del error con que se induce a la víctima.

- La utilización por parte del sujeto activo del delito de medios o artificios engañosos, dirigidos a conducir o mantener en error a la víctima.
- La real producción del error en el sujeto pasivo de la infracción, o el mantenimiento en el mismo como consecuencia de la falsa representación de la realidad en la victima como producto de los artificios o engaños desplegados por el agente delictivo.
- Un acto de disposición patrimonial realizado por el sujeto activo y con una relación casual, con las maniobras engañosas realizadas por el agente del delito.
- La obtención del provecho ilícito buscado por el agente con el consecuente perjuicio patrimonial de la víctima.

El delito de estafa es de naturaleza muy compleja, tanto es así que muchas veces se hace imposible saber si una conducta pertenece o no al campo de la estafa, confundiéndose con muchos otros actos ilícitos; por ellos corresponde al juzgador en su buen criterio, examinar los elementos que se presenten en un caso concreto y definir si en verdad esa conducta se adecua dentro del concepto de estafa, por existir diversas formas empleadas por los estafadores para quebrantar el patrimonio de otro.

Inducir es persuadir, es obligar a alguien con razones de creer algo, a creer que se le dice la verdad, de donde nace para el caso en estudio, lo que se conoce como la mentira eficaz, es decir que el agente debe convencer a la víctima; la mentira no puede ser fogosa, ridícula o entusiasta, no puede ser la narración fantástica de una historieta; es necesario hacer creer al sujeto pasivo que existe sensatez en lo que se está exponiendo, diciendo o afirmando.

Error es tener un concepto equivocado sobre algo, es un juicio falso y mediante el error una persona puede ser engañada fácilmente, como cuando el estafador dice vender una cadena de oro, pero esta es de cobre; el error es un vicio de conciencia, lo que hace apreciar las cosas de una manera diferente.

Engaño equivale a mentira, es faltar a la verdad e inducir a otro a creer en algo y tener por cierto lo que no es, con el engaño se produce en la victima una ilusión que hace ver las cosas como ciertas, es la equivocación cierta de lo que no es cierto; engañar es engatusar a la victiman para quebrantar su patrimonio, es distraer la verdad, es la equivocación fatal del sujeto pasivo sobre la verdad; en una palabra es disfrazar la verdad. El engaño de ser idóneo para inducir en error, sin importar cual fuere el medio empleado, habrá que estar subjetivamente dirigido al fin de engañar.

El provecho ilícito es un beneficio que se consigue para sí o para otro, es una utilidad. En el delito de estafa se consuma cuando el estafador obtiene un provecho ilícito y de ahí la diferencia con el hurto, el cual se perfecciona con el apoderamiento; en la estafa el fin perseguido es precisamente ese provecho ilícito ventaja sin soporte jurídico el cual puede recaer sobre bienes muebles e inmuebles, sobre cosas corporales o incorporales, sobre documentos, puede consistir en dar o no, hacer o no una cosa; debe haber una lesión de orden económico.

Provecho ilícito es el fin perseguido por el agente, luego su obtención es elemento material de la estafa; provecho ilícito es todo beneficio, toda utilidad, no importa cuál sea su naturaleza. Puede no ser directamente económico para el culpable, pero para la victima sí, porque como ya lo anotábamos, el provecho puede resultar de prestaciones de dar, hacer o no una cosa, con relación a bienes de cualquier clase, que resulte de ello un beneficio para el delincuente (directo) y para terceros (indirectos).

El delito electrónico de estafa, es una modalidad de la conducta punible de ESTAFA, pues este tipo penal no se encuentra tipificado directamente en nuestro Código Penal Colombiano, en razón a que en primer lugar los investigadores y funcionarios judiciales, deben investigar y juzgar este tipo de conductas enmarcándose en lo preceptuado en los artículos 246 y 247 ídem, teniendo en cuenta los elementos de la conducta y finalmente si se prueba que la maniobra engañosa se realizó por medios electrónicos, al indiciado solo se le imputara la circunstancia de mayor punibilidad en el artículo 58 del código penal, numeral 17.

Pues el legislador no describió la conducta directamente, como sucedió con el hurto por medios informáticos, sino que esta facultad se la dejo al Ente Investigador para que al momento de formular la imputación tuviera en cuenta la circunstancia de mayor punibilidad.

Atendiendo la complejidad en este tipo de delitos se tiene que conforme a la realidad que se presenta en los Despachos Fiscales, a estas conductas no se les está dando la importancia que se debe dar a cada investigación donde una persona resulte como víctima de un delito de estafa electrónica pues la ley 1273 de 2009 se creó para aumentar las penas, pero estos delitos están quedando en la impunidad, precisamente por ausencia de investigación, lo que significa que la justicia no está a la par con el cibercrimen.

El legislador ha anticipado excesivamente la tutela penal de conductas que se ponen en una fase preparatoria, respecto a la efectiva puesta en peligro de bienes jurídicos, con los que se violan los principios de proporcionalidad y de lesividad. La verdadera finalidad de estas incriminaciones, más que proteger bienes jurídicos, parece ser la d facilitar las actividades de investigación por parte de la policía.

Sugerimos que sería oportuno que el legislador diseñe estos delitos en línea con las recomendaciones internacionales, en donde se requiera que los programas maliciosos sean objetivamente diseñados o adaptados con el propósito de cometer un delito y que haya intención por parte del autor. Esto evitaría una indeseable sobre criminalización, permitiendo, al mismo tiempo el empleo de estas herramientas software para actividades de investigación y para fines de seguridad informática.

Por las razones antes expuestas las víctimas de delitos informáticos no denuncian los hechos porque no saben que han sido víctimas, no conocen la existencia de soluciones legales o creen que es inútil poner una denuncia.

Las empresas y los bancos prefieren resolver internamente los incidentes informáticos de los que son víctimas (phishing, espionaje informático, estafas, etc.), en lugar de denunciarlos por miedo a dañar su imagen y perder la confianza de los clientes.

También hay que agregar que a veces las autoridades de la policía no tienen los instrumentos legales y los conocimientos técnicos necesarios para averiguar y perseguir de manera eficaz a los criminales informáticos. En este sentido es oportuno que se siga el camino de la armonización no solamente del derecho penal sustantivo, sino también del derecho procesal penal vigente, para facilitar la cooperación entre las autoridades competentes nacionales y garantizar la persecución de estos delincuentes.

Finalmente se tiene para decir, que el internet es muy difícil de vigilar por parte de las autoridades de la policía y puede proporcionar un gran índice de anonimato a los criminales informáticos, lo que dificulta su persecución penal y los autores de estas conductas se aprovechan de esta debilidad que tiene el poder punitivo del estado.

6.6 Conclusiones

La evolución de la tecnología ha permitido que el ser humano acceda a medios de comunicación, antes inimaginables. Sin embargo, la internet sea convertido en centro de operaciones para muchas conductas desviadas criminales, quienes aprovechan la "fragilidad" de los sistemas de seguridad de la mayoría de los cibernautas, consiguiendo apoderarse de información personal y, en la mayoría de los casos, apoderarse de recursos patrimoniales que perjudican a sus verdaderos propietarios.

El convenio de Budapest se constituye en uno de los principales pilares para la construcción de las legislaciones encausadas a prevención y penalización de la

ciber delincuencia, la Unión Europea, es un claro ejemplo de que la cooperación internacional, podría ser la solución al delito informático. Delito que como se revisó desde varias legislaciones, es difícil de regular específicamente, dado que los avances tecnológicos, aunados a los conocimientos de los delincuentes, favorecen la transformación del hecho punible, para que la legislación penal quede obsoleta con la aparición de nuevos delitos informáticos. Los países latinoamericanos han adoptado en sus ordenamientos jurídicos, los ajustes o adiciones necesarias para el delito informático. Es claro que el problema radica en la falta de una legislación global, que permite la integración de los organismos de investigación, autoridades y legisladores competentes, para que la ley penal evolucione al tiempo que los ciber delincuentes.

Por otro lado, y frente al análisis del Derecho Comparado en el análisis doctrinal y jurisprudencial se observa que el Organismo Internacional más adecuado sobre el cual debe recaer la función punitiva frente a los delitos informáticos es la Corte Penal Internacional, debido a sus características y sistema organizacional que permiten a través de la forma de adhesión voluntaria de los Estados, que sea esta quien asuma la investigación, juzgamiento y sanción de estas conductas.

Con la promulgación de la ley 1273 de 2009, el Código Penal Colombiano, adiciono un artículo literal, con la que se convirtió en el primer país en elevar a bien jurídico tutelado la información y el dato, aquí radica la diferencia entre delito electrónico y delito informático. Los delitos electrónicos son los que atentan contra el patrimonio económico. En los que el sujeto activo aprovecha sus habilidades, destrezas o conocimientos acerca de los sistemas informáticos para realizar actos delincuenciales valiéndose de las computadoras como método o medio en la comisión del ilícito. El sujeto pasivo, al utilizar sistemas automatizados de información por lo general, conectados con otros puede ser víctima del delito de estafa, el ordenamiento colombiano exige la realización de la transferencia "no consentida" de activos en perjuicio de terceros como resultado producido por la manipulación informática. Se concluye que, para efectos del delito de estafa informática, debe existir una apropiación de activos que tengan representación mediante anotaciones o registros contables informáticos cuya modificación, supresión o alteración cause la traslación de un valor económico con la correspondiente perdida por el tutelar de la posesión de los mismos, sin que sea necesaria otra operación o la intervención humana para la producción del daño patrimonial.

Igualmente se concluye que la ley 1273 de 2009 no tipifica directamente el delito de estafa informática, que es uno de los ilícitos que más se presentan actualmente, donde personas inescrupulosas utilizan los medios electrónicos para engañar consiguiendo finalmente vulnerar el bien jurídico del patrimonio económico.

En este orden de ideas, corresponde a la Fiscalía en primer lugar adecuar la conducta típica en el delito de estafa descrito en el artículo 246 del C. Penal e imputarle circunstancias de mayor punibilidad señaladas en el artículo 58 del Código Penal numeral 17 adicionado por la ley 1273 de 2009, art 2°, que señala lo siguiente: "Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos telemáticos".

Para la fiscalía no es fácil lograr la individualización e identificación de los presuntos autores del punible de Estafa por medios electrónicos, por cuanto utilizan nombres e identificaciones falsas, lo mismo sucede cuando son empresas que ofrecen servicios y productos; quedando estos delitos impunes porque no se establece los posibles autores o participes, ya que las personas que se dedican a este tipo de actividades ilícitas son expertas para incurrir en defraudaciones electrónicas.

Es importante agregar que antes de la vigencia de la ley 1273 de 2009, no se imputaba la circunstancia de mayor punibilidad consagrada en el artículo 58 del código penal, numeral 17, modificada por el artículo 2 de esta ley, por tanto se adelantaba solo como estafas, de análoga manera sucedía con el delito de hurto por medios electrónicos.

Con las anteriores consideraciones, se observa que el legislador ha tipificado este tipo de conductas penales tardíamente, toda vez que los medios informáticos hace mucho tiempo estaban funcionando mundialmente, por ese motivo para que no queden impunes este tipo de conductas, el estado colombiano debe firmar un tratado con todos los países del mundo para poder cumplir con las investigaciones cabalmente, en razón a que el delito de estafa se puede presentar desde cualquier parte del mundo como por ejemplo, una persona que se encuentre en la china puede estafar a alguien que esté en Colombia y viceversa, lo que se busca en particular es que finalmente que estas conductas penales no queden impunes, por consiguiente es significativo que se firma un tratado para combatir este flagelo, así mismo instruir el ente investigador y de policía, para que las denuncias tengan resultados positivos, es por ello que las personas que se dedican a estas actividades ilícitas continúan estafando porque saben que nunca van a ser descubiertos.

En síntesis, el delito de estafa informática por medios electrónicos, requiere de interés en la investigación para que este tipo de conductas no queden en la impunidad pues son muchas las víctimas de este flagelo, pero prefieren simplemente no denunciar los hechos, ya que la justicia penal no está dándoles el trámite que corresponde a la investigaciones, para que lleguen a juicio, si no que terminan simplemente en la fiscalía en una orden de archivo.

Frente a la atipicidad de la estafa informática en la ley penal de Colombia, no obstante lo anteriormente consignado en este estudio, se debe manifestar que la persona que mediante la manipulación informática logra consignar a su cuenta

dinero ajeno y luego, mediante procedimiento informático obtiene una transferencia a la cuenta de otra persona, con el propósito de cancelar una transferencia a la cuenta de otra persona, con el propósito de cancelar una obligación, incurre en una conducta que de cara a la legislación colombiana es atípica; puesto que dicha conducta no se enmarca en el ilícito del hurto, de estafa o de otro delito patrimonial y en consecuencia, una conducta de la naturaleza señalada queda impune.

6.7 Referencias bibliográficas

Acuario del Pino, Santiago. (2011). Delito informático: Generalidades.p.20.Disponible en http://www.oas.org /juridicos /spanish /cyb_ecu_delitos_inform.f. Archivista blessmes/Jus another Word/Press.com.site/on March 14, in documents de Word.

Aldama Baquedano, Concepción. (1993). Los medios informáticos. Poder Judicial (30), 9-26.

Álvarez Marañón, Gonzalo & Pérez García, Pedro Pablo. (2004). Seguridad informática para la empresa y particulares. Madrid: McGraw-Hill.

Balmaceda Hoyos, Gustavo. (2009). El delito de estafa informática. Bogotá D.C., Colombia: Editorial Leyer, junio de 2009, p.390.

Bajo Fernández Miguel. (2004). Los delitos de estafa en el Código Penal. Madrid: Editorial Centro Ramón Areces.

Balanta Heidy. (2009). Aproximación legal a los delitos informáticos. Una visión de derecho comparado. Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal. Santiago de Cali.

Bauza Relly, Marcelo. De la Informática Jurídica y el Derecho Informático, al Derecho Informático, Telemático y del Ciberespacio. Disponible en REDI,No.031,febrero de 2001,www.alfa-redi.com.Buenos Aires .Editorial Paraninfo,1991.

Bequai, August. Computer Crime.p.33 y ss., y del mismo, White-Collar Crime: a 20thCentury Crisis.p.105.Citado por HERNÁNDEZ DÍAZ, Leyre. El delito informático. En: Eguzkilore No.23 .San Sebastián, Dic.2009.

Bramont Arias Torres, Luis Alberto. Delitos informáticos. En: Revista Peruana de Derecho de la Empresa. Derecho informático y teleinformática jurídica.No.51.

Bueno Arus, F. (1994). *El Delito Informático*. En: Actualidad Informática Aranzadi. A.I.A. Núm. 11 de abril, Ed. Aranzadi, Elcano (Navarra.)

Bustos Ramírez, Juan. Manual de derecho Penal. Bogotá: Temis, 1996.

Calderon Garcia. (2000). *Los delitos inform@ticos.* Lima Peru: Editora RAO SRL.

Camacho, Luis. El delito Informático. Madrid: Gráficas Cóndor S.A., 1987.

Canto R. D. (2002). *Delincuencia informatica.*

Castillo, J. L. Blanco Parra, B., y Pérez Flórez, R (2010). *La protección de la información y los datos como delito informático en Colombia: sanciones penales*. Universidad Libre – Seccional Cúcuta.

Castro Ospina, S. J. (2002). *La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano*. Universidad Externado de Colombia.

Carvajal Avellaneda, M. A. (2015). *Análisis Comparativo Del Tratamiento Jurídico Dado A Los Delitos Informáticos En El Derecho Penal Colombiano Y Español.* Cucuta: Universidad Libre.

Conde, F. M. (1989). *Teoría general del delito,.* Valencia: Tirant lo blanch.

Choclan Montalvo, José Antonio. Estafa por computación y criminalidad económica vinculada a la informática. Actualidad Penal (47).1997.

Cohen, Daniel. Sistemas de Información. México: Editorial McGraw Hill, 1995.

Código Penal. Colombiano con ANOTACIONES Y LEYES REFORMATORIAS. Editor: Francisco Miguel Martínez Martín. Editorial Imprenta del Departamento.2007.

Campoli, G.A. (2002) "Hacia una correcta Hermenéutica Penal - Delitos Informáticos vs. Delitos Electrónicos", No. 048 - Julio del 2002, AR: Revista de Derecho Informático,

ISSN 1681-5726, Edita: Alfa-Redi. http://www.alfa-redi.org/rdiarticulo.shtml?x=1480, Página consultada abril de 2015.

Colombia. Congreso de la República. Gaceta 645 de Diciembre 10 de 2007.Disponible en: http://www.secretariasenado.gov.co.marzo de 2010.

Colombia. *Constitución Política de 1991.*

Colombia. *Ley 599 de 2000*: Código Penal Colombiano.

Colombia. *Ley 1273 del 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.

Colombia. *Ley 1266 de 2008.* Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Cuervo A., J. (1999). *"Delitos Informáticos: Protección Penal de la Intimidad"*, Revista Electrónica de Derecho Informático, No. 6, enero, 1999. Disponible: http://www.derecho.org.

Corcoy Bidasolo, Mirentxu. Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y el ámbito espacio temporal de comisión de los hechos. En: Eguzkilore cuaderno del Instituto Vasco de Criminología, No.21, 2007.

Cruz de Pablo, José Antonio. (2006). Derecho penal y nuevas tecnologías. Aspectos sustantivos. Madrid: Difusión.

Davarra Rodríguez, Miguel Angel. (2002). Manual de derecho Informático 4ª Edición. Madrid: Aranzadi S.A.480 p.

De la Mata Barranco, N. J., & De la Cuesta Arismendi, J. L. (2010). *Derecho Penal Informático.* Obtenido de Dialnet: https://dialnet.unirioja.es/servlet/libro?codigo=562957

De Miguel Asencio, Pedro Alberto. (2001). Derecho privado de Internet.2ª Edición. Madrid: Editorial Civitas.

Díaz del Campo, S. Propuesta de términos para la indización en Ciencias de la Información.

Descriptores en Ciencias de la Información (DeCI). Disponible en: http://cis.sid.cu/E/tesauro.pd

Dobon, A. (2002). «Apuntes sobre la perspectiva...», cit., pág. 484. Citado en: ROVIRA del CANTO,- Delincuencia Informática y fraudes informáticos. Granada - España: Editorial Comares.P. 78. .

Faraldo Cabana, Patricia. (2010). La respuesta española al cibercriminal. Algunas reflexiones. XXXII Jornadas internacionales de derecho penal. Derecho penal y económico y de la empresa. Bogotá: Universidad Externado.

Fernández García, Emilio Manuel. Los fraudes con tarjetas de pago y otros supuestos de delincuencia informática patrimonial. Incidencia. Drogas de abuso: aspectos científicos y jurídicos. Experiencias de la LORPM. Madrid: Ministerio de Justicia, 2004.

Fernández Teruelo, Javier Gustavo. Respuesta penal frente a fraudes cometidos en Internet:

estafa, estafa informática y los nudos de la red. En: Revista de Derecho Penal y CRIMINOLOGÍA No.19.Enero, 2007.

Galán Muñoz, Alfonso. El fraude y la estafa mediante sistemas informáticos (análisis del artículo 248 C.P., tirantloblanch).Valencia, 2005.

Gómez Pava Jeau, Carlos Arturo. (2006). EL PRINCIPIO DE LA Antijuricidad Material. Quinta edición. Colección Justicia Material. Bogotá: Giro Editores Ltda.

González Rus, Juan José. (1986). Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos. En: Revista de Derechos de la Universidad Complutense.

Gutiérrez Francés, María Luz. (1991). Fraude informático y estafa. Madrid: Ministerio de Justicia.

LA ELECTROSFERA. Ventajas y desventajas de la ley especial de delitos informáticos. Disponible en: http.//geopelia.wordpress.com/2008/04/13/ventajas y-desventajas-dela-ley-especial-de-delitos-informáticos.

Luzon Peña, D. F. (julio de 2017). *Fundación internacional de ciencias penales.* Obtenido de http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20171008_05.pdf: http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20171008_05.pdf.

Mata Martín, Ricardo. Estafa convencional, estafa informática. Pamplona: Thomson Aranzadi, 2007.

MagnoliaMarckovicth,ClaudioPaul.DelincuenciainformáticaenChile,proyecto de ley. Santiago de Chile: alfa-redi, derecho y nuevas tecnologías.p.4.Disponible en:http://www.alfa-red.org/node/9228.

Méndez Pérez, Néstor. (2006). El derecho en la sociedad de la información. En: Revista de la información básica.Vol.1 No.2, p.18. Bogotá.

Morales García, Oscar. (2001). Delincuencia informáticos y delitos comunes cometidos a través de la informática. Valencia: Tirant Lo Blanch.

Muñoz, G. (2005). *Fraude.*

Ojeda-Pérez, Jorge Eliécer; Rincón-Rodríguez, Fernando; Arias-Flórez, Miguel Eugenio & Daza-Martínez, Libardo Alberto (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11 (28), 41-66.

Oneca, A. (1958). *Nueva Enciclopedia Jurídica .* Madrid: Editorial Francisco Seix, Estafa, t. IX.

Pais, D. E. (6 de Octubre de 2012). *Diario El Pais.* Obtenido de Diario El Pais: http//www. elpais.com.co/elpaios/judicial/noticias/reyes-estafa.

Parker, Donn B. Crime by computrer.p.12 ss y 237 ss. Citado por Hernández Díaz, Leyre. El delito informático .En Eguzkilore, No 23.Sa Bestaían, Dic. 2009.

Paterlini, Nora; Vega, Carolina; Guerreiro, Gabriela y Velásquez, Mercedes. Delitos Informáticos. Antecedentes internacionales para una legislación nacional. Buenos Aires. Asociación Argentina de derecho de Alta tecnología,19 de Agosto de 2012.p.2. Disponible en: http://www.aadat.org/delitos_informaticos20.htm.

Pérez Manzano, Mercedes. (1998). Compendio de Derecho Penal. Parte Especial II. Madrid: Ceura.

Preda del Puerto, Ricardo.(2012). Ley contra los delitos informáticos .Breve reseña. Asunción: ABC.com, 22 de agosto de 2012.p23.Disponible en http://www.abc. com.py/articulos/ley-contra-los-delitos-informaticos-breve-resena358709.html.

República de Perú. Sala de la Comisión de Justicia y derechos Humanos del Congreso de la República, pre dictamen de la comisión de justicia y derechos humanos recaído en los Proyectos de Ley 034/2011-CR Y 307/2011 –CR. Disponible en: http://iriartelaw.com/site/ default/files/ PreDictamen-Comisión-Justicia_Delitos_Informaticos.pdf.

Rincón Ríos S, J. (2011). Justicia Internacional, una alternativa válida para el Delito Electrónico. Ponencia presentada en el Foro Delito Informático En Colombia, (Evaluación necesaria a dos años de inicio). Seguridad Informática Vs Delito Febrero 23 al 25 de 2011.

Ponencia presentada en la Universidad Santiago de Cali. Cali, Colombia.

Rincón Ríos, J. (2013). Fraude en la Contratación Electrónica Internacional. Biblioteca de Tesis Doctorales No. 13. Bogotá D.C.: Grupo Editorial Ibáñez.

_____. (2015) El delito en la cibersociedad y la justicia penal internacional.

tesis doctoral. universidad complutense de Madrid. facultad de derecho. EL Madrid.

Reyna Alfaro, Luis Miguel. Fundamentos para la protección penal de la información (almacenada, tratada y transmitida mediante los sistemas de procesamiento de datos) como valor económico de empresa. En: Revista de Derecho Informático. Alfa-Redi, 1999.

Romeo Casabona, Carlos María. Poder informático y seguridad jurídica. Madrid: Fundesco, 1988.

_____De los delitos informáticos al cibercrimen. En: Universitas Vital. Homenaje a Ruperto Núñez Barbero. Salamanca: Ediciones Universidad de Salamanca, 2007.

Rovira del Canto, E. (2002). Delincuencia informática y fraudes informáticos. Granada: Colmares.

Serrano Gómez, Alfonso. (2006). Derecho Penal, Parte especial. 11a ed. Madrid: Dykinson.

Suarez Sánchez, Alberto. (2009). La estafa informática. 1a edición. Bogotá: Grupo Editorial Ibáñez.

Sánchez Bernal, J. (s.f.). Madrid: Ministerio de Educacion, Politica social y deporte.

Sentencia, radicado 16.565 (Corte Suprema de Justicia. 16 de diciembre de 1999).

Sentencia, 20182 (Corte Suprema de Justicia 19 de noviembre de 2002).

Suarez Sánchez, A. (2009). *Estafa Informática.* Bogota Colombia: Ibañez.

Tiedemañ, K. (1993). *Lecciones de Derecho económico.* Madrid: Promociones y publicaciones.

Téllez Valdez, Julio. (1995). Derechos Informático.2ª ed. México: McGraw Hill.

Teruelo, J. G. (2007). *Cibercrimen. Los delitos cometidos a través de internet*, Ed. Constitutio Criminalis Carolina, 1ª edición, Oviedo.

Unión Europea. *Convención sobre Delitos Informáticos o Convenio sobre Ciberdelincuencia.* 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.

Valdecacres Ortiz, María Isabel (1996). Comentarios al Código Penal de 1995.Volumen II (ART.234 A disposiciones finales) Valencia: Tirant Lo Blanch.

Valla Muñiz, José Manuel; Quintero Olivares, Gonzalo. Comentarios a la parte esencial del Derecho Penal.7ª ed. Cizur Menor: Thomson-Aranzadi, 2008.

Velásquez Elizarras, Juan Carlos. El estudio de caso en las relaciones jurídicas internacionales. Modalidades de aplicación del derecho internacional. México: Universidad Nacional Autónoma de México, 2007, p. 286

Viega, María José; Carnikian, Federico. (2010). Respuesta a los delitos informáticos: su visión desde la privacidad y la seguridad de la información, Ponencia presentada al

Seminario "Nuevas Tecnologías: Privacidad y Seguridad". Cartagena de Indias, 21 al 23 de Julio.

Vives Antón, Tomás Salvador; González Chusca, José Luis. Comentarios al Código Penal de 1991.Vol II. Valencia. Tirant Lo Blanch, 1996.

Hoy la tecnología interpela al derecho penal y desafía a la criminalística; "obtener pruebas" y "hacer justicia" requiere indefectiblemente del dominio de la tecnología, en particular de la informática aplicada. Esto hace que la informática se constituya en la herramienta fundamental de las Ciencias Forenses en la actualidad.

En este contexto, poner el foco en estas herramientas tecnológicas y su aplicación a la investigación y práctica en ciencias forenses es clave en el ámbito académico. La cooperación para el logro de estos objetivos es fundamental para las instituciones y genera las posibilidades ciertas de desarrollo institucional y de los estudiantes y egresados. Esta publicación conjunta viene a poner en evidencia el trabajo de dos Universidades comprometidas en este campo y que comparten generosamente sus desarrollos con la comunidad académico-científica internacional.

Este compendio de trabajos científicos es la primera actividad de cooperación académica entre la Universidad FASTA de Mar del Plata, Argentina, y las Maestrías en Derecho Penal y Criminalística y Ciencias Forenses de la Universidad Libre Seccional Cali. Actividad que también hace parte de los fines planteados por la Red Iberoamericana de Universidades e Institutos con Investigación en Derecho e Informática - Red CIIDDI.Esperamos que continúen estos esfuerzos académicos y que sea el comienzo de un fructífero camino de cooperación internacional propiciado desde las universidades e instituciones que pertenecen a la Red.

9 789585 545786

UNIVERSIDAD LIBRE COLOMBIA

UNIVERSIDAD FASTA