ÁMBITO DE VALIDEZ DE LA PRUEBA ELECTRÓNICA EN LOS DELITOS INFORMATICOS

Eduwin Jesús Nobles Pérez

Édison Narváez Chala

Andrés Felipe Rúgeles Montoya

Resumen

En el presente artículo de revisión, se esbozan los elementos de validez de la prueba electrónica en el caso de los delitos informáticos, con ocasión a la Ley 1273 de 2009, la cual, entró a modificar el código penal, Ley 599 del 2000. Lo cual, se realizó a partir del enfoque metodológico de la naturaleza cualitativa, enmarcado en el método dogmático y haciendo venia al método de recolección de información, consistente en la revisión documental.

Además, cuestiona la realidad subjetiva a través de la pregunta de investigación, ¿Cuáles son los criterios de validez vigentes de la prueba electrónica en los delitos cibernéticos? Lo que implicó, establecer el abordaje conceptual del objetivo general consistente en analizar los criterios de validez vigentes de la prueba electrónica y la prueba convencional en los delitos cibernéticos, implementados por la Ley 1273 de 2009. El cual, se diluye en dos objetivos específicos: i) Definir los elementos objetivos que debe cumplir la prueba electrónica a diferencia de la prueba convencional; ii) Determinar el ámbito jurídico penal de los delitos cibernéticos consagrados en el código penal colombiano, Ley 599 de 2000.

Logrando concluir que, toda evidencia digital debe obedecer con los criterios de autenticidad, confiabilidad y suficiencia y debe acatar la normatividad del sistema jurídico colombiano. Entendiendo que no procederá ninguna prueba digital sin que cumpla con los requisitos normativos.

Palabras clave: Delitos informáticos, prueba electrónica, Legaltech, digitalización de la justicia, prueba digital.

Keywords: Computer crimes, electronic evidence, Legaltech, digitization of justice, digital evidence.

Abstract

In this review article, the elements of validity of electronic evidence in the case of computer crimes are outlined, on the occasion of Law 1273 of 2009, which, entered to modify the criminal code, Law 599 of 2000. It which, was made from the methodological approach of the qualitative nature, framed in the dogmatic method and coming to the method of collecting information, consisting of the documentary review.

In addition, it questions the subjective reality through the research question, What are the current validity criteria of electronic evidence in cyber crimes? Which implied, establishing the conceptual approach of the general objective consisting of analyzing the current validity criteria of electronic evidence in cybercrimes. Which, is diluted in three specific objectives: i) Define the

objective elements that the electronic test must meet in contrast to the conventional test; ii) Determine the criminal legal scope of cyber crimes enshrined in the Colombian criminal code, Law 599 of 2000.

Achieving the conclusion that all digital evidence must comply with the criteria of authenticity, reliability and sufficiency and must comply with the regulations of the Colombian legal system. Understanding that no digital test will proceed without complying with the regulatory requirements.

Introducción

El avance tecnológico de la sociedad actual ha implicado que cada día se torne con mayor normalidad, el hecho de darle un espacio de mayor relevancia a la interacción digital, ejemplo de ello son las redes sociales, el internet de las cosas y la digitalización de la justicia. Sobre este avance, al cual el derecho no le es ajeno, la evidencia digital presta un rol importante. Por tanto, Toro (2019) la define como "toda información generada, almacenada o trasmitida a través de medios electrónicos que pueda ser utilizado" (p. 30).

Ésta evidencia digital, es posible encontrarla en medios de almacenamiento como celulares, computadores o tabletas. Además, de los medios de prueba que se pueden aportar a un proceso judicial como una foto, un video o un chat, como un mensaje de datos. De ahí que, si bien las disposiciones normativas de la evidencia digital analógicamente están dadas por el medio de prueba documental, ésta información digital ostenta una naturaleza distinta, al estar compuesta por bytes de información y éste cambio de paradigma, permite plantear diferentes modos de incorporarla, controvertirla y valorarla en el proceso penal colombiano.

En efecto, el estudio del Legaltech es la base fundamental para el conocimiento y regulación de la sociedad respecto de la informática e información digital. Por Legaltech, se entiende tecnología jurídica, término acuñado por Micha Bues, al describirlo en el uso de las tecnologías digitales modernas, basadas en la informática, para automatizar, simplificar y mejorar el proceso de definir, aplicar, acceder y gestionar la administración de justicia a través de la innovación. (Lösing, 2020)

Por otra parte, es importante definir el documento electrónico, como todo objeto mueble que mediante una ficción jurídica cumple el propósito representativo o declarativo, que una vez aportado a un proceso de carácter judicial con el propósito de formar una convicción en el juez, sobre la certeza de los hechos enunciados en la demanda o su contestación.

De modo que, un documento tradicional consta con la información y el soporte, mientras que un documento electrónico tiene un tercer elemento al contener un mensaje encriptado que debe ser traducido por una aplicación o un experto. Elemento que le permitió a Reyes (2013) afirmar:

> Los documentos electrónicos han sido aludidos como una especie dentro del género de la prueba digital. La cual, también podrá manifestarse como SMS[1] y los sistemas de video conferencia en streaming aplicados a las pruebas testimoniales. (p. 15)

[1] Short Message Service

Ahora bien, un documento almacenado digitalmente es todo aquel que tiene como soporte un almacenamiento electrónico mediante instrumentos electrónicos, por lo que, todo documento electrónico es un documento almacenado digitalmente, pero no todo documento almacenado electrónicamente es documento electrónico. (Arrabal, 2020)

En virtud de lo anterior, todo documento almacenado electrónicamente que se aporte al proceso judicial debe corresponder al contenido en el medio electrónico original, para que tenga valor jurídico probatorio, de acuerdo al artículo 8° de la Ley 527 de 1999, el cual podrá ser corroborado mediante la firma digital o firma electrónica. (1999)

Ésta ley reguló el comercio electrónico en Colombia, estableciendo aspectos esenciales y orgánicos para el uso general de los mensajes de datos en los procesos judiciales. En tal sentido, el Legislador señaló aquello que debe entenderse como mensaje de datos y señaló los requisitos para que tenga el mismo valor probatorio atribuido a un documento en papel, esto es, el principio de equivalencia funcional (Restrepo, 2014).

Esta ley definió el mensaje de datos como: "la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos o similares, como, el intercambio electrónico de datos, internet, el correo electrónico, el telegrama, el telefax, entre otros" (Congreso de Colombia, 1999)

Por otra parte, la Ley Estatutaria 270 de 1996 de la Administración de Justicia, reguló el ejercicio de la justicia en Colombia, facultando a los jueces y magistrados de todas las jurisdicciones, para valorar los medios de prueba que acarree consigo la innovación de la tecnología. (Congreso de Colombia, 1996)

El artículo 95 indica que la tecnología al servicio de la administración de justicia implica que el Consejo Superior de la Judicatura deba propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Acción enfocada principalmente a mejorar la práctica probatoria, la formación, conservación y reproducción de expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información.

Además, los juzgados podrían usar cualquier medio técnico, electrónico o digital, para el cumplimiento de sus funciones. Igualmente, 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. (Reyes, 2020)

De lo anterior, es evidente que con la tecnología la rama judicial ostentaría amplias facultades al servicio de la justicia, incluyendo deberes para su administración en aras de mejorar la práctica de pruebas digitales, mediante el desarrollo de planes por parte del Consejo Superior de la Judicatura para estimular la incorporación tecnológica en los procesos judiciales.

Al tratarse de una prueba digital, Restrepo (2014) afirma que:

> Los documentos digitales, deben tener unos requisitos objetivos que permitan establecer judicialmente su autenticidad. Tales características también han sido decantadas por la ley y la jurisprudencia. En ocasiones es posible pensar que el material presentado ha sido alterado, por ello el documento no ha sido bien recibido por algunos despachos. No obstante, la ley permite que quienes pretendan hacer

> valer éste tipo de prueba en juicio, lo hagan garantizando la confiabilidad de éste tipo de documento. (p. 58)

Ahora bien, si la prueba es objeto de impugnación por la falta de integridad del mensaje o la conversación se está impugnando que el mensaje ha sido manipulado, mediante la mutilación, sustitución o añadido de palabras o expresiones. Lo procedente sería una prueba pericial informática sobre el dispositivo electrónico de la parte proponente de la prueba y, si fuera posible, sobre el dispositivo de la otra parte interviniente en el proceso de comunicación. (Abel, 2019)

No obstante, justo es reconocer que bajo la óptica del poder punitivo y, mediante él, la regulación penal existente en la actualidad, permite concretar la comisión de diversos tipos penales autónomos a partir de hechos generadores en virtud de medios electrónicos que, por antonomasia podrían ser probados electrónicamente.

Así, el caso que en particular convoca éste ejercicio, se configura en los delitos cibernéticos, puesto que como se comentó anteriormente, el cambio del paradigma en torno a la tecnología, implica también una mutación de los móviles que usan los delincuentes para consumar su acto delictual, generando también, una evolución por parte del ente persecutor de la acción penal, al renovarse las formas y estrategias para que la policía judicial, los forenses informáticos y, el investigador de la defensa recopilen los elementos de prueba digitales y; puedan incorporar y practicar en juicio oral tales medios de convicción. (Reyes, 2020)

Dicho lo anterior, se parte de cuestionar la realidad subjetiva a través de la pregunta relativa a ¿Cuáles son los criterios de validez vigentes de la prueba electrónica en los delitos cibernéticos?

Para resolver la interrogante, fue necesario establecer el abordaje conceptual del objetivo general consistente en analizar los criterios de validez vigentes de la prueba electrónica y la prueba convencional en los delitos cibernéticos, implementados por la Ley 1273 de 2009. El cual, se diluye en dos objetivos específicos: i) Definir los elementos objetivos que debe cumplir la prueba electrónica a diferencia de la prueba convencional; ii) Determinar el ámbito jurídico penal de los delitos cibernéticos consagrados en el código penal colombiano, Ley 599 de 2000.

Además, está enmarcado en el plano metodológico en la naturaleza cualitativa, la cual está concebida bajo un enfoque de investigación dogmático-jurídico, en tanto, se instituye como un estudio normativo que describe analiza, interpreta y aplica normas jurídicas. Para tal fin, conoce y estudia las normas jurídicas, elabora conceptos y métodos para construir instituciones y un ordenamiento dinámico, ayuda a la producción y creación de otras nuevas normas, las interpreta y aplica, contribuye a regular con ellas comportamientos humanos y a resolver conflictos de efectividad (Díaz, 1998)

En ese orden de ideas, como se sabe, las normas jurídicas pueden proceder formalmente de la legislación (normas jurídicas legislativas), la jurisprudencia (normas jurídicas jurisprudenciales), la costumbre (normas jurídicas consuetudinarias), la doctrina (normas jurídicas doctrinarias), los negocios jurídicos (normas jurídicas negóciales), y los principios generales del derecho (normas jurídicas princípiales).

Además, esta investigación tiene la fiel pretensión de ir más allá de la mera descripción de la prueba electrónica, para centrarse más en los elementos objetivos que se deben tener en

cuenta en los criterios de validez vigentes de la prueba electrónica en los delitos cibernéticos. Por ello, la recolección de la información será a partir de la revisión documental.

En tal sentido, Para McDonald & Tipton, la investigación documental es:

Una herramienta de investigación dentro de las disciplinas sociológicas, y se han venido desarrollando históricamente, este tipo se basa en el estudio de la documentación entendida como la amplia gama de registro y símbolos, así como cualquier material y datos disponibles en las bases de datos (2016, p. 216)

Así, la estrategia de la investigación documental implicó un esfuerzo por identificar un patrón subyacente tras una serie de apariencias, visiones, percepciones, y comprensiones sobre un evento o situación que se analiza. La investigación documental se eligió, ya que, la construcción del conocimiento desde las fuentes es una forma de velar por la tradición del pensamiento original y desde esa perspectiva, traerlo al presente, con una lectura hermenéutica que favorezca la discusión al hacer nuevos aportes al desarrollo jurídico colombiano con propuestas que pueden ser cuestionadas permanentemente pero que siempre se orientarán a alcanzar nuevos desarrollos. (Artheta, 2015)

Por consiguiente, en este tipo de investigaciones se estudian a detalle las reglas jurídicas jurisprudenciales procedentes de estas fuentes formales. En el caso sub examine se estudiarán normas jurídicas jurisprudenciales emanadas por la Corte Constitucional y la Corte Suprema de Justicia, Sala penal, lo que permitirá resolver la pregunta de investigación. (Artheta, 2015)

Igualmente, el método es hermenéutico, porque, se da a partir del ejercicio interpretativo intencional y contextual se enmarca en el paradigma comprensivo. Algo bastante importante sobre este método lo expuso Habermas (2015) cuando dijo “con la reflexión hermenéutica, quien está ya siempre arrojado a un lenguaje, toma conciencia de sus peculiares libertades y dependencias respecto del lenguaje” (p. 31).

Esto, no significa repensar y reinterpretar más allá de la exegesis de la lectura de la norma y de las sentencias, sino, una interpretación más axiológica y deontológica para una mejor aplicación de los preceptos sustanciales de la prueba electrónica por parte de la judicatura.

Tal como lo indica Valencia Zea (2003) cuando expresa que, tiene como punto principal el concepto del sistema, que es un conjunto de elementos interrelacionados con un objetivo común, en este caso, el ordenamiento jurídico interno, que se ve nutrido por el derecho internacional y las reglas jurisprudenciales emitidas por los altos tribunales, Corte Constitucional y la Corte Suprema de Justicia, Sala Penal.

Ahora bien, en relación al marco jurídico, se enuncia a continuación, los componentes normativos que recogen la legislación relativa al tema de la prueba digital y el proceso penal en Colombia que, integrado con los antecedentes jurídicos anteriormente mencionados, constituyen los elementos objetivos para desarrollar el tema denominado “Ámbito de Validez de la Prueba Electrónica en los Delitos Informáticos”.

Norma	**Objeto**
Constitución Política de Colombia de 1991 (Asamblea Nacional Constituyente, 1991)	Clausula general del Estado Social de derecho, debido proceso, supremacía constitucional jerárquica y bloque de constitucionalidad

Ley 599 de 2000, Código Penal	Delitos cibernéticos
Ley 906 de 2004, Código de Procedimiento Penal	El régimen probatorio con reglas de requisito intrínseco y extrínseco, como lo es, la conducencia, pertinacia, utilidad o cláusula de exclusión
Ley 1273 de 2009, por medio de la cual se modifica el Código Penal. (Congreso de la República, 209)	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 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" (Congreso de Colombia, 1999)	Define el concepto de mensaje de datos
Ley 270 de 1996. (Congreso de Colombia, 1996)	Regula la administración de justicia y establece el plan de digitalización de la misma.
Ley 1564 de 2012, mediante la cual se expide el Código General del Proceso	Clausula residual de la reglamentación de las pruebas, cuando no está regulado especialmente

Fuente: Elaboración propia 2020

Resultados

Capítulo 1: los elementos objetivos de la prueba electrónica a diferencia de la prueba convencional

En el presente apartado, se abordan los elementos objetivos que se deben verificar en la prueba electrónica y en la convencional, con el fin de demostrar que, pese al cumplimiento del mismo fin dentro del proceso, las primeras, pueden tornarse frágiles o volátiles de no recopilarse y custodiarse de la manera adecuada.

Es así, como la prueba convencional debe cumplir unos requisitos intrínsecos que son llamados elementos objetivos, estos son, la conducencia, la pertinencia y la utilidad. Ello implica que, la pertinencia se refiera a que el medio de prueba, debe estar relacionado con el tema de prueba, qué a su vez, tiene como fin demostrar un hecho que se esté debatiendo en el proceso. (Bernal & Montealegre, 2013)

Por su parte, la conducencia apunta a la aptitud e idoneidad legal de una prueba para acreditar un hecho, por ejemplo, será el registro civil la prueba documental idónea para demostrar el estado civil; por último, la utilidad, se perfecciona cuando resulta provechoso para el proceso (Ayazo, 2008).

Sobre el requisito anterior, es importante aclarar dos aspectos, el primero, es que no se analiza la utilidad de la prueba desde la óptica del beneficio para las partes, sino, para el proceso; y el segundo, la ley presume algunos hechos como ciertos. Por ende, cualquier prueba que intente acreditarlos ese sería inútil. (Toscano, 2019)

Si la prueba convencional no reúne esos tres requisitos, el artículo 164 del Código General del proceso reza “el juez rechazará, mediante providencia motivadas pruebas ilícitas, las notoriamente impertinentes, las inconducentes y las manifiestamente superfluas o inútiles”. (Congreso de Colombia, 2012)

Por otra parte, para analizar los requisitos que deben cumplir las pruebas electrónicas, es menester precisas que dentro de un proceso la valoración de la prueba por parte del juez o tribunal, tiene como propósito generar un alto grado de convicción sobre un hecho determinado, el cual es relevante para proferir una decisión. (Rincón, 2008)

Por lo que, actualmente, varios medios probatorios digitales han cambiado desde lo jurídico hasta el punto que, el documento digital, goza de aceptación como medio probatorio, el cual, no se puede ignorar, en virtud, de la automatización y uso masivo de aparatos electrónicos (Morales, 2016).

No obstante, se deben cumplir una serie de procedimientos y características imperativas, para alcanzar el valor probatorio de los soportes informáticos que deben tener como requisito su reproducción en forma de texto, de sonido, de imagen y los mismos instrumentos de almacenamiento, de reproducción y generación de cálculos matemáticos y contables (Bielli, 2018).

Una de las características imprescindible debe ser la de asegurar su autenticidad y autoría, que pueden ser validados por un perito experto en seguridad informática, en este sentido expusieron Sentis & Liebman (1980) que:

> Quien promueva la verificación de un hecho, deberá proponer los medios de prueba disponibles. Ello implica que las pruebas sean admitidas, pero revisten una importancia particular los escritos de comparación, que el interesado deberá producir o, si no está en su posesión, deberá indicarlo. De modo que, el juez tropos oportunamente dispondrá la custodia del documento, establecerá el término para el depósito de los escritos de comparación, nombrará un perito para el examen grafológico y proveerá la admisión de las otras pruebas. Una vez determinados los documentos que deben ser comparados, es tarea del juez admitir todos aquellos que las partes consideren provenientes de la persona que aparece como autor del documento; o, en defecto de acuerdo, aquellos declarados como ciertos por reconocimiento o por sentencia (Sentis, 1980, p. 335).

Lo anterior, en razón a que, las pruebas digitales son altamente manipulables a causa de las posibilidades que ofrecen los mensajes de datos y las aplicaciones de donde se generan. En tal sentido, la Corte Constitucional, se refirió al contenido del mensaje de datos en la sentencia del 8 de junio de 2000, con ponencia del Magistrado Fabio Morón Díaz, de la siguiente manera:

La noción de mensaje comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación, bajo la configuración de los progresos técnicos que tengan

contenido jurídico. En la definición de mensajes de datos, hace referencia a los medios similares, con la finalidad de dejar abierto a todos los avances tecnológicos que se generen con el tiempo. (Corte Constitucional, 2000)

Así las cosas, el concepto de datos es polimorfo y abarca varios ámbitos entre esos la transacción electrónica del e-comerce, que puede ser consultada posteriormente y que puede ser o no alterada, cuyo soporte puede ser físico o digital, que para ser utilizada se requiere de la utilización de un medio electrónico y puede tener incidencia real y directa sobre la voluntad. (Arrabal, 2020)

Sin embargo, la ley colombiana no niega la eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original, allí debe entrar a evaluar la confiabilidad en la forma en que se haya generado, archivado, comunicado y conservado a fin de garantizar su autenticidad e integridad. (Contreras, 2015)

Las características esenciales que debe tener el mensaje de datos para fungir como evidencia digital son según Rincón (2015):

Primero, debe ser una prueba de la existencia y naturaleza de la manifestación de la voluntad de las partes de obligarse, por lo que debe ser expresa, clara, exigible o de fácil inferencia. Además, debe ser un documento legible que podrá ser presentado ante entidades públicas o despachos judiciales. Igualmente, debe admitir el almacenamiento e inalterabilidad en el tiempo.

Acto seguido, deberá facilitar la revisión y auditoría para fines contables, reglamentarios e impositivos. Finalmente, debe afirmar derechos y obligaciones jurídicas entre los intervinientes, cuyo acceso debe ser permanente para su posterior consulta.

Por otro lado, los mensajes de datos salvaguardan la integridad de la información, gracias a los sistemas de protección como son: la criptografía, firmas digitales, huellas digitales y las empresas que certifican la protección de la información en diversas etapas de la transacción, dentro del marco de la autonomía. Adicionalmente, cuando el contenido de un mensaje de datos sea completo y esté alterado, pero exista algún anexo inserto, este no afectará su originalidad, asimilable como el sobre utilizado para enviar ese documento “original” (2008)

Además, la evidencia digital debe cumplir el requisito de la confiabilidad, es decir, se entiende como confiable la cuando se emana de fuentes creíbles y verificables. Es decir, la prueba digital es confiable siempre y cuando el sistema que la haya generado no haya sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba. (Velasco, 2008)

Es preciso acotar que, el valor probatorio de la prueba digital, debe además de garantizar lo expuesto, reunir los mismos requisitos que se refieren a la esencia instrumentales probatorias propias de todo acto o contrato, como: ser un instrumento público o privado, reconocido por el ordenamiento jurídico y reunir los requisitos de eficiencia que establecen los códigos de procedimiento para que sean creíbles y ostentan valor probatorio en juicio (2008)

Otra de las características, es la suficiencia, esta se refiere a la presencia de toda evidencia necesaria para adelantar el caso (Echeverry, 2017), algo similar a la aptitud e idoneidad de la que se habla en las pruebas convencionales.

El requisito de confiabilidad y suficiencia se complementa, ya que, una prueba es suficiente, si ésta es completa y para que sea completa, se requieren instrumentos de integridad, sincronización y centralización que admitan percibir una imagen completa de la situación objeto de análisis.

Se reitera que la prueba digital tendrá el valor probatorio que el juez en su sana crítica le otorgue y se deberá tener en cuenta la confiabilidad en tres aspectos, estos son: la forma que se generó, la forma como se ha conservado y la forma como se identifique el iniciador (2015).

Capítulo 2: ámbito jurídico de los delitos cibernéticos consagrados en el código penal colombiano, Ley 599 de 2000

En el presente apartado, se enuncian los elementos jurídicos de los delitos cibernéticos consagrados en la Ley 599 de 2000, la cual, mediante la Ley 1273 de 2009, la cual modificó el Código Penal. Sin embargo, lo importante de dicha ley es que creó en el ordenamiento jurídico colombiano el bien jurídicamente tutelado cuyo nombre es el de la protección de la información y de los datos, es decir que se implementaron los delitos informáticos.

Esta ley se construyó para dar herramientas a la política criminal para afrontar los retos riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos, procurando la protección de los datos personales y los bienes jurídicos titulados de la confidencialidad, integridad de los datos y sistemas informáticos.

Es menester considerar lo previsto en la ley 1273 de 2009, que busco definir los tipos penales, las consideraciones, agravantes y atenuantes en conexión con los principios de necesidad, proporcionalidad y razonabilidad de las penas descritas.

La descripción típica del artículo 269I y siguientes del Código Penal, adicionado por la Ley 1273 de 2009, extrae la intención del legislador de crear tipos autónomos y específicos de los delitos ya extenientes, los cuales cumplen condiciones legales y jurisprudenciales a los verbos rectores contemplados en el delito de hurto por medios informáticos y semejantes es una modalidad del injusto de hurto calificado.

La ampliación del delito de hurto a modalidades informáticas o cibernéticas, tiene como fundamento los nuevos comportamientos y preocupaciones que se generan en la sociedad, en donde ya no solo se concibe la comisión del delito, como la sustracción de un bien, sino que la evolución del internet, permite desarrollar el delito mediante medios electrónicos y sin la necesidad del uso de la violencia.

Con la modificación normativa de la ley 599 de 2000, mediante la Ley 1273 de 2009, se incluyeron delitos contra el Acceso abusivo a un sistema informático (art 269 A), Obstaculización ilegítima de sistema informático o red de telecomunicación (art 269 B), Interceptación de datos informáticos (art 269 C), Daño Informático (art 269 D), Uso de software malicioso (269 E), Violación de datos personales (art 269 F), Suplantación de sitios web para capturar datos personales (art 269 G), Circunstancias de agravación punitiva (art 269 H), Hurto por medios informáticos y semejantes (art 269 I), Transferencia no consentida de activos (art 269J), y se Adiciónese al artículo 58 del Código Penal con un numeral 17; Adiciónese al artículo 37 # del Código de Procedimiento Penal # con un numeral 6.

La pretende resolver la atipicidad relativa a aquellas conductas asociada a la acción delictiva que de los sistemas de datos e información que vulneran la intimidad y confidencialidad de las personas mediante sistema de datos, endureciendo las penas de los tipos penales del hurto calificado.

La legitimidad del documento electrónico, el dato y la información en nuestra legislación, permite que el bien jurídico tutelado vulnerado, se asocie al de delito “electrónico” debe haber dos presupuestos básicos, uno es que esté tipificada en la Ley y el segundo que mediante sentencia condenatoria se haya demostrado la existencia de una conducta típica, antijurídica y culpable; presupuestos que se traduce en una atipicidad de una conducta socialmente reprochable.

Precisamente los bienes jurídicos titulado contemplado en la ley 1237 de 2009, permite determinar la autoría, titularidad, verbo rector y sanción cuando se ilustra en la siguiente tabla:

Bien jurídico tutelado: de la protección de la información y de los datos	
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 269 B:	*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 269 C:	*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 269 D:	*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 269 E.	: *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 269 F:	*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.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
Artículo 269 H:	*Circunstancias de 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: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.
Artículo 269 I:	*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 269 J:	*Transferencia no consentida de activos.* El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 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 2º Adiciónese al artículo 58 del Código Penal con un numeral 17, así:	***Artículo 58 Circunstancias de mayor punibilidad.*** Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: 17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.
Artículo 3º Adiciónese al artículo37 del Código de procedimiento Penal con un numeral 6, así:	***Artículo 37 De los Jueces Municipales.*** Los jueces penales municipales conocen: 6. De los delitos contenidos en el título VII Bis.

Fuente: Elaboración propia.

La denominación y alcance del bien jurídico tutelado a proteger la violación a la disponibilidad de datos informáticos y las circunstancias de agravación punitiva como la instalación un programa de ordenador o dispositivo que atente contra la confidencialidad o integridad de los datos informáticos almacenados en el sistema informático, que los datos informáticos almacenados en el sistema informático pertenezcan a una entidad que cumpla funciones públicas, que los datos informáticos almacenados en el sistema informático pertenezcan al sector financiero, que la acción se realizare por una persona con una relación contractual con el propietario de los datos, que la persona obtuviere provecho para sí o para un tercero y cuando se den a conocer a terceros los datos informáticos así obtenidos o se procese, recolecte o circule los datos personales o los datos de autorización o autenticación del sistema informático.

Conclusiones

Toda evidencia digital debe obedecer con los criterios de autenticidad, confiabilidad y suficiencia y debe acatar la normatividad del sistema jurídico colombiano. Entendiendo que no procederá ninguna prueba digital sin que cumpla con los requisitos normativos.

La prueba cuando esta programada en el sellado de tiempo o código hash, requiere que la cadena de custodia este en contacto directo con los elementos materiales probatorios, grabando dicha cadena en la conexidad con el hash

Por otra parte, en relación a la presunción de inocencia, no es posible que se simplifique la individualización del sujeto a la virtualidad de la dirección electrónica IP, del presumir que quien usa la rede social es el titular, pruesto que ello constituye una reducción en los elementos constitucionales de protección en relación al objeto de la prueba y su práctica en la era digital.

Conductas como el espionaje informático, el acceso ilegítimo a sistemas informáticos y falsedad informática no están incluidos en la Ley 1273, conductas descritas en los tipos penales que también poseían gran importancia como forma de protección de los datos personales, en sus características de amplitud, titularidad, autoría, integridad, disponibilidad, seguridad, transmisión, confidencialidad e intimidad

El hurto por medios informáticos, este es un tipo penal que rompe con todo lo ya mencionado en las exposiciones de motivos en razón a que los tipos penales debían ser autónomos puesto que la idea era la tipificación de nuevas conductas y la construcción de un bien jurídico tutelado exclusivo para estas conductas

Referencias

Abel, X. (2019). la impugnación de la Prueba tecnologica. En Agudelo, Pabón, Toro, Bustamante, & Vargas, *Teoría y Práctica* (págs. 559-595). Medellín: Universidad de Medellín.

Arrabal, P. (2020). La Tecnología y el derecho procesal. En D. Ramirez, *Justicia digital: un analisis internacional en época de crisis* (págs. 570-615). Medellín: Universidad de Salamanca.

Artheta, M. (2015). *La Hermenéutica Crítica de Habermas: una profundización de la Hermenéutica Gadameriana .* Valencia: Revista Internacional de Filosofia.

Asamblea Nacional Constituyente. (1991). *Constitución Política de Colombia.* Bogotá: Gaceta Constitucional.

Ayazo, J. I. (2008). *Prueba Judicial: Análisis y Valoración.* Bogota D.C: Escuela Judicial Rodrigo Lara Bonilla.

Bernal, J., & Montealegre, E. (2013). *Fundamentos Constitucionales y Teoría General de Derecho Penal.* Bogotá: Universidad Externado.

Bielli, G. (2018). *Los mensajes de WhatsApp y su acreditación en el proceso civil.* Bogota: Universidad Externado.

Congreso de Colombia. (1996). *Ley 270 "Estatutaria De La Administración De Justicia".* Bogotá: Diario Oficial No. 42.745, de 15 de marzo de 1996. Recuperado el 20 de agosto de 2020, de Diario Oficial No. 42.745, de 15 de marzo de 1996

Congreso de Colombia. (1999). *Ley 527 "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".* Bogotá: Diario Oficial No. 43.673, de 21 de agosto de 1999. Recuperado el 20 de agosto de 2020, de http://secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html

Congreso de Colombia. (2012). *Ley 1564 "Por medio de la cual se expide el Código General del Proceso y se dictan otras disposiciones.".* Bogotá: Diario Oficial No. 48.489 de 12 de julio de 2012.

Congreso de la República. (209). *Ley 1273 "por medio de la cual se modifica el Código Penal, se crea un nuevo bienjurídico 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".* Bogotá: Diario Oficial.

Contreras, A. (22 de julio de 2015). *derecho informatico universidad externado*. Recuperado el 31 de octubre de 2020, de universidad externado: https://derinformatico.uexternado.edu.co/evidencias-digitales-y-su-valor-probatorio/

Corte Constitucional. (2000). *Sentencia de Constitucionalidad C-664 del 08 de junio, M.P.: Fabio Morón Díaz.* Bogotá: Gaceta de la Corte Constitucional.

Diaz, E. (1998). *Curso de Filosofía del Derecho.* Barcelona: Moira Helm.

Echeverry, J. (17 de 07 de 2017). ¿Cómo lograr que una evidencia digital tenga validez jurídica? *Adalid.com*, págs. 55-60. Recuperado el 02 de noviembre de 2020, de https://www.adalid.com/evidencias-digitales-validez-juridica/

Lösing, N. (2020). Justicia digital y legaltech en Alemania. En D. Ramirez, *Justicia Digital: analisis internacional en época de crisis* (págs. 2-37). medellín: fundación red para el estudio del proceso y la justicia.

McDonald, & Tipton. (2016). *The Spectrum Of Qualitative Research: the Use of Documentary Evidence.* Madrid, España: Moira Helm.

Morales, F. (2016). *validez de la prueba electronica, un estudio sobre la firma digital y electronica.* Bogotá: Universidad Católica de Colombia.

Restrepo, A. (2014). *El documento electronico como medio de prueba en el procedimiento laboral colombiano (trabajo de grado).* Cali: Universidad Javeriana.

Reyes, C. (2013). *La Prueba Electronica en materia civil.* Cucuta: Universidad Libre.

Reyes, J. (2020). El delito informático en Colombia: Insuficiencias regulativas. *Derecho Penal y Criminología, 28*(84), 101-118.

Rincón, E. (2008). *Aproximación jurídica a la firma digital y a los mensajes de datos.* Bogotá: Universidad Javeriana.

Rincón, E. (2015). *Derecho del Comercio Electrónico y de Internet (2ª ed.).* Bogotá: Universidad Javeriana.

Sentis, M., & Liebman, E. (1980). *Manual de derecho procesal civil.* Buenos aires: Ed. buenos aires.

Toro, N. (2019). *el mensaje de datos y la prueba electronica.* Bogotá: Leyer.

Toscano, F. (2019). *la prueba de oficio en el proceso civil colombiano.* Bogotá: Universidad Externado.

Valencia Z, A. (2003). *Guia Del Desarrollo De Iniciativas Con Enfoque Sistemico En El Derecho.* Bogotá: Innpulsa.

Velasco, A. (2008). *El derecho informatico y la gestión de la seguridad de la información.* Barranquilla: Universidad del Norte.