APLICACIÓN DE LA EQUIVALENCIA FUNCIONAL DE LOS DATOS Y SU OBSERVANCIA A LA LEGALIDAD PROBATORIA EN LOS PROCESOS JUDICIALES DE DELITOS INFORMÁTICOS EN COLOMBIA[1]

Brayan José Hoyos Mieles[2]

Juan Ricardo Ulloa guerrero[3]

Luis Mateo Tamayo Patiño[4]

Resumen

Este trabajo investigativo tiene como objetivo establecer las acepciones jurídicas del cumplimiento de la legalidad probatoria en el trato de los datos electrónicos como documentos en Colombia desde el año 2019, también pretende buscar irregularidades en el tratamiento de las pruebas electrónicas en el delito de transferencia no consentida de activos. En cuanto a la metodología, se acudió al enfoque cualitativo, mediante el análisis de documentos. Como una de las principales conclusiones, aunque se observan muchos principios constitucionales, se denota que hay una vulneración al debido proceso, en cuanto a que no todos los jueces se encuentran capacitados para hacer una correcta valoración de los documentos tecnológicos que se practican como pruebas.

Palabras claves: debido proceso, delitos informáticos, equivalencia funcional de los datos, legalidad probatoria, neutralidad tecnológica.

[1] Artículo de revisión para la obtención del título de Abogado de la Universidad Católica Luis Amigó de la Facultad de Ciencias Políticas y Derecho, bajo la asesoría metodológica de la Doctora Laura Victoria Cárdenas y temática del Doctor Dany Steven Gómez; presentado por:

[2] Estudiante de Derecho de la Universidad Católica Luis Amigó. brayan.hoyosmi@amigo.edu.co

[3] Estudiante de Derecho de la Universidad Católica Luis Amigó juan.ulloagu@amigo.edu.co

[4] Estudiante de Derecho de la Universidad Católica Luis Amigó luis.tamayopa@amigo.edu.co

Abstract

This investigative work aims to establish the legal meanings of compliance with evidentiary legality in the treatment of electronic data as documents in Colombia since 2019, it also seeks to search for irregularities in the treatment of electronic evidence in the crime of non-consensual transfer of assets. Regarding the methodology, the qualitative approach was used, through the analysis of documents. As one of the main conclusions, although many constitutional principles are observed, it is noted that there is a violation of due process, in that not all judges are qualified to make a correct assessment of the technological documents that are practiced as evidence.

Key words: Cybercrime, due process of law, functional equivalence, Legal Standard of Proof, Technological neutrality.

INTRODUCCIÓN

Este artículo discurre sobre la observancia a la legalidad probatoria y el debido proceso en el tratamiento que, a la equivalencia funcional de los datos, se le ha dado en los procesos judiciales, en el delito informático de transferencia no consentida de activos en Colombia desde el año 2019.

Desde su adopción en el ordenamiento jurídico colombiano, la equivalencia funcional de los datos representó una alternativa afanada ante el lento desarrollo legislativo que no tenía prevista la forma en dar tratamiento a las pruebas electrónicas o digitales; de esta manera, tal y como su nombre lo indica, merced, a la equivalencia propuesta por dicha institución jurídica, a las pruebas digitales en procesos de delitos informáticos, pudo dárseles el mismo tratamiento procesal que a las documentales.

Respecto al tema procesal, la legalidad probatoria constituye uno de los presupuestos garantistas del sistema penal colombiano regulado en la Ley 906 de 2004, la cual establece los procedimientos, ritos y requisitos que deben tener las pruebas, entre ellas las documentales, para gozar de legalidad y respetar del debido proceso de quienes son procesados.

En ese sentido, este trabajo aborda el interrogante de cómo se ha observado la legalidad probatoria ante la equivalencia funcional, entre las pruebas digitales y documentales, esto a partir de un enfoque cualitativo hermenéutico riguroso, que permite identificar y analizar desde las diferentes acepciones jurídicas, leyes y sentencias judiciales en casos de delitos informáticos, la posible existencia de irregularidades o vulneraciones a la legalidad probatoria.

Este trabajo se propone desde una crítica dogmática jurídica el objetivo específico de establecer de qué manera se observa el debido proceso para quienes son o han sido procesados por el delito de la transferencia no consentida de activos, ante la aplicación de la equivalencia funcional de los datos desde 2019, y de esta manera, asentar conocimientos que generen inquietudes acerca de la aplicación de dicha figura.

A la fecha no se registran investigaciones que den cuenta de cómo la aplicación de la equivalencia funcional, ha observado la plenitud o cumplimiento de la legalidad probatoria en el mencionado delito informático en Colombia, a partir del análisis de decisiones judiciales que aborden dicho delito; circunstancia que hace que las investigaciones que tengan como propósito u objetivo no solo el indagar sobre la constitucionalidad de tal principio, si no las implicaciones sociales y jurídicas del tratamiento que se ha venido desarrollando desde los últimos años en relación a la equivalencia en los procesos judiciales, sean jurídicamente relevantes.

Este trabajo se propone en sus demás objetivos el análisis desde un ejercicio hermenéutico, en ese sentido se ha mencionado que:

> Es un trabajo constitutivo donde la interpretación, la crítica y la argumentación racional, juegan un papel preponderante porque permiten llevar a cabo inferencias y relaciones. Se trata de ir de la parte (unidad de análisis) al todo (fenómeno estudiado a través de la representación teórica), para explicitar un argumento de sentido que explique y totalice una cierta visión "paradigmática, semántica y pragmática" en orden a dilucidar una particular manera de apreciar el fenómeno, una construcción global de significados y una trascendencia en lo real de estos elementos con repercusiones prácticas en el entorno social. (Hoyos,2000, p.42)

En cuanto a la metodología, se acudió al enfoque cualitativo, mediante el análisis de literatura especializada, sobre el particular, Duque, González, Cossio & Martínez (2018) afirman: "su interés está centrado en la cotidianidad que es el espacio para comprender la realidad" (p. 61).

El anterior análisis se realizó con algunos precedentes judiciales acontecidos desde el año 2019, que hayan resuelto el aludido delito informático y las distintas acepciones jurídicas referentes al cumplimiento de la legalidad probatoria en el trato de los datos electrónicos como documentos, esto, para establecer la forma como se ha observado la legalidad probatoria en la aplicación de la equivalencia funcional de los datos, y el debido proceso de personas que hayan sido procesadas por este tipo penal.

I. Acepciones jurídicas del cumplimiento de la legalidad probatoria en el trato de los datos electrónicos como documentos

El desarrollo tecnológico en las últimas décadas ha hecho del internet no solo un escenario de redes sociales, sino también de redes criminales, convirtiéndose quizás en el espacio predilecto para la comisión de conductas reprochables que atentan contra bienes jurídicamente tutelados, como el patrimonio económico y la información. Esta situación obligó a los distintos Estados, entre ellos Colombia, al establecimiento de tipos penales y herramientas jurídicas que de alguna manera han permitido el enjuiciamiento de tales conductas. A este respecto se ha dicho que:

> Los delitos cometidos a través de las nuevas tecnologías han aumentado de manera proporcional a los avances producidos en la materia, ello ha dado lugar a la transformación del proceso de investigación criminal, reflejado en cierta medida en la última reforma de la Ley procesal penal. (Rodríguez, 2018, p.3)

Sumado a lo anterior, otros autores afirman que:

> En Colombia y el mundo, cada año aumentan las cifras de este tipo de conductas antijurídicas, toda vez que al incrementarse la ciber-criminalidad, la sociedad de hoy en día se ve expuesta como sujeto activo de dependencia de estos sistemas automatizados, en donde se controla todo tipo de áreas sea marítima, aérea o terrestre, en donde solo se pretende llegar a una seguridad autónoma con el fin de establecer un mejor desarrollo global en relación al derecho penal moderno, pues en sí, la informática ha establecido parámetros de desarrollo en la sociedad muy relevantes, y también se han creado vulneraciones hacia este nuevo sistema ya que nos encontramos en la era de la globalización, en la era de la tecnología en donde la sociedad actual depende de ésta ya que se han perdido aquellas costumbres que se establecieron algún día como medios de comunicación, trabajo, diversión, diálogos, entre otros. (Reyes, 2007. p.84.)

Respecto a lo anterior, debe agregarse que las tecnologías no solo influyeron en el ámbito penal, sino también en el resto de las áreas del derecho, de ahí que la normatividad colombiana tuviese que ajustarse desde su administración para adaptarse a las nuevas formas de relación en que la sociedad se encontraba inmersa. Así pues, la Ley Estatutaria de Administración de Justicia señalaría:

> El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información. Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones. Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales (Ley 270, 1996, art 95).

De esta manera, sería esta la primera disposición legal en Colombia en establecer las premisas concernientes a las pruebas digitales, manifestando que los documentos emitidos por medios técnicos, electrónicos, informáticos y telemáticos gozarían de validez y eficacia probatoria siempre que se garantizara su autenticidad, integridad y el cumplimiento de los demás requisitos exigidos por la ley, presupuestos estos de la legalidad probatoria. Respecto a estos medios, podrían entenderse de una manera genérica como datos informáticos, y conforme a estos, el Convenio de Budapest (2001) expresó que "Por datos informáticos se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función" (p.4).

Si bien esta norma aludida de alguna manera fue la primera en relacionar las pruebas digitales con las documentales, sería la Ley 527 de 1999 la que anunciaría la equivalencia funcional entre estos medios de prueba, significando esto que los ritos, procedimientos y elementos para estos serían iguales, respecto de las pruebas contenidas en papel. En ese sentido, esta norma en su artículo 6 rezaría respecto al reconocimiento jurídico de los mensajes de datos:

“No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos” (Ley 527, 1999, art. 6).

Conforme a lo anterior, se infiere que la intención del legislador con esta disposición fue la de reconocerle validez y eficacia probatoria a las pruebas digitales o datos informáticos, y la herramienta que utilizaron para esto, fue la antes mencionada, equivalencia funcional de los datos, el cual los hermanos Landáez Otazo y Landáez Arcaya (2007), afirman: “consiste en atribuirle la eficacia probatoria o mismo valor probatorio, a los mensajes y firmas electrónicas, que los que la ley consagra para las documentales ” (p.15).

En este orden de ideas, se entiende que la equivalencia funcional de los datos, como lo indica su nombre, hace equivalente el trato probatorio entre las pruebas digitales y documentales, no estableciendo procedimientos distintos entre estos en el proceso penal. Respecto a la relación entre la prueba digital y documental, se ha enunciado el documento electrónico, y en ese sentido el Consejo de Estado ha señalado que:

> Está contenido en soporte diverso al papel, lo que no significa que por esa razón no sea capaz de representar una idea o un pensamiento. Por ello lo han definido como cualquier representación en forma electrónica de hechos jurídicamente relevantes, susceptible de ser asimilado en forma humanamente comprensible. El documento electrónico es un método de expresión que requiere de un instrumento de creación, conservación, cancelación, y transmisión; tal instrumento está constituido por un aparato electrónico. De esta forma la disciplina de dicho documento no puede prescindir del computador que lo crea, lo conserva y lo cancela, y la red de terminales de computador que permiten su transmisión. (Consejo de Estado, Sección Cuarta, T-17155, 2011).

El interrogante que surge de las anteriores afirmaciones, es si la aplicación de la equivalencia funcional de los datos observa la legalidad probatoria y consecuentemente, el debido proceso; razón por la que es necesario establecer desde los criterios jurídicos, qué se ha entendido por esta.

Dentro de las diferentes acepciones jurídicas sobre el cumplimiento de la legalidad probatoria en la aplicación de la equivalencia funcional entre las pruebas digitales y documentales, se encuentra con la idea de autores, instituciones u organismos judiciales de que la legalidad probatoria se sustenta en la permisión que confiere la ley de introducir una prueba

digital o electrónica al proceso como una documental (equivalencia funcional de los datos), es decir, algunos juristas consideran que si dentro de la ley está permitida la aplicación de esta institución jurídica, se está cumplimiento la legalidad probatoria.

En ese sentido el Ministerio de Justicia y Derecho en concepto rendido ante la Corte Constitucional expresó que:

> El artículo 294 del nuevo Código Penal recoge en forma integral y general el concepto de documento y lo coloca acorde con nuestra realidad social y económica, a tono con los adelantos tecnológicos y científicos que se están presentando a nivel de la comunidad internacional con ocasión del fenómeno de la globalización, inclusive con aspectos relativos a la informática. A juicio del Ministerio de Justicia y del Derecho el artículo 294 del Código Penal engloba de manera amplia a los documentos electrónicos enmarcándolos dentro del principio de legalidad probatoria (Corte Constitucional, Sala Plena, C-356, 2003)

De esta manera, tal y como se mencionó, la legalidad probatoria se concibe como la aceptación que la ley confiere a la aplicación del dato electrónico en el proceso penal, como una prueba documental.

De otro lado, hay autores que definen la legalidad probatoria como aquel cumplimiento estricto de cada uno de uno de los requisitos intrínsecos y extrínsecos de la prueba, desatendiendo la creencia de que se basa exclusivamente en que la ley permita la aplicación de un medio de prueba. Así, Bedoya (2012) establece que:

> Además de la legalidad del procedimiento que da lugar a su obtención, las evidencias físicas son confiables cuando la parte que pretende usarlas como prueba se encuentra en capacidad de demostrar su autenticidad, esto es, cuando puede demostrar que una cosa u objeto es aquello que se dice que es, no sólo en cuanto a su entidad física (características, cantidad, peso, entre otras), sino en lo que se refiere a su origen (un documento elaborado o suscrito por una determinada persona), así como al lugar en el que fue hallada (la droga encontrada en un determinado domicilio o en poder de una determinada persona), entre otros aspectos. (p. 207)

Bajo esta premisa, se puede encontrar que son dicotómicos o contrarios estos paradigmas respecto de la legalidad probatoria, pues cada uno se sirve a determinar su definición, situación que hace más complejo analizar si en un caso específico una prueba digital tratada como documental cumple u observa la legalidad probatoria.

Partiendo de la idea de que la legalidad probatoria, tal y como lo alude la definición de que se entiende por ésta, el cumplimiento de los requisitos legales o el reconocimiento del debido proceso, es necesario evaluar si la aplicación de la equivalencia funcional observa los elementos, ritos y procedimientos necesarios para aprobar dicho presupuesto.

El código de procedimiento penal en su artículo 359, establece la exclusión, rechazo, e inadmisibilidad de los medios de prueba, permitiendo esto desde un ejercicio hermenéutico entender que el legislador también ve la legalidad probatoria como el reconocimiento del debido proceso, a partir del cumplimiento de los requisitos intrínsecos y extrínsecos de la prueba, como también de los demás preceptos probatorios que hacen legal la prueba, determinando las consecuencias a utilizar de no tenerse presente.

Es preciso tener en cuenta que si se habla de los requisitos intrínsecos de la prueba, se hace referencia a la conducencia del medio, la pertinencia o relevancia del hecho objeto de la prueba, la utilidad del medio, la ausencia de prohibición legal; y cuando se habla los requisitos extrínsecos se refiere a la oportunidad procesal o ausencia de preclusión, las formalidades procesales, la legitimación y postulación del juez que la decreta de oficio, la competencia del juez, la ausencia de impedimentos legales entre el juez y los funcionarios que operan en la producción de la prueba, entre otros criterios que determinan la legalidad y licitud de la prueba. A continuación, con el objeto de precisar conceptos, se explicará los requisitos intrínsecos de la prueba más relevantes para esta investigación.

Como se mencionó anteriormente, el primer elemento o requisito para la admisión de la prueba es la conducencia, respecto a este Echandía (2000) manifiesta que “la conducencia de la prueba es la aptitud legal o jurídica de la prueba para convencer al juez sobre el hecho a que se refiere”. (p.158)

Por otro lado, otro elemento del requisito intrínseco es la cadena de custodia, respecto a este es importante aclarar que la cadena de custodia de los elementos materiales probatorios que hacen parte del proceso, se expone que estos deben ir acorde a el Manual de Cadena de Custodia, por lo que deben seguir ciertos parámetros para que gocen de completa autenticidad, de manera que se evidencie la correcta aplicación del principio de mismidad, dicho esto, es correcto afirmar que para el derecho procesal penal, los elementos materiales probatorios gozan

de autenticidad, es decir, demuestran que sí son los mismos descubiertos o recolectados, cuando los protocolos de cadena de custodia han sido respetados, pero cuando se han incumplido o cumplido parcialmente aquellos protocolos, el elemento de prueba queda afectado en su aptitud probatoria, es decir, no tiene eficacia demostrativa porque carece de credibilidad y la valoración que en su momento hace el juez resulta afectada, en perjuicio del proceso penal, para Quijano (2000), "los actos que vulneren garantías reconocida por esta constitución carecen de toda eficacia probatoria". (p.25)

Ahora bien, los responsables de aplicar los protocolos de cadena de custodia, son los servidores públicos que entran en contacto con los elementos de prueba o evidencia física y en ocasiones los particulares por razón de su trabajo o función, tal y como así lo regula el artículo 255 del Código de Procedimiento Penal, (2004), lo cual indica que el incumplimiento a uno o a varios de esos factores, hace que el elemento de prueba carezca de convicción por no estar acreditada su procedencia o sobre la forma como se produjo o recolectó. Es importante aclarar que para la conservación de la cadena de custodia en los delitos informáticos tales como la "transferencia no consentida de activos" la aplicación del mencionado principio de mismidad resulta diferente, puesto que la conservación de dichos elementos de autenticidad y veracidad recaen sobre el sujeto pasivo, pudiéndose comprobar a partir de la informática forense, la cual permitirá al Juez tener una correcta apreciación de las pruebas digitales aportadas al proceso, para que de esta manera se pueda tener certeza de la veracidad de las mismas, aplicando así el debido proceso. (Fiscalía General de la Nación, 2012, p. 215)

Además, la ley procesal penal exige cumplir los procedimientos establecidos para garantizar la protección o conservación del elemento de prueba o evidencia física, a partir de su descubrimiento o recaudo, tal es el caso de las memorias USB que tal y como manifiesta Nissimblat (2013) "...se pueden presentar como prueba, pero no se deben abrir por ningún motivo, y se deben embalar".(p.236) Para la Corte Suprema de Justicia, Sala de Casación Penal, Radicación 25.920, (2007) "el incumplimiento de estos protocolos afecta la aptitud probatoria del elemento y traslada la carga de acreditación a la parte que alegue defectos en la cadena de custodia" (p. 8).

La finalidad del principio de mismidad (cadena de custodia), más que garantizar la autenticidad de los elementos de prueba, con miras a preservar su fuerza demostrativa y validez jurídica, tiene relación con el derecho al debido proceso el cual eventualmente resulta violado si en las actuaciones judiciales tendientes a la recolección de los elementos de prueba o evidencias físicas, se violan las disposiciones que regulan el proceso de cadena de custodia regulado en los artículos 254 a 266 del Código de Procedimiento Penal.

Otro elemento intrínseco, como antes se mencionó, que indispensablemente debe respetarse es la autenticidad de la prueba, respecto a este se ha dicho que:

> El uso probatorio y el valor probatorio de los documentos tiene importancia una vez que se asume que el documento es genuino y auténtico, y esto es obvio cuando el documento reúne las condiciones para ser empleado como prueba de un hecho o de un acto jurídico (Ragone, 2014,p.199)

Conforme a lo anterior se infiere que la prueba debe ser contentiva de estos elementos para el respeto del debido proceso, indicando esto, según algunos juristas, los valores que determinan la legalidad probatoria y que serán necesarios evaluar en la aplicación de la equivalencia funcional de los datos para determinar su observancia.

II. Transferencia no consentida de activos y sus irregularidades en el tratamiento de las pruebas electrónicas

En este acápite se tratará el tema de cómo la revolución tecnológica de las últimas décadas, hizo de las redes informáticas un estadio de constantes y permanentes interacciones humanas, situación que obligó al legislador colombiano al establecimiento de delitos informáticos que protegieran bienes jurídicamente tutelados, ante el crecimiento exorbitante de conductas lesivas contra estos que venían presentándose. Así pues, como respuesta a esta problemática, se expidió la Ley 1273 de 2009, el cual expresa:

> Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Ley 1273, 2009).

La creación del bien jurídicamente tutelado de la información posibilitó hacer punible las conductas que atentaran contra esta, siempre que la conducta tuviese como medio o acontecieran en el escenario informático, aspecto distinto a los tipos tradicionales. Respecto del delito informático se ha dicho:

> Son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinada a producir un perjuicio a la víctima, atentados a la sana técnica informática, lo cual, generalmente producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.(Díaz, 2010, p.5)

Como complemento de lo anterior, Rodríguez (1997) respecto a la definición de los delitos informáticos expresó que es "una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o elemento telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (p.15).

Entendida la definición de los delitos informáticos, es presente establecer los elementos principales del delito que se estudia en este trabajo, el cual es la transferencia no consentida de activos, tipo penal enunciado en la misma Ley 1273 de 2009, de esta manera se podrá determinar las irregularidades que se presentan en el enjuiciamiento de este delito, como consecuencia de la aplicación de la equivalencia funcional de los datos. Así pues, el artículo 269J de esta normativa expresa que:

> Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
>
> Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad. (Congreso de Colombia, Ley 1273, 2009).

En este orden de ideas, la transferencia no consentida de activos, es entendida desde esas transferencias en lo contable y también en la parte automática que se desliga de los valores activos, estos comprendidos como dinero en la parte contable; es por esto que, al no ser autorizado, ni la manifestación de la voluntad hay carencia de consentimiento, por tanto, el titular de esto, perjudica a un tercero. Al tenor, Gómez (2012) manifestó: "respecto de las manipulaciones informáticas, se entiende toda alteración o modificación de datos ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración". (p.424)

La criminalidad en el área informática, cubre casi todas las figuras punibles tradicionales, ya que a su modalidad, son ejecutadas por un sujeto activo, esto lo hace en modo circunstancial en las redes de la información o también llamadas de la comunicación, desde los telemáticos, sistemas informáticos, bases de datos, hasta los correos electrónicos, dejando evidencia de cada una de sus actuaciones o manipulaciones; los cuales ponen en peligro los bienes jurídicos individuales como lo es claramente, la libertad, la intimidad y como lo es en este caso, el patrimonio económico.

Este delito se faculta por las acciones y funciones realizadas en la informática que van orientadas, desde adquirir información, acceder, a divulgar, disponer, crear, manipular, transferir, conocer, procesar, adquirir, almacenar, con un fin que no es consentido por el titular de estos datos; debido a esto que como prueba estaría, la " transferencia hasta el momento en el que se "consigue" el traspaso fáctico de los activos patrimoniales, pues, se estima que dicha obtención de fondos afecta el patrimonio económico del sujeto pasivo". (Maya, 2012, p.16)

Expuesto lo que se entiende por el delito de transferencia no consentida de activos, es menester analizar las evidencias que sirven como medio de prueba para este tipo penal, así como también la forma como se valoran estas en el proceso penal, circunstancias que permitirán determinar su observancia a la legalidad probatoria.

En este sentido, como garantía para velar la seguridad de las personas en cuanto al funcionamiento, como también con la aplicación de las pruebas electrónicas, existe una protección por parte de las entidades, que busca una seguridad a los usuarios desde la no divulgación de sus datos electrónicos, que se encuentren en su poder, ya que, si no se autoriza,

estos no deben ser transferidos a otras entidades, debe existir un consentimiento, o cuando alguna autoridad, estime necesario ser conocedor de estos datos, con un fin específico.

> Dentro de estos mismos poderes debe existir la posibilidad que las autoridades competentes puedan exigir al prestador del servicio los datos llamados por nuestra legislación "sensibles". E incluso con la posibilidad de registro y decomiso, sin la necesidad de solicitar una orden ante el juez de control de garantías (competente), sin desconocer que esta actividad debe ser realizada por personal altamente calificado e idóneo en la materia. (Naranjo, 2011, p.45)

Lo establecido, por el artículo Art. 275 del código de procedimiento penal, Ley 906 del 2004, abarca, cuales elementos materiales probatorios y evidencia física e información, es por esto, que toda evidencia que se dé por transacción sin un consentimiento manipulación entrarían a ser parte de los elementos materiales probatorios y así convertirse en prueba si se incorporan en el juicio y cumplen los tres criterios de valoración: legalidad, autenticidad e identificación técnica científica.

La prueba digital es algo relativamente nuevo, por lo que es entendida como todo lo que se obtener desde los formatos digitales, es por esto que cualquier información que sea obtenida por medios electrónicos o de comunicación, donde exista la manipulación del ser humano, esto da lugar a que se debe:

> Considerarse a la evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales. Con esto nos referimos a registros almacenados en el equipo de tecnología informática, como pueden ser correos electrónicos, archivos de aplicaciones de ofimática, imágenes, entre otros; también registros generados por los equipos de tecnología informática, como por ejemplo auditoría, transacciones, eventos, entre otros; y registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática, en tal caso serán hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, entre otras. (Bendinelli, 2014, p.4)

Al dar paso a un delito en el campo de la informática o de las comunicaciones, ha cambiado sustancialmente la forma de como probar los hechos, ya que estos delitos se dan en una esfera diferente, al no ser algo tangible o convencional, se ha dado ciertas especialidades que dan lugar al tratamiento de estas pruebas y a su valoración, por lo que, "así mismo, en los medios de prueba electrónica hay dos clases, la primera, es la información almacenada en un dispositivo

electrónico y la segunda, es la que se transfiere por redes de comunicación, ejemplo el internet, telefonía fija o móvil" (Sichaca, 2019, p.15).

En el campo del Derecho procesal, la valoración de una prueba digital ha tenido gran impacto ya que es clave cada detalle a la hora de probar y por tanto darle el valor a esta, buscando como finalidad esclarecer el suceso que dio lugar al hecho, donde el juez desde la sana crítica y las reglas de la experiencia, da esa valoración al momento de que esa prueba es incluida en el proceso y al momento de fallar, ya que esta puede tener la característica de objeto y medio para probarse y darle un valor.

> Siempre que se trate de probar un hecho ocurrido en un medio electrónico, el medio de prueba que debe servir como ruta de acceso, debería ser el dictamen pericial, o de lo contrario, de nada serviría aportar una prueba de este tipo a un proceso, en donde el juez está imposibilitado para entender algo para lo que no está preparado, por no ser ingeniero o perito informático, según sea el caso, o por lo menos el caso se tornaría de una complejidad bastante alta que debería probarse con base en la probabilidad que le ofrezcan otros medios de prueba (Reyes, 2013, p.1060).

El juez debe valorar los documentos y pruebas digitales de igual forma que los tangibles, de lo contrario, existiría una violación al principio de contradicción de la prueba, es por esto que el código general del proceso colombiano trae en su artículo lo siguiente que fue incluida como la:

> Valoración de mensajes de datos. Serán valorados como mensajes de datos los documentos que hayan sido aportados en el mismo formato en que fueron generados, enviados, o recibidos, o en algún otro formato que lo reproduzca con exactitud. La simple impresión en papel de un mensaje de datos será valorada de conformidad con las reglas generales de los documentos" (Ley 1564, 2012, art.247).

Ahora bien, es importante hacer referencia a la alteración de documentos electrónicos, puesto que es uno de los principales riesgos a los que se pueden ver expuestos estos elementos materiales probatorios, en ese sentido, expresa la Real Academia Española (s.f.), el verbo alterar implica: " 1. tr. Cambiar la esencia o forma de algo. 2. tr. Estropear, dañar, descomponer.", entendido de esta manera, ¿Qué herramientas procesales pueden ser utilizadas para controvertir una prueba digital alterada?, para resolver este interrogante, nos referiremos a la tacha de falsedad, la cual es entendida como:

> (...)los documentos en general, y entre ellos los documentos públicos, pueden ser objeto de falsedad, en dos modalidades: material e ideológica. Si se trata de falsedad material en medio judicial idóneo para redargüir la autenticidad del documento público, es el incidente de tacha de falsedad previsto en los artículos 289 y ss donde se entra a establecer si el mismo ha sido objeto de alguna alteración en su texto a través de tachaduras, borrones, supresiones, en fin todo aquellos que conduzca a mutar su tenor literal. A contrario sensu, el mismo incidente no fuera si la falsedad es ideológica, pues consistiendo la misma en la falsedad intelectual del contenido del documento, su demostración queda sujeta a la libertad de medios probatorios, de modo tal que el interesado en provocar su declaración pueda valerse de diferentes pruebas para acreditar que pese a la autenticidad de un documento su literalidad refleja una realidad que dista ostensiblemente de la verdad.(...) (Consejo de Estado Sección Quinta, Rad 11001-03-28-000-2006-00090-00, 2008).

Tal y como lo expone lo anterior, la tacha de falsedad constituye una primera garantía para que el procesado controvierta la autenticidad de la prueba digital aportada, esto ante la presunción de legalidad de la que goza la misma, queriendo decir esto que si no se desvirtúa tanto la mismidad, integridad y la misma autenticidad, la prueba digital gozará de validez y eficacia probatoria. Cabe mencionar que para el ejercicio de la tacha de falsedad la defensa, es necesario recurrir a la informática forense, al tenor se ha dicho que: la informática forense se define como una disciplina o herramienta que permite adquirir, preservar, recuperar y presentar los datos que han sido procesados electrónicamente y almacenados en soportes informáticos, para que de esta manera se puedan recopilar y analizar datos de los sistemas informáticos y redes para que luego puedan ser incluidas como pruebas en un proceso penal. Esta herramienta serviría como auxiliar de la justifica asegurando así el debido proceso. (Informática Forense Colombiana, 2017; Federal Bureau of Investigation, s.f.)

Sumado a lo anterior, la informática forense como técnica para hallar los datos electrónicos se sirve de procedimientos técnicos, como, por ejemplo:

> La creación de copias "bit a bit" de la información almacenada y/o eliminada, a través del llamado 'writeblocking' para garantizar que la información original no se cambie y el archivo criptográfico 'hash', o firmas digitales, con el fin de demostrar posibles cambios en la información. (Ronderos, 2015, p.35)

Además de la tacha de falsedad, según Correa D, Peña E & Viera G,(2008) las partes gozan de la cláusula de exclusión para desvirtuar o quitarle validez probatoria a un documento

electrónico. Ésta es una garantía constitucional contenida en el inciso final del artículo 29 de la Constitución Política de Colombia.

Expuestos someramente estos mecanismos de contradicción como prerrogativas del derecho fundamental del debido proceso, habrá que determinar si basta con el ejercicio de estos para que se garantice el debido proceso, ante la aplicación de la equivalencia funcional de los datos. En este sentido, se entiende por el debido proceso el derecho a "presentar pruebas y a controvertir las que se alleguen en su contra; es nula, de pleno derecho, la prueba obtenida con violación del debido proceso".(Const.,1991, art.29)

Dicho de otro modo por la doctrina:

> El debido proceso es un derecho fundamental que comprende las garantías constitucionales que debe reunir todo proceso penal para asegurar al imputado la certeza, la justicia y la legitimidad de su juzgamiento, desde el inicio del proceso, pasando por los actos de investigación, sus controles judiciales, la actividad preparatoria y probatoria, las distintas audiencias públicas, los mecanismos de impugnación, el respeto de los términos procesales, hasta la obtención de un fallo basado en la prueba y en la justicia del caso… (Jiménez & Valdés, 2009, p. 27).

De igual manera, la Corte Constitucional se ha manifestado en incontables ocasiones acerca de la importancia del debido proceso, estableciendo que toda autoridad tiene sus competencias definidas y sus actuaciones deben ceñirse estrictamente al cumplimiento del principio de legalidad (Corte Constitucional Sala Octava, Sentencia T-1341,2011), así como también ha dicho en repetidas ocasiones que la cobertura de este principio ha de extenderse a todo tipo de actuaciones realizadas por la administración pública (Corte Constitucional, sentencias T-442, 1992; T-020,1998; T-386,1998; T-009,2000).

Aludidos los elementos o principios que deben reunirse para la garantía del debido proceso, es indispensable determinar si bajo la aplicación del principio de equivalencia funcional en los delitos informáticos, específicamente en la transferencia no consentida de activos, se observa el cumplimiento de cada uno de estos.

Dicho anteriormente, los mecanismos tales como la tacha de falsedad y la exclusión de la prueba han sido observados plenamente en el trato de las pruebas digitales, circunstancia que colige la garantía de estos. Respecto al principio de legalidad y defensa técnica, es factible

evidenciar que igualmente se obedecen, toda vez que el primero se tiene que disposiciones anteriormente aludidas como la Ley 270 de 1996 y la 527 de 1999 regulan dicha figura, y del segundo sobraría decir además que se faculta al procesado a que tenga un defensor. En relación al juez competente y la observancia de la plenitud de las formas propias de cada juicio, es donde surgen los interrogantes respecto a su cumplimiento, pues los jueces no han sido capacitados para el manejo de las pruebas digitales, al tenor de dijo que:

> Ahora bien, dentro del Plan de Formación del año 2020 las temáticas incluidas en el subprograma de Tecnologías de la Información y las Comunicaciones son: el uso de herramientas informáticas en la Rama Judicial, el manejo de plataformas digitales y herramientas colaborativas como office 365 y la ponencia digital, el uso de las TIC en la gestión judicial, las audiencias virtuales, las notificaciones digitales y la prueba digital, entre otras.

Dado que, a partir del Plan de Formación del presente año, se incluyó en el subprograma de TIC la temática de la prueba digital, no es posible aportar información o estadísticas previas en los procesos de formación de años anteriores, como tampoco la cantidad de servidores judiciales capacitados, toda vez que no hemos iniciado su ejecución. (Consejo Superior de la Judicatura, Escuela Lara Bonilla,Respuesta Derecho de Petición , Rad: EJO20-409, mayo 2020).

De lo anterior se infiere pues que el tipo penal de la transferencia no consentida de activos protege no solo el patrimonio económico, sino también la información, queriendo decir que el legislador quiso darle a esta la calificación de activo, consistiendo en la transferencia malintencionada de datos sensibles del sujeto pasivo.

III. Precedentes judiciales del delito de transferencia no consentida de activos

La equivalencia funcional de los datos, ha sido una figura jurídica cuestionada mediante demandas de inconstitucionalidad, por representar un trato indiscriminado de las pruebas digitales y documentales en el proceso penal , se afirma que hay una flagrante violación a la legalidad probatoria y el debido proceso, toda vez que a juicio de los distintos demandantes, esta disposición legal no previa que por su naturaleza los documentos tradicionales y los

digitales deprecan de unos ritos, procedimientos y requisitos diferentes a fin de garantizar la legalidad probatoria. En ese sentido, dicha normativa señala que:

> Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente, habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente. (Ley 527,1999, art. 11)

En ese sentido, puede observarse que Ley 597 de 1999 de alguna manera establece los requisitos que deben emanar de la prueba digital para su plena legalidad probatoria, el cual es, la identificación de la integridad, autenticidad y confiabilidad; criterios no diferenciables de los documentos tradicionales como medios de prueba, que en últimas terminan por gozar de los mismos, situación que evidencia una intención del legislador de dar plenamente ese trato equivalente sin establecer premisas o requisitos propios, que distinga entre las pruebas digitales y documentos físicos. En esos términos, se ha expresado que:

> Así las cosas, el documento electrónico tiene una naturaleza diversa al documento tradicional, pues este se materializa a través de un software y un hardware, es inmaterial, por cuanto no tiene un carácter tangible, y cuenta con una serie de características que le otorgan un grado de seguridad jurídica similar a la del documento en papel, debiendo contar con las características de la norma técnica NTC/ISO 15489-1, las cuales son: autenticidad, integridad, fiabilidad y la disponibilidad, características que ha reconocido el Ministerio de Tecnologías de la Información y las Comunicaciones (Gómez, 2020, p.224).

Es precisamente la manifestación divergente de la prueba digital lo que se ha discutido jurisprudencialmente, pues la Ley no es lo suficientemente precisa al establecer las prerrogativas por las que probatoriamente se adelanta la equivalencia funcional de los datos, queriendo decir esto el trato sería completamente igualitario e indiscriminado, siendo los procedimientos, ritos y requisitos iguales tanto para las pruebas documentales como para las digitales.

Ha sido labor de la jurisprudencia establecer si la naturaleza distinta entre los documentos y mensajes de datos, exige del establecimiento de procedimientos no comunes entre estas formas de pruebas, con el fin de determinar si constituye la equivalencia funcional de los

datos, o la norma que lo regula, una violación de los principios constitucionales y por ende una declaración de inexequibilidad. De manera aproximada esta autoridad judicial manifestó que:

> En suma, para la impugnación, la inconstitucionalidad del aparte cuestionado se deriva de que, al otorgar el mismo valor probatorio a la impresión de los mensajes de datos que a los mensajes de datos mismos, presentados estos de la manera exigida por la Ley 527 de 1999, se ignora que la primera modalidad no refleja "ni sumariamente" el contenido de la información, de manera que "*si en todos los casos que medien pruebas, se les diera validez jurídica a los mensajes de datos impresos, es decir, a la simple impresión de un documento digital, se estaría violando el debido proceso, el derecho defensa, además del derecho de contradicción que se puede ejercer sobre estos*".(Corte Constitucional, Sala Plena, C-604, 2018)

Lo anterior evidencia la constante inquietud de que por el contenido mismo de las pruebas digitales, se debería dar un trato discriminado o diferente a las mismas en relación con las pruebas documentales, pues como se ha expresado, los mensajes de datos son elementos intangibles susceptibles de alteraciones o modificaciones que implican un mayor análisis que evidencie su integridad, autenticidad y fiabilidad; premisas que serían complejas evaluar si el procedimiento que se sigue es el mismo de las pruebas documentales.

Al día de hoy la jurisprudencia no ha declarado inexequible la normatividad que consagra la aplicación de la equivalencia funcional de los datos en los delitos informáticos, esto bien sea porque a su juicio el trato indiscriminado no representa una violación a la legalidad probatoria o al debido proceso mismo, o por que las personas que han acudido a la acción pública de inconstitucionalidad no han podido comprobar en los cargos la forma como estos se manifiestan. No obstante, habrá que analizarse propiamente desde los expedientes judiciales de casos de delitos informáticos, del delito de transferencia no consentida de activos consagrado en el artículo 269I del Código Penal Colombiano, que es el objeto de este estudio, si se presentan irregularidades o vulneraciones a la legalidad probatoria en la aplicación de la equivalencia funcional de los datos.

CONCLUSIONES

Luego de realizar un análisis hermenéutico de las acepciones jurídicas que estipulan la aplicación de la equivalencia funcional de los datos y su observancia a la legalidad probatoria en los procesos judiciales de delitos informáticos en Colombia, específicamente el de transferencia no consentida de activos; se puede evidenciar que en las diferentes etapas del proceso penal pese al reciente crecimiento de la ciberdelincuencia y sus diferentes modalidades, el sistema procesal penal ha implementado la equivalencia funcional de los datos y la legalidad probatoria, tomando estas pruebas que por su características son intangibles, dándoles un trato y valoración similar o igualitaria a las pruebas tangibles o también llamadas documentales.

La aplicación de la equivalencia funcional de los mensajes de datos en su mayoría, ha tratado de garantizar el debido proceso, y demás requisitos intrínsecos y extrínsecos que debe reunir la prueba para ser aportada al proceso; sin embargo, hablándose de principios tales como la competencia del juez o tribunal con observancia de la plenitud de las formas propias de cada juicio quedan en tela de juicio, toda vez que la Escuela Judicial Rodrigo Lara Bonilla, no había capacitado a los funcionarios judiciales al manejo de las pruebas digitales, sólo hasta 2020 inició con los módulos de formación en el tema, circunstancia que denota improvisación (más allá de una asignación de competencia legal o constitucional) al momento de valorar la prueba digital, razón por la que algunas de las decisiones podrían tener confusiones.

Se tiene además que elementos intrínsecos como la cadena de custodia deben guiarse a partir de procedimientos orientados por la informática forense, un factor distintivo de las pruebas documentales, los cuales tendrán aplicación una vez el procesado o la misma Fiscalía General de la Nación mediante el organismo adscrito a esta, el Cuerpo Técnico de Investigación(CTI) soliciten su análisis, garantía esta del debido proceso; pese a esto, se halla una desventaja por parte del procesado para establecer desde la tacha de falsedad y la cláusula de exclusión la falta de autenticidad, integridad y mismidad de la prueba, factor más que podría verse como inobservancia a la legalidad probatoria y el debido proceso.

Se tiene por propuesta que el legislador dé o establezca un tratado discriminado a las pruebas electrónicas a fin de que sus intentos ritos garanticen el debido proceso.

Referencias

Bedoya Sierra,L (2012) *Prueba en el proceso penal colombiano* (Informe, Fiscalía General de la Nación)

Bedoya, L. (2008). *La prueba en el proceso penal colombiano.* https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/LaPruebaenelProcesoPenalColombiano.pdf

Bendinelli, M. (3 de Diciembre de 2014). Microjuris.com Inteligencia juridíca. doi: MJ-DOC-6987-AR | MJD6987

Caballero, A. G. (28 de Abril de 2016). Legis Ámbito Jurídico: https://www.ambitojuridico.com/noticias/procesal-y-disciplinario/la-valoracion-de-l a-evidencia-digital-en-el-codigo-general-del

Cano, J. J. (2006). Introducción a la Informática Forense, Una disciplina técnico-legal. Sistemas (96), 64-73.

Congreso de Colombia (31 de agosto de 2004) por la cual se expide el Código de Procedimiento Penal. [Ley 906 de 2004]. DO: 45.658

Congreso de Colombia (18 de agosto de 1999) Artículo 11. Ley de uso de los mensajes de datos. . [Ley 527 de 1999].DO: 43.673

Congreso de Colombia. (5 de enero de 2009). Artículo 269F [Título I]. Ley de delitos informáticos [Ley 1273 de 2009]. DO: 47.223.

Congreso de Colombia. (7 de marzo de 1996) Ley Estatutaria de Administración de Justicia. [Ley 270 de 1996]. DO: 42.745.

Congreso de la República, (12 de julio de 1996), Ley 290 de julio 1996, por la cual se modifica el parágrafo 1º del artículo 51 de la Ley 152 de 1994. DO:42.830

Congreso de la República, (24 de julio de 2000), Ley 599 del 24 de julio de 2000, por el cual se expide el Código Penal, DO: 44.097

Consejo de Estado, Sección Cuarta. (10 de febrero de 2011) Sentencia T-1715, 2016.[C.P. Hugo Fernando Bastidas]

Consejo de Estado, Sección Quinta. (19 de septiembre de 2008) Rad 11001-03-28-000-2006-00090-00, 2008.[C.P. Reinaldo Chavarro Buriticá]

Consejo Europeo, (23 de Junio de 2001) Página 2 (Preámbulo) *Convenio sobre la Ciberdelincuencia*,: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo Superior de la Judicatura, Escuela Judicial “Rodrigo Lara Bonilla” (mayo 2020) Respuesta a Derecho de Petición, Rad: EJO20-409.

Constitución Política de Colombia [Const.] (1991) Artículo 29 [Titulo II]. 2da Ed. Legis.

constitucionales y técnicas criminalísticas. Bogotá D.C. Defensoría del Pueblo.

Correa D, Peña E & Viera G,(2008) La Cláusula de Exclusión (Trabajo de Grado) https://repository.ucc.edu.co/handle/20.500.12494/10218?mode=full

Corte Constitucional de Colombia (30 de julio de 1998)T-386-98 [MP Carlos Gaviria Díaz]

Corte Constitucional de Colombia, Sala de Revisión No.6 (3 de julio 1992) sentencia T-442-92 [MP Simón Rodríguez Rodríguez]

Corte Constitucional de Colombia, Sala Octava. (11 de diciembre de 2001) Sentencia T-1341[MP Álvaro Tafur Galvis]

Corte Constitucional de Colombia, Sala Primera de Revisión (10 de febrero de 1998) Sentencia T-020-98 [MP Jorge Arango Mejía]

Corte Constitucional de Colombia, Sala Tercera de Revisión (18 de enero de 2000) T-009-00 [MP Eduardo Cifuentes Muñoz]

Corte Constitucional de Colombia, Sala Plena. (2 de noviembre 2016) Sentencia C-604/16 [M.P. Luis Ernesto Vargas Silva]

Corte Constitucional de Colombia, Sala Plena. (6 de mayo de 2003) Sentencia C-356-03 [MP Jaime Araujo]

Corte Constitucional, Sala Plena (2003) Sentencia C-356-03 [MP Dr. Jaime Araujo Rentería]

Corte Suprema de Justicia, Sala de Casación Penal, (2007, febrero), Radicación 25.920, [M.P. Javier. Zapata Ortiz]

Corte Suprema de Justicia, Sala de Casación Penal. (12 de junio de 2013) Sentencia 243368-2013. [MP José Leonidas Bustos Martínez]

Corte Suprema de Justicia, Sala de Casación Penal. (15 de mayo de 2019) Sentencia AP1802-2019. [MP Luis Antonio Hernández Barbosa]

Díaz García, A. (7 de enero de 2010). Aniversario en Colombia del nuevo delito de violación de datos personales. Primer año de vigencia de la Ley de Delitos Informáticos. En Derecho, telecomunicaciones y tecnología. disponible en: http://alejandrodelgadomoreno.com/2010/01/aniversario-de-la-ley-de-delitos.html

Duque, S, González, F, Cossio, N & Martínez, S. (2018). *Investigación en el saber jurídico*. Universidad de Antioquia.

Echandía, D. (2000) Compendio de la Prueba Judicial- Tomo I https://www.academia.edu/35320329/COMPENDIO_DE_LA_PRUEBA_JUDICIAL_TOMO_I_HERNANDO_DEVIS_ECHANDIA_p

Federal Bureau of Investigation(s.f.) 10 tools used by FBI for PC analysis

Fiscalía General de la Nación (2012). Manual de procedimientos para cadena de custodia. Bogotá: Fiscalía General de la Nación.

Gómez (2020) Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. Ratio Juris, 15 (30),15-282. doi: 10.24142/raju.

Gómez, L. O. (2012). Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. (U. Facultad de Derecho y Ciencias Sociales, Ed.) Derecho y Realidad (20), 424. ISSN: 1692-3936

Hoyos, C. (2000) Un modelo para Investigación Documental. Medellín: Señal Editora, 2000.

Informática Forense. (2017) Informática Forense en Colombia.: http://www.Informatica forense.com.co/index.php/joomla-overview

Jiménez Montes, Fernando & Valdés Moreno, Carlos. (2009). Fundamentos

Landáez Otazo, & Landáez Arcaya (2007) *La Equivalencia Funcional, la Neutralidad Tecnológica y la Libertad Informática (1) (P 24)*: http://servicio.bc.uc.edu.ve/derecho/revista/3-2007/art%201.pdf

Maya, R. P. (12 de Septiembre de 2012). El delito de transferencia no consentida de activos. Revista de Derecho y comunicaciones y nuevas tecnologías (8), 16. doi:ISSN 1909-7786

Mesa Elneser, Vásquez Santamaría, Lalinde Pulido & Pineda Cárdenas. (2013) Aproximación a la informática forense y el derecho informático: Ámbito Colombiano: Universidad Católica Luis Amigó

Naranjo, J. R. (2011). Dificultades en el manejo de la evidencia digital en el proceso penal Colombiano. 45. doi: CONPES 3701 DE 2011

Naranjo, J. R. (2011). *dificultades en el manejo de la evidencia digital en el proceso penal colombiano* . (U. A. Latinoamericana, Ed.) 39. doi: CONPES 3701 DE 2011

Nissimblat, N, (2013). Derecho probatorio: introducción a los medios de prueba en el Código general del proceso : principios y medios de prueba en particular. https://www.academia.edu/5102407/DERECHO_PROBATORIO_NATTAN_NISIMBLAT

Pino, S. A. (2009). Manual de manejo de evidencias digitales y entornos informáticos. Ecuador: Fiscalía General del Estado.

Quijano, J (2007): *Manual de derecho probatorio*, Librería de ediciones del profesional, décima sexta edición, pág. 25 y 70, Bogotá.

Ragone, Álvaro. (2014).La prueba documental en el Código General del Proceso de Colombia.

Real Academia Española (s.f.), Definición del concepto alteración.

Reyes Cuartas, J. F. (2007). El delito informático en Colombia: insuficiencias regulativas. Revista Universidad Externado, (28), 84.

Reyes, C. C. (20 de Enero de 2013). La valoración del documento electrónico en Colombia 103: file:///C:/Users/ROBINSON/Downloads/Dialnet-LaValoracionDelDocumentoElectronicoEnColombia-6713655.pdf

Rodríguez, M. (2018)*La prueba digital en el proceso penal.* Tenerife: Universidad de la Laguna: https://riull.ull.es/xmlui/bitstream/handle/915/7290/LA%20PRUEBA%20DIGITAL%20EN%20EL%20PROCESO%20PENAL.pdf?sequence=1&isAllowed=y

Ronderos, J. (2015) La Prueba Digital en el Contexto Jurídico Actual. https://www.deceval.com.co/portal/page/portal/Home/Marco_Legal/Eventos/Presentacion_Deceval_JGRFINAL.pdf

Sichaca, D. P. (2019). Requisitos jurídicos para la validez jurídica de la prueba digital. 15 : https://repository.ucatolica.edu.co/bitstream/10983/23853/1/Trabajo%20Prueba%20Digital%20aprobado.pdf