LA EVIDENCIA DIGITAL EN EL PROCEDIMIENTO PENAL EN COLOMBIA: ESTUDIO LEGAL Y SALVAGUARDAS PROCESALES EN EL SISTEMA DE ACUSACIÓN

Ahylen Valentina Ladino Bolaños

Mónica Lorena Cendales Leguizamón

Facultad de derecho

Universidad La Gran Colombia

Bogotá, D.C.

2026

La evidencia digital en el procedimiento penal en Colombia: estudio legal y salvaguardas procesales en el sistema de acusación

Ahylen Valentina Ladino Bolaños

Mónica Lorena Cendales Leguizamón

Trabajo de Grado presentado como requisito para optar al título de Abogado.

Víctor Manuel Caceres Tovar

Director

Facultad de derecho

Universidad La Gran Colombia

Bogotá, D.C.

2026

Dedicatoria

A Dios, a nuestros padres y alma mater.

TABLA DE CONTENIDO

Resumen

El presente trabajo analiza la regulación y valoración de la prueba digital en el proceso penal colombiano, identificando los principales retos que plantea frente al derecho a la defensa. Se parte de la conceptualización de la evidencia digital como todo medio probatorio en formato de mensaje de datos, abordando sus características de volatilidad, duplicabilidad, anonimato y posibilidad de alteración. Se estudia el marco normativo vigente, en especial la Ley 527 de 1999 sobre mensajes de datos y la Ley 906 de 2004, cuyo vacío regulatorio ha obligado a la jurisprudencia a suplir la ausencia de reglas específicas. En este sentido, se examinan sentencias de la Corte Suprema de Justicia y de la Corte Constitucional, que han establecido criterios para la admisibilidad, autenticidad e integridad de la prueba digital, así como precedentes internacionales relevantes como *Riley vs. California* y *Carpenter vs. Estados Unidos*. El análisis concluye que, aunque existe un reconocimiento legal de la prueba digital, persisten grandes desafíos: la ausencia de protocolos claros para su recolección y preservación, el riesgo de manipulación de información, la debilidad en la protección de los derechos fundamentales y la dificultad de la defensa para controvertir pruebas electrónicas. Finalmente, se resalta la necesidad de actualizar la normativa procesal penal colombiana, garantizando un equilibrio entre la eficacia de la evidencia digital y la salvaguarda del debido proceso y la intimidad de los procesados.

Palabras clave: evidencia digital, prueba electrónica, derecho a la defensa, jurisprudencia, debido proceso.

Abstract

This paper analyzes the regulation and assessment of digital evidence in Colombian criminal proceedings, identifying the main challenges it poses to the right to defense. It begins by conceptualizing digital evidence as any evidentiary medium in data message format, addressing its characteristics of volatility, duplication, anonymity, and the possibility of alteration. It studies the current regulatory framework, specifically Law 527 of 1999 on data messages and Law 906 of 2004, whose regulatory gap has forced jurisprudence to fill the gap in specific rules. In this regard, it examines rulings from the Supreme Court of Justice and the Constitutional Court that have established criteria for the admissibility, authenticity, and integrity of digital evidence, as well as relevant international precedents such as Riley v. California and Carpenter v. United States. The analysis concludes that, although digital evidence is legally recognized, significant challenges persist: the lack of clear protocols for its collection and preservation, the risk of information manipulation, the weakness in the protection of fundamental rights, and the difficulty for defense counsel in challenging electronic evidence. Finally, it highlights the need to update Colombian criminal procedural regulations, ensuring a balance between the effectiveness of digital evidence and the safeguarding of due process and the privacy of defendants.

Keywords: digital evidence, electronic evidence, right to defense, jurisprudence, due process.

Introducción

A pesar de la importancia de este tema se trata de un área que no goza de una regulación univoca dentro de la legislación colombiana. Por lo tanto, es necesario acudir a los principios básicos y elementales de la informática, así como a los principios básicos y elementales del derecho probatorio de ello se desprenden algunos debates, incluso en la forma en que debe denominarse, pues en algunos textos se habla de evidencia digital para señalar que no todo medio con vocación probatoria en materia digital se convierte en prueba. Es por eso que, en este trabajo se utiliza la palabra prueba de manera genérica entendiéndola como aquello que puede corroborar la existencia o no existencia de algo siendo este el sentido al que se refiere la presente investigación.

Dentro del discurso académico, la evidencia digital ha experimentado un auge conceptual significativo, propulsada por las metamorfosis tecnológicas que remodelaron la creación, el almacenamiento, y la evaluación de los elementos probatorios. En síntesis, la prueba digital se puede entender como cualquier dato o conjunto de datos originados, conservados o difundidos a través de plataformas electrónicas; estos datos poseen la facultad de validar un acontecimiento con pertinencia jurídica en el contexto de un procedimiento judicial (Bautista, Mosquera, Obando, & Ríos, 2021)

Sin embargo, la comprensión de la prueba digital exige trascender su dimensión meramente tecnológica, siendo necesario analizarla en función del rol que desempeña dentro del proceso. En esta línea, la literatura jurídica destaca que la noción de prueba se encuentra estrechamente vinculada con su aptitud para generar convicción en el juzgador,

con independencia del medio a través del cual se manifieste. En este sentido, como señala (Taruffo, 2012), la prueba constituye un instrumento epistemológico orientado a la reconstrucción de los hechos, característica que adquiere especial relevancia en el entorno digital, donde la percepción del contenido se encuentra mediada por instrumentos tecnológicos.

En lo que respecta a esta materia, autores como (Chaia R. , 2024) sostienen que la evidencia digital presenta cualidades intrínsecas que justifican su estudio autónomo como una categoría con características particulares, diferenciadas de los medios probatorios tradicionales. Entre dichas características se encuentran la rapidez de modificación, la facilidad de alteración y reproducción, así como su estrecha vinculación con los sistemas informáticos, aspecto fundamental para su comprensión, el cual incide directamente en su valoración dentro del procedimiento penal.

En Colombia, la ausencia de reglas claras y sistemáticas sobre la prueba digital en el Código de Procedimiento Penal ha propiciado la aplicación de criterios doctrinales y jurisprudenciales para determinar su admisión y validez probatoria. Aunque puede considerarse la prueba digital como un documento en atención a su función análoga, dicha equiparación resulta incompleta frente a los retos técnicos y jurídicos que plantea la evidencia electrónica. (Bautista, Mosquera, Obando, & Ríos, 2021)

Por ende, el análisis de la evidencia digital requiere de un marco teórico sólido que permita comprender sus fundamentos conceptuales, sus particularidades técnicas y su relación con los pilares del derecho probatorio, tales como la libertad probatoria, la sana crítica y el derecho de contradicción. Este entendimiento resulta esencial para desentrañar

los conflictos que surgen con la utilización de este tipo de prueba y para la salvaguarda de derechos fundamentales como el debido proceso, la intimidad y el derecho de defensa.

Los penalistas, y especialmente los procesalistas en materia penal, reservan el término prueba de manera estricta y exclusiva para aquel elemento que ha surtido todos los trámites necesarios y suficientes para ser apreciado por el juez. En este sentido, la doctrina procesal entiende por prueba aquel material que ha sido recolectado, descubierto, solicitado, decretado, practicado, valorado y finalmente apreciado por la autoridad judicial.

No obstante, en el presente trabajo la palabra prueba ha sido utilizada en un sentido genérico, pudiendo también referirse como evidencia o medio probatorio, con un énfasis particular en el "medio digital", que constituye el eje central de esta investigación. En este contexto, algunos autores emplean igualmente la expresión prueba electrónica o evidencia electrónica.

De manera particular, autores como el profesor Rubén Chaia, reconocido especialista en la materia, utilizan la denominación prueba digital y han desarrollado una obra titulada *La prueba digital*, publicada por la editorial Hammurabi en dos tomos. Para esta investigación, dicho autor se considera uno de los referentes contemporáneos que mayor esfuerzo ha dedicado al estudio de los problemas asociados a la prueba digital, la evidencia digital, la prueba electrónica y la evidencia electrónica. (Chaia, 2024)

Aunque el autor aplica su análisis a la legislación argentina, toma como base dos referentes del derecho norteamericano, lo que permite una aproximación cercana a su obra. Si bien algunos pasajes resultan aplicables de manera exclusiva al contexto argentino, se trata de un trabajo con vocación de universalización.

En el tercer capítulo de esta investigación se hará referencia a algunos de los precedentes que el profesor Chaia desarrolla en su texto, los cuales contribuirán de manera significativa al entendimiento de la evidencia digital.

Frente a la diferenciación entre evidencia digital y prueba electrónica, la doctrina ha desarrollado diversas clasificaciones según su relación con el hardware, el software, los sistemas intermedios o la red, lo que permite identificar múltiples aproximaciones conceptuales dentro de esta materia. Estas distinciones, si bien enriquecen el debate académico, introducen diferentes definiciones que facilitan la comprensión del fenómeno digital. No obstante, dado que el propósito de este trabajo es ofrecer una introducción general al tema y abordar de manera directa problemas concretos, se prescindirá de profundizar en dichas discusiones. En consecuencia, en esta investigación se utilizará el término "prueba digital" en sentido genérico, tal como se ha venido indicando, comprendiendo dentro de esta expresión tanto la prueba digital como la prueba electrónica de manera indistinta. Este enfoque deja por fuera debates terminológicos más especializados, los cuales resultan propios de contextos de mayor profundidad o de estudios en los que la nomenclatura constituye el problema central.

El presente trabajo iniciará con un concepto de identificación, orientado a determinar qué se entenderá como prueba digital dentro del marco de este "juego de lenguaje" que se establece entre el investigador y el lector a lo largo del desarrollo de la investigación. En segundo lugar, se abordarán las características de la prueba digital, partiendo de la premisa de que su configuración puede depender, en cierta medida, de la autoridad judicial que la valore o emita. Para el desarrollo de este apartado, el trabajo se apoyará en un documento de la Escuela Judicial Rodrigo Lara Bonilla, el cual responde a estándares internacionales y ha sido elaborado por el Doctor (Bautista, Mosquera, Obando,

& Rios, 2021), quien además funge como capacitador de dicha institución. Este referente resulta útil para ampliar, desde una perspectiva técnica, las expresiones utilizadas en torno a la prueba digital, razón por la cual se adopta la definición propuesta por la mencionada Escuela, considerándola un insumo suficiente para los fines de esta investigación.

Posteriormente, en el capítulo 2 se abordará, de manera crítica, la desregulación existente en materia de admisibilidad de este tipo de pruebas. En este sentido, se evidencia que el Código de Procedimiento Penal, pese a tener más de 20 años de vigencia, no contiene una regulación desarrollada sobre la prueba digital, limitándose en lo sustancial a la referencia del documento digital y, en algunos casos, al mensaje de datos, categorías que ya existían al momento de su expedición. Esto ocurre aun cuando el código ha sido objeto de múltiples modificaciones a lo largo del tiempo, por lo que se advierte una ausencia significativa de actualización normativa en este ámbito. Si bien puede entenderse esta situación como una forma de no adoptar una postura rígida, en la práctica ha sido la jurisprudencia la que ha permitido sortear las limitaciones del texto legal vigente, no obstante, una regulación más clara y sistemática resultaría de gran utilidad para el tratamiento de esta materia.

En el tercer capítulo se abordará la forma en que debe recopilarse o recogerse la prueba desde la denominada interfaz de usuario, expresión que no es más que una forma técnica de referirse a lo que comúnmente se conoce como pantallazo. Este concepto, aunque de uso cotidiano, permite enfatizar que no se trata de la captura del software en sí mismo, sino de la imagen que dicho software presenta al usuario. Por ello, resulta fundamental diferenciar ambos aspectos, en la medida en que lo que se registra es la representación visual de la información y no el contenido interno del sistema. En consecuencia, se planteará que un screenshot de WhatsApp no constituye, por sí solo,

prueba digital en sentido estricto. Así mismo, se precisará que el objeto de este análisis no está dirigido a los pantallazos obtenidos de WhatsApp o de cualquier otra aplicación, ya sea desde dispositivos móviles u otros equipos que permitan capturar la pantalla.

Lo anterior se explica en la medida en que el denominado pantallazo no es más que la forma en que una aplicación presenta al usuario la información que resulta visible y relevante para su interacción, en ese sentido, para que pudiera hablarse de prueba digital en sentido estricto, dicho pantallazo debería dar cuenta de todos los datos que se encuentran detrás de la imagen que se muestra, lo cual implicaría abandonar la propia lógica de la captura visual, pues ya no se trataría de una simple imagen, sino de la exposición del código o estructura de programación subyacente. De igual forma, el dispositivo móvil constituye una realidad que merece especial atención y que no ha sido suficientemente desarrollada en la doctrina, especialmente en lo relativo a la información que allí se almacena y a la forma en que esta debe ser recolectada. Para este propósito, los aportes del profesor Chaia, junto con los precedentes norteamericanos previamente mencionados, resultan de gran utilidad para el análisis de estas problemáticas.

Por último, en el cuarto capítulo se abordará la admisión y la valoración de la prueba digital en Colombia, para ello, se tomará como guía la Ley 527 de 1999 y los desarrollos jurisprudenciales de la Corte Suprema de Justicia, particularmente de su Sala Penal, así como lo dispuesto por la Corte Constitucional, los cuales serán objeto de análisis crítico. En este punto, en concordancia con el profesor Ulises Carnosa y el profesor Andrés Felipe Arango, se plantea que la Corte ha incurrido en interpretaciones discutibles al considerar, por ejemplo, que los denominados pantallazos de la interfaz de usuario, como el pantallazo de WhatsApp, pueden ser tratados como indicios. Esta postura, se sostiene,

responde a un modelo anterior y a una comprensión inadecuada del fenómeno de la prueba digital.

En las conclusiones se presentará el panorama planteado a partir de la pregunta problema: ¿cómo se regula y valora la prueba digital en el proceso penal colombiano, y cuáles son los desafíos jurídicos que esta plantea para el ejercicio del derecho de defensa?

Como metodología para el desarrollo del presente trabajo de investigación, este estudio se enmarca en un enfoque cualitativo. En este sentido, se busca examinar e interpretar el tratamiento jurídico de la evidencia digital en el proceso penal colombiano, a partir del análisis de la normatividad, la doctrina y la jurisprudencia, sin recurrir a métodos cuantitativos ni a la medición de variables. Este enfoque permite comprender problemáticas jurídicas complejas desde una perspectiva interpretativa, centrando el análisis en el contenido de las fuentes jurídicas y doctrinales (Hernández, Fernández, & Baptista, 2014)

Además, se trata de una investigación básica o teórica, cuyo propósito principal es ampliar el conocimiento sobre la evidencia digital y su incidencia en el derecho de defensa, sin buscar una aplicación directa en casos particulares. El estudio se fundamenta en la revisión y análisis de fuentes secundarias, tales como la normatividad, las decisiones judiciales y la doctrina especializada (Tamayo M. , 2003). De igual forma, la investigación se orienta hacia un enfoque exploratorio, en la medida en que aborda un problema que, aunque ha sido parcialmente desarrollado por la doctrina, aún presenta vacíos normativos e interpretativos en el contexto jurídico colombiano. En consecuencia, no se pretende alcanzar certezas absolutas, sino identificar tendencias, dificultades y aspectos relevantes relacionados con la admisión, verificación y valoración de la evidencia digital (Hernández, Fernández, & Baptista, 2014)

Dentro de este marco, la coherencia entre lo que se busca y lo hallado en la investigación se comprende a partir del análisis y la interpretación, en donde los resultados no se asumen como verdades absolutas, sino como aproximaciones debidamente sustentadas en el estudio riguroso de las fuentes consultadas. De esta manera, los hallazgos obtenidos se alinean con el propósito de explicar, evaluar y cuestionar el tratamiento otorgado a la evidencia digital en Colombia, en consonancia con el carácter exploratorio del estudio.

Objetivos

Objetivo General

Analizar el tratamiento normativo, jurisprudencial y práctico de la prueba digital en el proceso penal colombiano, identificando los principales desafíos para su admisibilidad, autenticidad y valoración.

Objetivos Específicos

1. Identificar la conceptualización y caracterización de la prueba digital y su forma de almacenamiento.
2. Examinar la legislación colombiana aplicable a la prueba digital en el proceso penal.
3. Estudiar la jurisprudencia relevante de la Corte Suprema de Justicia y la Corte Constitucional sobre la admisión y validez de la prueba digital.
4. Evaluar las tensiones entre la obtención de las pruebas digitales y el derecho al debido proceso, la intimidad, y el derecho a la defensa.

CAPÍTULO I:

PRUEBA DIGITAL DESDE SU CONCEPTO Y CARACTERÍSTICAS

Resulta necesario definir qué se entiende por evidencia digital y qué se concibe como prueba digital dentro del presente "juego de lenguaje" que se establece entre el investigador y el lector a lo largo del desarrollo de este trabajo académico. Esta precisión es indispensable, en la medida en que podría existir una divergencia entre el concepto técnico y la representación mental que el lector construye durante su lectura. En este sentido, el proceso comunicativo solo resulta eficaz cuando la imagen mental que el investigador pretende transmitir guarda una correspondencia razonable con la que el lector configura al interpretar el texto. Esta idea se enmarca en el proceso de comunicación descrito por Saussure (Bigot, 2010), según el cual el emisor, al comunicar un mensaje, busca que el receptor construya una representación similar a la idea que se pretende expresar.

Conviene señalar que, en algunos casos, el lenguaje académico puede emplearse de manera que no aporte claridad al contenido, dando lugar a exposiciones excesivamente complejas, intervenciones cargadas de citas o construcciones argumentativas que dificultan la comprensión del mensaje. En tales escenarios, el resultado suele ser que el contenido pierde precisión comunicativa, aun cuando pueda percibirse como erudito o técnicamente elaborado.

Esta precisión se realiza debido a que el presente trabajo persigue un propósito contrario, se busca utilizar un lenguaje instructivo, claro y orientado a la comprensión, que permita guiar al lector y contribuir a la resolución de dudas en torno a un tema actual y en constante evolución como la prueba digital, el cual se encuentra estrechamente vinculado con el desarrollo tecnológico. En este contexto, para el ejercicio del derecho resulta

indispensable mantenerse actualizado frente a estas transformaciones, en la medida en que inciden directamente en la práctica del litigio y en la actividad jurídica.

¿Qué es la evidencia digital? Para efectos de la presente investigación, esta se entenderá como sinónimo de prueba electrónica. Al respecto, la Escuela Judicial Rodrigo Lara Bonilla señala:

> Entiéndase por evidencia digital cualquier medio probatorio en formato de mensaje de datos que es almacenado o transmitido en formato digital de tal manera que tenga vocación a probar un acto, contrato o hecho que sea relevante en un juicio o proceso judicial. (Bautista, Mosquera, Obando, & Rios, 2021, pág. 19)

Lo que más interesa de esta definición para el contexto del presente trabajo es centrar la atención en que se está haciendo referencia a datos, es decir, a estructuras compuestas por unos y ceros y a códigos de programación. Aunque el usuario, al interactuar con las aplicaciones, perciba imágenes, letras u otros elementos visuales, ello obedece a la forma en que el fabricante del software diseña la interfaz de usuario, entendida como el medio a través del cual se presenta el sistema a quien lo utiliza, sin embargo, aquello que se observa a simple vista no corresponde al contenido interno del programa ni constituye, en sentido estricto, la evidencia digital. (IBM, 2025)

Detrás de aquello que el usuario observa, como se indicó anteriormente, existe una estructura compuesta por múltiples códigos organizados de manera sistemática, así como un lenguaje de programación mediante el cual se construye el funcionamiento del sistema. A su vez, diversos softwares permiten procesar y presentar esos datos de una forma comprensible para el usuario, y es en ese nivel donde puede ubicarse la evidencia digital.

En este sentido, aunque la evidencia digital se configura primariamente a partir de datos codificados en lenguaje binario (unos y ceros), para que pueda ser comprendida por personas no especializadas en ingeniería de sistemas, necesariamente debe ser representada a través de una interfaz de usuario que facilite su interpretación.

De esta forma, la interfaz de usuario y el software a través del cual se presenta el contenido se encuentran tan estrechamente vinculados que llegan a ser elementos prácticamente inescindibles del dato para su adecuada apreciación. De no ser así, sería necesario presentar al juez un conjunto de documentos conformados por unos y ceros, con el fin de evidenciar la existencia de las conversaciones, situación que resultaría incomprensible para el operador judicial.

Incluso el sistema más básico de presentación, como un bloc de notas, requiere necesariamente de un software para permitir la visualización de una conversación, usualmente representada en archivos de extensión .txt. En ese escenario, también existe un programa encargado de interpretar y mostrar la información.

En este punto, lo que este trabajo busca resaltar es que, si se hablara de lo digital en sentido estricto, este debería expresarse en lenguaje binario, es decir, en unos y ceros. Sin embargo, siempre será indispensable un software que decodifique dicha información y la represente mediante una interfaz de usuario. Algunas interfaces resultan más amigables o visualmente elaboradas que otras; por ejemplo, puede resultar más intuitivo observar una conversación en WhatsApp o mediante un pantallazo que en un procesador de texto o en un formato HTML. No obstante, en todos los casos existe un proceso de decodificación, interpretación o presentación del código que permite su comprensión por parte del usuario.

1.1.Fundamentación teórica de la prueba digital

La prueba digital, también conocida como evidencia electrónica, ha adquirido una relevancia significativa en el escenario jurídico contemporáneo debido al impacto masivo de las tecnologías de la información en la sociedad, lo cual ha repercutido directamente en la evolución de los procedimientos judiciales. En términos generales, puede entenderse como cualquier dato, o conjunto de datos, producido, almacenado o transmitido a través de medios electrónicos, susceptible de ser utilizado para acreditar un hecho con relevancia jurídica dentro de un proceso judicial (Bautista, Mosquera, Obando, & Ríos, 2021)

No obstante, para comprender adecuadamente la prueba digital no basta con atender únicamente su dimensión tecnológica, sino que resulta necesario analizarla desde su función dentro del derecho probatorio. La doctrina ha sostenido que la prueba no se define exclusivamente por su forma de presentación, sino por su capacidad de generar convicción en el juez. En este sentido, (Taruffo, 2012) afirma que la prueba constituye una herramienta de conocimiento orientada a la reconstrucción de los hechos, aspecto que adquiere especial relevancia en el entorno digital, donde la información requiere del uso de tecnologías para su acceso, interpretación y valoración.

En el mismo ámbito, la prueba digital presenta características particulares que exigen un análisis diferenciado en relación con los medios probatorios tradicionales. De acuerdo con (Chaia R. , 2024), este tipo de evidencia se distingue por su volatilidad, la facilidad con la que puede ser modificada, su capacidad de reproducción y su estrecha relación con los sistemas informáticos, factores que inciden directamente en su tratamiento jurídico y en los criterios utilizados para su valoración dentro del proceso penal.

Un debate académico relevante se centra en la naturaleza jurídica de la prueba digital. En Colombia, ante la ausencia de una regulación específica y sistemática en el Código de Procedimiento Penal, se ha acudido al principio de equivalencia funcional para asimilarla a la prueba documental. Sin embargo, como señala (Parra J. , 2019), dicha equiparación resulta insuficiente, en la medida en que la evidencia digital presenta características propias, tales como su naturaleza intangible, su dependencia tecnológica y la necesidad de herramientas especializadas para su comprensión.

Por consiguiente, una parte considerable de la doctrina contemporánea sostiene que la evidencia digital debe ser concebida como una categoría probatoria autónoma, dotada de rasgos propios y diferenciados. En esa medida, su regulación y valoración no deberían quedar limitadas por las estructuras tradicionales del derecho probatorio. Este escenario adquiere especial relevancia en el ordenamiento jurídico colombiano, donde la ausencia de una normativa específica ha llevado a que la jurisprudencia y la doctrina desempeñen un papel fundamental en la construcción de los criterios necesarios para su admisión, autenticidad e integridad.

Finalmente, el análisis de la prueba digital exige una aproximación teórica que permita comprender su relación con los principios del derecho probatorio, tales como la libertad probatoria, la sana crítica y el derecho de contradicción. Este enfoque resulta fundamental para examinar las tensiones que surgen al conjugar este tipo de evidencia con la protección de derechos fundamentales como el debido proceso, la intimidad y el derecho de defensa, aspectos que constituyen el eje central de la presente investigación.

1.2.Almacenamiento

Uno de los principales problemas de la evidencia digital, especialmente de aquella de naturaleza estrictamente digital, radica en el lugar donde se almacena, aspecto que en ocasiones suele pasar desapercibido o no recibe la relevancia probatoria que realmente posee, en términos generales, los datos pueden encontrarse en tres espacios principales: almacenamiento en la nube, dispositivos físicos o información que circula en la red.

En relación con los datos en la red, por ejemplo, si se pretende establecer si un computador se conectó o no a internet en un momento determinado, dicha información no necesariamente se encuentra en la nube ni en el dispositivo físico. En estos casos, puede verificarse a través de fuentes como la red wifi de un lugar específico, revisando el historial de accesos registrado. A partir de estos registros es posible determinar aspectos como el momento de ingreso, la forma de conexión y la duración de la misma.

En cuanto a los dispositivos físicos, en ellos puede encontrarse información que no fue destinada a ser almacenada en la nube y que, por tanto, se conserva exclusivamente en el propio equipo. Distinta es la situación cuando la información se encuentra en la nube, pues, aunque pueda accederse a ella desde un teléfono móvil u otro dispositivo electrónico, los datos no se hallan contenidos en dicho aparato, en estos casos, el dispositivo funciona únicamente como un medio de acceso a la información, que permanece almacenada en servidores externos.

En este punto se identifican tres problemas relevantes en materia probatoria: en primer lugar, la determinación de quién es el titular del dato; en segundo lugar, la identificación del titular de la fuente; y, en tercer lugar, el papel de los terceros interesados en el dato o en la fuente. A modo de ejemplo, si una persona A almacena fotografías en su

iCloud, el titular de dichos archivos sigue siendo A, aun cuando la información repose en la nube. No obstante, al analizar la titularidad de la fuente donde se aloja el dato, está ya no corresponde a la persona A, sino al propietario de la infraestructura tecnológica que permite su almacenamiento, en este caso, la empresa Apple.

La denominada “nube” no es más que una forma de representación que evidencia que los datos no se encuentran ubicados en un dispositivo físico específico ni en un único lugar determinado, sino distribuidos en infraestructuras remotas. Esto resulta especialmente relevante, en la medida en que plantea dificultades prácticas y jurídicas, particularmente en lo relacionado con el acceso a la información almacenada en servicios como iCloud, siguiendo el ejemplo previamente expuesto.

Ahora bien, surge la cuestión de a quién debe solicitarse autorización cuando lo que se pretende es acceder al titular de la fuente. Para ello resulta pertinente el Convenio de Budapest (Consejo de Europa, 2001), relativo a la Ciberdelincuencia, el cual establece ciertos protocolos e instrumentos de cooperación para la obtención de información en entornos digitales, no obstante, incluso con la existencia de estos mecanismos, debe tenerse en cuenta que las empresas privadas que administran este tipo de datos suelen tener una capacidad operativa y económica considerable, al punto de que, en muchas ocasiones, pueden llegar a ser incluso más influyentes o poderosas que el propio Estado requirente de la información.

En determinadas materias, la cooperación internacional suele ser más proactiva en la lucha contra ciertas formas de delincuencia, pues no es equivalente un escenario de trata de personas frente a un caso de estafa, lo cual incide directamente en el nivel de acceso a las bases de datos. En el trámite ordinario para la obtención de información contenida en bases de datos públicas o privadas, se requiere, por regla general, la intervención de un juez

de control de garantías, quien expide la orden correspondiente para que esta sea canalizada a través de la Cancillería. Posteriormente, dicha entidad la remite al Estado en el que se encuentra la información, para que sus autoridades competentes soliciten a la policía judicial correspondiente la gestión ante la empresa titular de la base de datos, como puede ser el caso de compañías como Apple.

En este contexto, se evidencia que el mecanismo de cooperación internacional implica múltiples etapas y actores intervinientes, lo que puede dificultar significativamente el acceso efectivo a la información. Asimismo, se presentan diversos inconvenientes prácticos, entre ellos el hecho de que, en muchos casos, la sede principal de estas empresas se ubica en un país distinto a aquel donde se encuentran los servidores que almacenan la información, lo que complejiza aún más el procedimiento de obtención de los datos.

1.3.Características de la prueba digital

De conformidad con la guía elaborada por (Bautista, Mosquera, Obando, & Rios, 2021) con apoyo de la Escuela Judicial Rodrigo Lara Bonilla, la evidencia digital presenta una serie de características particulares, en las que, en muchos casos, cada ventaja puede implicar simultáneamente una desventaja. Uno de sus principales rasgos es su alta volatilidad, al respecto, resulta pertinente acudir a una máxima de la criminalística clásica atribuida a Edmond Locard: “El tiempo que pasa es la verdad que huye” (Universidad de Alcala, 2020) esta idea resulta especialmente aplicable al ámbito de la evidencia digital, en la medida en que los datos pueden ser altamente volátiles, al punto de que, si no son recolectados en el momento oportuno y bajo las condiciones adecuadas, pueden perderse de forma definitiva.

1.3.1. Eliminable y volátil

La evidencia digital, además de su carácter volátil, es susceptible de ser eliminada, ya sea de manera voluntaria o involuntaria. A ello se suman factores externos o acciones que pueden generar afectaciones en el hardware donde se encontraba almacenada la información. En este contexto, existen diversos softwares de almacenamiento que contemplan una vida útil determinada, dentro de la cual se realizan procesos de borrado sistemático conforme avanza el tiempo (Ochoa, 2018), un ejemplo de ello se observa en los sistemas de videovigilancia, en los cuales la información capturada suele ser altamente voluminosa debido a la grabación continua durante las 24 horas del día. Por esta razón, la mayoría de estos sistemas almacenan los datos por un periodo limitado, tras el cual la información se sobrescribe o se elimina automáticamente. En consecuencia, una vez transcurrido dicho tiempo, resulta imposible acudir a la fuente original para recuperar el material, ya que este ha dejado de estar disponible en el sistema y, en muchos casos, no se encuentra respaldado en otro lugar.

Por ello, cuando en determinados casos exista evidencia digital, resulta aconsejable remitir inicialmente un memorial, oficio o comunicación formal en el que se solicite la preservación de los datos almacenados en un servidor, en dicho escrito debe indicarse la relevancia de la información para un proceso judicial específico, así como la necesidad de su conservación como medida de aseguramiento probatorio. Esta actuación permite garantizar la disponibilidad del material mientras se adelantan las solicitudes formales correspondientes, conforme a los protocolos procesales aplicables.

Lo anterior obedece a que, si la defensa espera a que el juez de control de garantías programe la audiencia de búsqueda selectiva en base de datos, y posteriormente se surte la autorización y se adelanta la diligencia correspondiente, existe un alto riesgo de que, para ese momento, la información ya no se encuentre disponible, este aspecto resulta especialmente relevante para la práctica forense cotidiana, en la medida en que, cuando una información es pertinente para el proceso, debe procurarse su preservación de manera oportuna, dado que el control y conservación de estos datos no depende de quien los solicita, sino de un tercero, se hace necesario dejar constancia expresa de la importancia de su conservación desde el primer momento.

1.3.2. Duplicable

Otra característica de la prueba digital es su capacidad de duplicación, en la medida en que un mismo dato puede reproducirse en un dato gemelo o copia idéntica desde el punto de vista técnico, este proceso suele explicarse por la doctrina como una copia forense o copia experta, mediante la cual se busca preservar la integridad de la información, garantizando que los datos reproducidos correspondan fielmente a los originales. Para ello, se recurre al uso de funciones de hash, que permiten generar una nueva cadena de verificación que facilita la comparación entre el original y su copia.

El código hash puede entenderse como una especie de huella digital del archivo, es decir, un identificador único que permite reconocer y diferenciar cada dato digital. En ese sentido, cualquier archivo, documento o imagen digital posee una huella que lo individualiza y lo hace técnicamente irrepetible. (Agencia Nacional de Defensa Juridica del Estado, 2022)

Este elemento resulta relevante al momento de acreditar ante el juez que la información aportada proviene efectivamente del archivo original y no ha sido alterada con posterioridad, ya que cualquier modificación en el contenido implicaría una variación en el código hash. Sin embargo, pese a su importancia técnica, debe precisarse que el hash no constituye un requisito esencial para la admisibilidad de la prueba digital.

1.3.3. Anónima y modificable

Esta constituye una de las características más exigentes tanto para el trabajo del perito forense como para el análisis del operador judicial al momento de verificar la autenticidad de la evidencia digital, la principal dificultad radica en que no siempre es posible establecer con certeza que la persona que figura como autora de un dato digital sea efectivamente quien lo generó, en la medida en que el anonimato es una condición ampliamente presente en la estructura de las redes informáticas.

Adicionalmente, la evidencia digital es alterable y modificable, dado que los sistemas y softwares son susceptibles de sufrir cambios, manipulaciones o incluso falsificaciones. En este contexto, se presentan múltiples mecanismos de fraude digital, como el uso de páginas falsas o técnicas de suplantación, entre ellas el phishing, mediante las cuales se induce a los usuarios a ingresar información personal en plataformas que simulan ser legítimas. Asimismo, son frecuentes las estrategias de ingeniería social, como mensajes recurrentes de supuestas promociones o beneficios para clientes, que buscan captar datos de manera engañosa.

Por ello, estas circunstancias constituyen una alerta permanente para jueces y operadores judiciales en el análisis de la evidencia digital, debido a los riesgos asociados a su autenticidad e integridad. (Bujosa, Bustamante, & Toro, 2021)

En este punto, no resulta adecuado llevar el análisis al extremo de exigir como único criterio de validez la existencia de un código hash o la intervención exclusiva de un ingeniero especializado para su acreditación. Una exigencia de esta naturaleza podría afectar el acceso a la justicia de muchas personas, en la medida en que no todos cuentan con los recursos económicos para acudir a peritos o especialistas en informática que realicen este tipo de validaciones técnicas. Además, ello implicaría la creación de una especie de tarifa legal probatoria que no está prevista en el ordenamiento jurídico y que, por el contrario, los sistemas procesales contemporáneos han procurado superar, privilegiando criterios de valoración más flexibles y acordes con la sana crítica judicial.

Todo el sistema basado en tarifas legales o en reglas rígidas de valoración probatoria responde a una lógica propia de modelos procesales del pasado, por ello, los códigos tradicionales, incluido el Código de Procedimiento Penal, han evolucionado hacia esquemas más flexibles orientados al principio de libertad probatoria. Esta transición trae consigo consecuencias relevantes en la forma en que se concibe y se presenta la prueba, especialmente en materia digital, donde la valoración no puede quedar sujeta a formalismos estrictos, sino que debe atender a criterios de razonabilidad, autenticidad y contexto dentro del proceso.

CAPÍTULO II:

NORMATIVIDAD SOBRE LA PRUEBA DIGITAL.

En Colombia se evidencia una desregulación de la prueba digital, en la medida en que, al acudir a los códigos de procedimiento no se encuentra una normativa exhaustiva en materia penal, área sobre la cual se centra el presente análisis. Esta ausencia normativa ha conducido a que la regulación de este tipo de evidencia se soporte, en gran medida, en procesos de asimilación, conocidos doctrinalmente como equivalentes funcionales, a partir de los cuales se determina la correspondencia de la prueba digital con categorías probatorias tradicionales, según su contexto de aplicación. En este marco se desarrolla la presente investigación, al no ser posible fundamentarse exclusivamente en disposiciones directas del Código de Procedimiento Penal. No obstante, debe reconocerse la existencia de una norma de especial relevancia, considerada en cierta medida visionaria, como lo es la Ley 527 de 1999, la cual continúa siendo el principal referente en materia de mensajes de datos y evidencia digital. Esta ley, aunque breve, resulta particularmente significativa para efectos del presente trabajo, en especial en lo relacionado con los artículos 10, 11, 12 y 13, los cuales constituyen el eje normativo de análisis en este apartado.

Adicionalmente, resulta llamativo que la Ley 906 de 2004 (Código de Procedimiento Penal), pese a haber sido expedida cinco años después de la Ley 527 de 1999, no haya incorporado de manera expresa sus desarrollos en materia de mensajes de datos y admisibilidad probatoria. Ello no implica necesariamente que el legislador de 2004 desconociera estas discusiones, pero sí evidencia que ya existía un marco normativo previo que abordaba estas cuestiones desde el punto de vista probatorio.

Entre 1999 y 2004 se produjo, además, un periodo de transformación tecnológica significativo, marcado por la expansión del internet y el surgimiento progresivo de diversas redes sociales. En ese contexto, se aprecia una ausencia relevante de regulación específica por parte del legislador colombiano, particularmente frente a fenómenos que ya comenzaban a consolidarse en la práctica. En consecuencia, puede afirmarse que la discusión normativa sobre la prueba digital no fue abordada con la suficiente profundidad en ese momento legislativo.

Lo primero que debe señalarse es que, conforme al artículo décimo de la Ley 527 de 1999, los mensajes de datos no pueden ser inadmitidos por el solo hecho de tener dicha naturaleza. Desde ese momento, el legislador colombiano dejó claro que la condición de mensaje de datos no constituye una razón suficiente para excluir su valor probatorio, lo que implica un reconocimiento expreso de su validez dentro del sistema jurídico.

Asimismo, la norma introduce un aspecto fundamental en materia de prueba digital: no se exige que la evidencia sea aportada en su forma original para su admisibilidad. En ese sentido, el legislador ya advertía que la evidencia digital puede ser incorporada al proceso sin necesidad de presentarse en su estado primario, lo cual resulta coherente con la naturaleza propia de este tipo de información, esto adquiere especial relevancia si se tiene en cuenta que, en la práctica, gran parte de la información digital no se conserva en un formato original fácilmente identificable o accesible, lo que haría inviable una exigencia estricta de este tipo dentro del proceso judicial.

Cuando se realiza un respaldo de una conversación de WhatsApp, ese backup constituye una reproducción del contenido original, pero no es idéntico en sentido estricto al archivo primario. Existen mecanismos técnicos que permiten verificar si ha existido o no intervención humana en la manipulación de los datos, con el fin de establecer si se trata de

una copia fiel del original; sin embargo, aún bajo estas verificaciones, seguirá tratándose de una reproducción, en este contexto, resulta relevante destacar que el artículo 10 de la Ley 527 de 1999 acierta al establecer que no puede rechazarse el valor probatorio de un mensaje de datos por el simple hecho de su naturaleza digital. Aunque la norma no emplea expresamente términos como “evidencia digital”, “prueba digital” o “prueba electrónica”, su alcance es claro al impedir que se niegue su eficacia, validez o fuerza probatoria dentro de cualquier actuación administrativa o judicial.

De esta manera, desde 1999 se supera el argumento según el cual la falta de presentación en formato original excluye la admisibilidad de la prueba, criterio que queda desvirtuado dentro del marco normativo vigente.

> se contemplan, respectivamente, la prohibición de restar valor probatorio a un mensaje electrónico por el solo hecho de no ser presentado en su forma original y se consagran medidas para garantizar la posibilidad de controvertir la copia de un documento, en este caso, la copia impresa de un mensaje de datos. (Corte Constitucional de Colombia, Sentencia C-604/16, 2016)

2.1. Fundamento constitucional de la prueba digital.

El análisis de la prueba digital en el proceso penal colombiano encuentra su fundamento en los preceptos consagrados en la Constitución Política, particularmente en las garantías asociadas al debido proceso. En este sentido, el artículo 29 constitucional establece que toda actuación judicial debe respetar la legalidad probatoria, garantizar el derecho de contradicción y ser valorada conforme a criterios racionales, principios

plenamente aplicables a los elementos de carácter digital (Constitución Política de Colombia, 1991, art. 29).

Bajo esta perspectiva, la incorporación, práctica y valoración de la evidencia digital exige que su obtención e inclusión dentro del proceso se ajusten estrictamente a dichas garantías, evitando cualquier afectación a los derechos de las partes. Al respecto, la Corte Constitucional ha reiterado que el debido proceso no se limita al cumplimiento formal de reglas procedimentales, sino que constituye una garantía sustancial de protección de los derechos fundamentales en la actuación judicial (Corte Constitucional, Sentencia C-591 de 2005). Asimismo, el artículo 15 de la Constitución reconoce el derecho a la intimidad, el cual adquiere una especial relevancia en el entorno digital, en la medida en que dispositivos y sistemas electrónicos suelen contener información personal y comunicaciones privadas. En consecuencia, el acceso a este tipo de datos exige un control judicial estricto y el cumplimiento de los principios de legalidad, necesidad y proporcionalidad, especialmente cuando se trata de información sensible (Constitución Política de Colombia, 1991, art. 15; Corte Constitucional, Sentencia C-336 de 2007).

En definitiva, la prueba digital debe ser analizada desde una perspectiva constitucional, en la que su valor probatorio se armonice con la protección de derechos fundamentales como la intimidad, el debido proceso y el derecho de defensa.

2.2. Conservación de la prueba digital.

> La preservación de la evidencia digital constituye un pilar fundamental en el proceso penal contemporáneo, en la medida en que de ella depende, en gran parte, la posibilidad de asegurar la autenticidad, integridad y fiabilidad de los elementos probatorios que se presentan ante el juez. A diferencia de las pruebas de naturaleza física, la evidencia digital se caracteriza por su intangibilidad, su facilidad de reproducción y su alta susceptibilidad a modificaciones sutiles que, en ocasiones, pueden no dejar rastro evidente. Estas particularidades exigen, por tanto, un tratamiento más riguroso y técnicas especializadas de conservación que permitan garantizar su valor probatorio (Chaia R. , 2024)

La adecuada conservación de la evidencia digital no se limita únicamente a su resguardo seguro, sino que requiere la implementación de mecanismos técnicos y jurídicos que garanticen su inmutabilidad desde el momento de su obtención hasta su valoración en sede judicial, de esta forma, la preservación se configura como un elemento esencial para su validez probatoria, en tanto cualquier alteración, pérdida o manejo inadecuado puede afectar de manera significativa su credibilidad y, en consecuencia, su eficacia dentro del proceso penal.

Respecto a la legislación colombiana, se evidencia la ausencia de una regulación clara y sistemática enfocada específicamente en la preservación de la prueba digital.

Sin embargo, la Ley 906 de 2004, mediante la cual se expidió el Código de Procedimiento Penal, incorpora disposiciones de carácter general aplicables a los distintos medios probatorios, las cuales resultan pertinentes al momento de analizar la evidencia digital. En particular, la cadena de custodia se erige como el principal mecanismo jurídico

de protección, orientado a salvaguardar la integridad y autenticidad de los elementos materiales probatorios a lo largo del proceso.

La cadena de custodia se entiende, por tanto, como el conjunto de procedimientos debidamente documentados que permiten establecer la trayectoria, control y manejo de un elemento material probatorio desde su hallazgo hasta su incorporación y valoración en juicio. Su finalidad es evitar cualquier alteración, sustitución o contaminación del elemento probatorio, garantizando así su confiabilidad dentro del proceso.

En el caso de la evidencia digital, este mecanismo adquiere un grado de complejidad mayor, en la medida en que no se limita a la preservación de un objeto físico, como un dispositivo electrónico, sino que se extiende a la protección de la integridad e inmutabilidad de los datos contenidos en él (Ley 906 de 2004).

Comprendiendo esta faceta, la preservación de la evidencia digital exige la adopción rigurosa de protocolos técnicos especializados, entre ellos la elaboración de copias forenses, entendidas como duplicados exactos del dato original que permiten conservar su integridad. A través de estas réplicas se trabaja sobre una reproducción del material probatorio, evitando la intervención directa sobre la fuente original, asimismo, el uso de funciones hash se presenta como un instrumento fundamental, en la medida en que permite generar un código único asociado a la información digital. De este modo, cualquier modificación, por mínima que sea, puede ser detectada mediante la comparación de los valores obtenidos antes y después de una eventual alteración (Chaia R. , 2024)

Paralelamente, un aspecto esencial en la custodia de la evidencia digital consiste en la documentación rigurosa de cada actuación realizada sobre el elemento probatorio. Esto implica el registro detallado de los accesos a la información, el momento en que se efectuaron, las circunstancias en que tuvieron lugar y el propósito de cada intervención.

Dicha trazabilidad resulta fundamental para garantizar la transparencia en la gestión de la prueba y permitir su posterior verificación dentro del proceso judicial.

En la práctica, la preservación de la evidencia digital presenta dificultades significativas, especialmente en relación con elementos como capturas de pantalla, chats, correos electrónicos y otros registros electrónicos. A pesar de su potencial valor probatorio, estos medios son altamente vulnerables a la manipulación, por ejemplo, una captura de pantalla puede ser alterada con relativa facilidad si no se cuentan con mecanismos idóneos para garantizar su autenticidad. En consecuencia, la forma en que se obtiene, documenta y resguarda la información resulta determinante, en la medida en que incide directamente en su fuerza probatoria.

Desde una perspectiva constitucional, la preservación de la prueba digital se encuentra estrechamente vinculada con el derecho al debido proceso consagrado en el artículo 29 de la Constitución Política de Colombia. Esta garantía implica que las partes puedan controvertir el material probatorio en condiciones de igualdad, lo cual solo es posible si la evidencia ha sido adecuadamente preservada y se mantiene incólume en su integridad (Constitución Política de Colombia, 1991, art. 29).

La correcta custodia de la evidencia digital guarda una relación directa con el derecho a la defensa, en la medida en que cualquier error en su manejo puede afectar la posibilidad de las partes de controvertir su veracidad o de aportar elementos probatorios en contrario. Al respecto, la Corte Constitucional ha reiterado que el debido proceso no se limita al cumplimiento de formalidades procesales, sino que constituye una garantía sustancial orientada a la protección efectiva de los derechos fundamentales durante el desarrollo del proceso judicial (Corte Constitucional, Sentencia C-591 de 2005).

Además, la retención de la prueba digital puede entrar en tensión con otros derechos fundamentales, como el derecho a la intimidad, especialmente cuando la información se encuentra en dispositivos que almacenan datos personales. En estos casos, la obtención y preservación de la evidencia deben sujetarse a los principios de legalidad, necesidad y proporcionalidad, con el fin de evitar afectaciones injustificadas a los derechos individuales.

En términos generales, la preservación de la evidencia digital trasciende el ámbito meramente técnico y se erige como un pilar del debido proceso, al cumplir una función de garantía dentro del sistema penal. Una adecuada gestión no solo fortalece la credibilidad de la evidencia, sino que también protege los derechos de las partes involucradas.

De igual manera, se advierte que la ausencia de una regulación específica sobre la conservación de la prueba digital en el ordenamiento jurídico colombiano pone de presente la necesidad de consolidar los criterios desarrollados por la doctrina y la jurisprudencia. En consecuencia, se hace necesario avanzar hacia la construcción de lineamientos más precisos que orienten la actuación de los operadores jurídicos, procurando un equilibrio adecuado entre la eficacia probatoria y la protección de los derechos fundamentales.

2.3.Libertad probatoria.

La valoración judicial de la evidencia digital dentro del proceso penal constituye una etapa fundamental de la actividad probatoria, en la medida en que a través de ella el juez determina el grado de fiabilidad y validez de los elementos aportados al proceso. En el caso de la evidencia digital, esta labor adquiere un nivel de complejidad adicional, debido a

las características propias de este tipo de material probatorio, entre las que se encuentran su naturaleza intangible, su facilidad de reproducción y su susceptibilidad a ser modificada.

En el sistema jurídico colombiano, la valoración probatoria se rige por el principio de la sana crítica, el cual exige al juez fundamentar sus decisiones en criterios de lógica, experiencia y conocimientos científicos, evitando apreciaciones arbitrarias o puramente subjetivas (Parra, 2019). Este principio resulta plenamente aplicable a la prueba digital, la cual no puede analizarse de manera aislada, sino en relación con el conjunto de elementos probatorios obrantes en el proceso.

En este marco, la doctrina ha señalado que la eficacia probatoria de la evidencia digital depende, en gran medida, de la garantía de su autenticidad e integridad.

Considerando la propuesta de (Chaia R. , 2024) la simple exhibición de un documento digital, mensaje o registro no resulta suficiente, en la medida en que se requiere acreditar que dicho contenido se mantiene inalterado y que representa fielmente los hechos que se pretenden demostrar, en consecuencia, la valoración de la evidencia digital exige un análisis cuidadoso que integre tanto una perspectiva jurídica como técnica, de manera complementaria.

La Corte Constitucional ha reiterado que la valoración probatoria debe ajustarse al derecho al debido proceso, lo que implica que las pruebas sean obtenidas de manera lícita y que se garantice a las partes la posibilidad de controvertirlas en condiciones de igualdad (Corte Constitucional, Sentencia C-591 de 2005). En relación con la evidencia digital, este aspecto adquiere especial relevancia, en la medida en que un manejo inadecuado puede generar desequilibrios procesales o afectar el ejercicio efectivo del derecho de defensa.

Desde una óptica operativa, la valoración de la evidencia digital debe considerar múltiples factores, entre ellos el proceso de obtención, los métodos empleados para su preservación, la existencia de una cadena de custodia y la posibilidad de verificar su autenticidad mediante herramientas técnicas idóneas.

En este sentido, elementos como capturas de pantalla o conversaciones de WhatsApp requieren un análisis especialmente cuidadoso, en la medida en que pueden ser objeto de alteraciones con relativa facilidad, lo que genera dudas sobre su origen y sobre la fidelidad de su contenido.

De igual manera, la evidencia digital no puede apreciarse únicamente desde su forma externa o su contenido inmediato; exige un examen más profundo que incorpore tanto aspectos técnicos como garantías procesales. En consecuencia, el juez debe asumir una postura crítica frente a este tipo de material probatorio, verificando su fiabilidad a través de medios objetivos y comprobables.

La ausencia de reglas específicas para la valoración de la evidencia digital en el sistema jurídico colombiano plantea desafíos significativos para la administración de justicia, en tanto obliga a los operadores judiciales a recurrir a la doctrina y la jurisprudencia como principales referentes interpretativos. En este contexto, resulta necesario fortalecer criterios que establezcan parámetros más precisos para su apreciación, evitando decisiones sustentadas en apreciaciones subjetivas o percepciones personales.

En definitiva, el análisis de la evidencia digital revela un proceso complejo que exige la articulación entre conocimientos jurídicos y técnicos. A su vez, demanda la observancia estricta de los principios constitucionales que estructuran el debido proceso. Aplicada de manera adecuada, esta valoración no solo contribuye a la eficacia probatoria en

el ámbito penal, sino que también garantiza la protección de los derechos fundamentales de las partes e incrementa la legitimidad de las decisiones judiciales.

2.4.Cadena de custodia

Frente al tema de la cadena de custodia, se presenta una problemática significativa, en la medida en que la formación inicial de muchos operadores jurídicos dentro del sistema penal ha contribuido a consolidar la idea de que esta se reduce exclusivamente al uso de una bolsa sellada, acompañada de un rótulo y una firma. Esta concepción ha llevado a confundir el procedimiento operativo de embalaje con la verdadera naturaleza jurídica y técnica de la cadena de custodia.

> El sistema de cadena de custodia es un proceso continuo y documentado aplicado a los EMP y EF, por parte de los servidores públicos y particulares que con ocasión a sus funciones deban garantizar su autenticidad y capacidad demostrativa, mientras que la autoridad competente ordena su disposición final. (Fiscalia General de la Nacion, 2018, pág. 11)

Se puede entender, entonces, que la cadena de custodia comprende cualquier mecanismo mediante el cual se pueda asegurar al juez que el elemento probatorio aportado corresponde efectivamente al mismo del que se ha venido haciendo referencia dentro del proceso.

En materia digital, esta garantía se refuerza mediante la acreditación del lugar y las condiciones en que el elemento fue almacenado durante el tiempo previo a su presentación en juicio, lo que permite sustentar su autenticidad e integridad.

> La cadena de custodia tiene como finalidad brindarle soporte veraz a la prueba digital ante el juez, en medio de lo que se conoce como el debido proceso. Por tal motivo deben establecerse los procedimientos indicados para garantizar la idoneidad de los métodos aplicados para la sustracción de la evidencia informática. Así se garantiza una base efectiva para el juzgamiento y la validez ante cualquier fuero judicial internacional. Para esto, es necesario que se eviten suplantaciones, modificaciones, alteraciones, adulteraciones o simplemente su destrucción (común en la evidencia digital, ya sea mediante borrado o denegación de servicio). Procedimiento controlado y supervisable, la cadena de custodia informático-forense se aplica a los indicios materiales o virtuales relacionados con un hecho delictivo o no, desde su localización hasta su Valoración por los encargados de administrar justicia. Este artículo lista los procedimientos en cada caso de recopilación de evidencia informática. (Arellano & Castañeda, 2012, pág. 1)

y, sobre todo, este aspecto resulta especialmente relevante, ya que cada vez que se manipula un elemento potencialmente constitutivo de prueba digital debe actuarse con extremo cuidado. En efecto, la simple acción de copiar y pegar un archivo y posteriormente presentarlo como prueba puede generar inconsistencias significativas en el análisis judicial. Por ejemplo, al revisar las propiedades del archivo en audiencia, pueden aparecer metadatos

como la fecha de creación o modificación correspondientes al momento en que fue copiado, lo cual puede afectar su credibilidad y autenticidad.

La actuación sobre este tipo de información exige cautela técnica y jurídica, evitando alteraciones que comprometan su valor probatorio, La cadena de custodia, en el contexto de la prueba digital, debe comprenderse más allá del esquema tradicional asociado al embalaje físico de los elementos, superando la visión meramente procedimental que históricamente se ha manejado.

2.5.Convención de Budapest

El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001 por el Consejo de Europa y vigente desde 2004, constituye el primer tratado internacional orientado a la prevención y persecución de los delitos informáticos y de aquellos cometidos mediante el uso de internet. Su relevancia radica en que establece estándares comunes en materia de derecho penal sustantivo, derecho procesal y cooperación internacional, con el propósito de asegurar una respuesta coordinada frente a los riesgos derivados del uso de las tecnologías de la información y la comunicación.

La expansión de internet durante la década de 1990 dio lugar a nuevas manifestaciones de criminalidad, entre ellas el acceso ilícito a sistemas informáticos, el robo de datos, el fraude electrónico y la distribución masiva de contenido ilegal. Estos fenómenos evidenciaron la necesidad de adaptar el derecho penal a realidades no previstas en los ordenamientos tradicionales. En este contexto, el Convenio de Budapest surge como respuesta a dicha problemática, con el objetivo de armonizar las legislaciones nacionales y

facilitar la cooperación transfronteriza en la investigación y sanción de este tipo de conductas delictivas.

Su principal objetivo es proporcionar un marco legal uniforme que permita tipificar conductas delictivas relacionadas con la informática y, al mismo tiempo, fortalecer los mecanismos de cooperación internacional. Así, se intenta superar las dificultades que supone la territorialidad del derecho penal frente a delitos cometidos en un entorno globalizado.

El Convenio se estructura en cuatro ejes centrales. En primer lugar, el derecho penal sustantivo, que establece una serie de conductas delictivas específicas que los Estados parte deben tipificar en sus legislaciones internas, entre ellas el acceso ilícito a sistemas informáticos, la interceptación ilegal de comunicaciones, la interferencia en datos y sistemas, y el uso indebido de dispositivos o programas diseñados para la intrusión. Asimismo, incluye delitos informáticos vinculados al contenido, como la pornografía infantil distribuida por medios digitales, así como conductas relacionadas con infracciones a los derechos de propiedad intelectual.

El Convenio introduce herramientas procesales novedosas para la investigación de delitos informáticos, como la conservación expedita de datos almacenados en redes, las facultades de registro y aseguramiento rápido de información digital y el acceso transfronterizo a datos bajo ciertas condiciones. Estas medidas buscan preservar la evidencia digital, la cual es particularmente volátil y susceptible de alteración o pérdida (Gonzalez J. , 2019). El Convenio establece un marco de cooperación internacional que contempla mecanismos de asistencia judicial entre los Estados parte, incluyendo la posibilidad de compartir información en tiempo real, la creación de canales de contacto

directo entre autoridades y la existencia de puntos de enlace permanentes disponibles 24/7 para la atención de solicitudes urgentes.

Por supuesto, el Convenio tiene en cuenta la protección internacional de los derechos humanos, al reconocer la necesidad de equilibrar la lucha contra la ciberdelincuencia con la salvaguarda de los derechos fundamentales. En este sentido, exige que todas las medidas adoptadas respeten la Convención Europea de Derechos Humanos, en particular el derecho a la privacidad, la libertad de expresión y las garantías del debido proceso.

Aunque el Convenio de Budapest fue promovido por el Consejo de Europa, su influencia se ha extendido a nivel global. Países latinoamericanos como Chile, Costa Rica, República Dominicana y Panamá lo han ratificado. Colombia aún no es parte formal del Convenio, pero ha incorporado varias de sus disposiciones mediante la Ley 1273 de 2009, la cual modificó el Código Penal para incluir los delitos informáticos. (Patiño, 2021)

La adhesión a este Convenio permitiría a Colombia fortalecer su marco normativo y, especialmente, mejorar la cooperación internacional frente a crímenes transnacionales como el phishing, el fraude electrónico, el ransomware y el ciberterrorismo.

CAPÍTULO III:

Jurisprudencia.

3.1.Jurisprudencia internacional

3.1.1. Caso Riley Vs California – privacidad vs seguridad

El 2 de agosto de 2009, David Riley, presunto miembro de la pandilla Lincoln Park, se encontraba estacionado en un barrio de San Diego junto con su novia y otros tres hombres. En ese momento, un integrante de una pandilla rival, el señor Webster, cruzó la intersección cercana, y los acompañantes de Riley le dispararon en varias ocasiones. Tras el choque del vehículo del señor Webster, los tres atacantes huyeron en el automóvil de Riley. Testigos del hecho señalaron que Riley pudo haber participado en el tiroteo, aunque no fue identificado de manera concluyente como uno de los autores. Al día siguiente, el vehículo de Riley fue hallado en una zona asociada a la pandilla Lincoln Park, parcialmente oculto.

Posteriormente, el 22 de agosto de 2009, Riley fue detenido por conducir con la matrícula vencida en un segundo vehículo, un Lexus. Durante la detención, el oficial de policía de San Diego verificó además que el conductor tenía la licencia suspendida. Conforme a la política del Departamento de Policía, el vehículo fue remolcado y confiscado con el fin de impedir que continuara circulando.

Además, la política exigía la realización de un inventario del vehículo, lo que en este caso condujo al hallazgo de dos armas de fuego que, mediante análisis balísticos, fueron posteriormente vinculadas con el tiroteo del señor Webster ocurrido el 2 de agosto. El agente Dunnigan desconocía esta información al momento de la detención de Riley.

A partir del descubrimiento de las armas y otros elementos asociados a actividades de pandillas durante el registro del vehículo, la policía procedió a la detención de Riley y, posteriormente, efectuó el registro de su teléfono celular sin orden judicial. Como resultado de dicha inspección, se obtuvo información que lo vinculaba con la pandilla Lincoln Park, incluyendo fotografías, contactos, mensajes de texto y videoclips.

Entre las fotografías obtenidas se incluía una imagen del vehículo Oldsmobile involucrado en el tiroteo del señor Webster. El demandante solicitó la exclusión de la evidencia obtenida del teléfono celular durante el juicio, sin embargo, el juez la admitió tanto en el primer juicio como en el nuevo juicio. Finalmente, Riley fue condenado por tres cargos, decisión que fue posteriormente confirmada por el Tribunal de Apelaciones de California.

El problema jurídico de este caso, y por el cual resulta relevante para esta ¡investigación académica, radica en si, en este contexto, ¿A la Corte Suprema de los Estados Unidos se le presenta la oportunidad de considerar si los teléfonos celulares deberían estar sujetos a registros sin orden judicial por parte de la policía?

Los argumentos a favor del demandante radican en que los teléfonos inteligentes contienen una cantidad de información personal tan amplia que no deberían ser objeto de registro por parte de la policía sin una orden judicial. Por ejemplo, la Asociación Americana de Bibliotecas sostiene que se perderían las protecciones constitucionales si la policía pudiera registrar el teléfono inteligente de cualquier persona arrestada sin orden previa, especialmente si se tiene en cuenta que más de la mitad de los adultos en Estados Unidos posee este tipo de dispositivos. (Riley vs California, 2014)

Los teléfonos inteligentes, argumenta la Asociación, revelan los pensamientos más privados del estadounidense promedio, en la medida en que contienen amplios registros de

los libros leídos, los sitios web visitados y las conversaciones sostenidas con amigos y familiares del propietario. La defensa sostuvo que, si la policía puede revisar la gran cantidad de datos almacenados en la mayoría de los teléfonos inteligentes al momento del arresto, estos serán utilizados para implementar técnicas de investigación más agresivas. En este sentido, los teléfonos inteligentes se han convertido en un repositorio moderno de información personal, que con frecuencia contiene datos íntimos y altamente sensibles de diversa índole.

Además, se sostiene que los teléfonos inteligentes son dispositivos tan sofisticados como las computadoras personales y, por tanto, deben ser tratados de manera equivalente, al constituir una verdadera ventana a la vida privada de su titular. En consecuencia, no resulta admisible que un objeto de tal nivel de intimidad y capacidad de almacenamiento sea confiscado y registrado en el marco de procedimientos policiales rutinarios que no exigen orden judicial.

El demandado, el Estado de California, sostiene que es necesario que los agentes de policía puedan confiscar los teléfonos celulares sin orden judicial, debido a que estos pueden representar una amenaza significativa para la seguridad de los oficiales. En este sentido, California advierte la posibilidad de que los dispositivos hayan sido manipulados para detonar a distancia o incluso explotar al ejecutarse una acción específica mientras permanecen en posesión del propietario.

Además, el Estado argumenta que los teléfonos celulares pueden ser utilizados por sus propietarios para solicitar asistencia, lo cual podría representar una amenaza potencialmente significativa tanto para los agentes como para el público. Igualmente, aunque el peticionario considera la sofisticación de los teléfonos inteligentes como una razón para evitar su registro sin orden judicial, el Estado advierte que estos dispositivos

pueden emplearse para rastrear la ubicación de sus usuarios, facilitando así la intervención de terceros que podrían frustrar las actuaciones de los agentes o asistir al propietario sin que este haya solicitado apoyo.

El examen del teléfono permitiría a los agentes determinar si ha sido utilizado como un instrumento que pueda comprometer la seguridad de los oficiales o del público. Además, el Estado sostiene que los teléfonos celulares pueden servir para ayudar a la policía a confirmar de manera rápida la identidad de sus propietarios, lo cual suele constituir una preocupación inmediata en el contexto de la detención. En este sentido, el Estado argumenta que dicha revisión resulta necesaria.

Por su parte, la defensa de Riley argumenta que, incluso si la revisión del contenido digital de un teléfono celular responde a un interés legítimo del Estado, dicho registro resulta irrazonable en la medida en que vulnera la privacidad personal en un grado sin precedentes. Riley enfatiza la sensibilidad de la información que puede almacenarse en un teléfono móvil y sostiene que estos dispositivos pueden entenderse como un almacén virtual o incluso como una extensión de la mente de su usuario.

En su opinión, si bien una persona arrestada puede verse privada del derecho a la privacidad respecto de su ropa y pertenencias físicas, ello no autoriza al Estado a realizar un registro indiscriminado de la información contenida en su teléfono celular. En este sentido, se sostiene que gran parte de la información que hoy almacenan los teléfonos móviles antes se encontraba resguardada en la intimidad del hogar. Riley argumenta que, dado que los dispositivos modernos concentran una cantidad de información mucho mayor que la que anteriormente podía transportarse, no resulta admisible permitir búsquedas ilimitadas en ese extenso registro digital.

Además, se argumenta que la información contenida en los teléfonos celulares involucra cuestiones relacionadas con la Primera Enmienda en materia de libertad de expresión y de asociación, en la medida en que la búsqueda e incautación de materiales de carácter expresivo, como listas de contactos y registros de llamadas, debe ser específica a fin de evitar la vulneración de estos derechos. Riley sostiene que no resulta razonable registrar las comunicaciones personales en el contexto de un arresto, ya que dicho registro expondría información protegida al escrutinio estatal sin la debida justificación que debería otorgar una orden judicial.

Frente a ese argumento, el Estado de California sostiene que los avances tecnológicos no justifican la adopción de reglas especiales para los teléfonos celulares en el contexto de registros incidentales a un arresto. En este sentido, reafirma que el arresto en sí mismo autoriza una injerencia significativa en la privacidad, en la medida en que permite a los agentes investigar la comisión de un delito. Asimismo, el Estado argumenta que el volumen de información que una persona decide portar no debería determinar ni limitar los objetos que pueden ser objeto de registro en el momento de la detención.

California señala que la información personal contenida en un teléfono celular es fundamentalmente similar a la que puede llevarse en hojas de papel, fotografías, billeteras o bolsos. En consecuencia, el Estado sostiene que los teléfonos móviles representan una evolución en la cantidad de información que una persona puede portar, pero no en la naturaleza de dicha información, por lo que las reglas tradicionales de registro en el contexto de un arresto deberían aplicarse también a los teléfonos celulares.

El Estado también argumenta que no existe razón para limitar específicamente los registros de teléfonos celulares en el contexto de un arresto, en la medida en que no hay evidencia de que en este caso se vean comprometidos derechos relacionados con la Primera

Enmienda. Sostiene, además, que la información que podría obtenerse de documentos físicos de una persona es equivalente a la que puede extraerse de un teléfono celular. En síntesis, el Estado afirma que este tipo de registro puede implicar una afectación importante del derecho a la privacidad, pero que se encuentra justificado en el contexto de una detención bajo custodia.

Conclusión. En este caso, la Corte Suprema debe determinar si los teléfonos celulares pueden ser objeto de registros incidentales a un arresto. El demandante Riley sostiene que las dos justificaciones tradicionales para este tipo de registros, la seguridad del agente y la preservación de la evidencia, no resultan aplicables al registro de un teléfono celular. Por su parte, el Estado de California propone una regla categórica según la cual todos los objetos que una persona porta o tiene bajo su control al momento del arresto pueden ser objeto de registro legal. Además, afirma que un teléfono celular puede representar un riesgo para la seguridad de los agentes y para la preservación de la evidencia. En este sentido, el caso plantea el alcance de la protección de la Cuarta Enmienda frente a los dispositivos tecnológicos modernos y si existe un interés reforzado en la privacidad de la información contenida en los teléfonos móviles durante una detención. (Riley vs California, 2014)

3.1.2. Caso Carpenter vs Estados Unidos

La inacción del Congreso en materia de privacidad de datos ha generado que tribunales, corporaciones y consumidores enfrenten importantes vacíos regulatorios, viéndose obligados a resolver de manera aislada algunos de los problemas más complejos de la era digital. En este escenario, las empresas de redes sociales y telecomunicaciones recopilan grandes volúmenes de metadatos de los usuarios, los cuales son posteriormente

utilizados para el funcionamiento de sus algoritmos y sistemas de análisis de comportamiento.

Estados y naciones extranjeras se aprovechan de los datos de los usuarios para interferir en las elecciones federales, mientras que las fuerzas del orden emiten citaciones de manera reiterada, accediendo a grandes volúmenes de información civil confidencial con apenas una sospecha razonable que respalde sus solicitudes. En medio de estos conflictos convergen múltiples intereses en tensión, todos ellos buscando una solución legislativa en el Congreso, sin que hasta el momento se haya alcanzado un consenso efectivo.

La última ley importante sobre privacidad de datos aprobada por el Congreso fue la Ley de Privacidad de las Comunicaciones Electrónicas de 1986. Evidentemente, la tecnología ha avanzado de manera significativa en las casi cuatro décadas transcurridas desde su promulgación, por lo que debe reconocerse que el Congreso ha modificado dicha norma y sus disposiciones en varias ocasiones desde 1986.

Sin embargo, en una época en la que el teléfono celular de una persona puede albergar información financiera, datos de ubicación, correos electrónicos, mensajes de texto, registros de llamadas, calendarios personales e incluso información de salud confidencial, la necesidad de contar con estándares nacionales de privacidad de datos que sean actuales, viables y claros resulta innegable. Un ámbito en el que la ausencia de estos estándares es particularmente problemática es el relativo a las protecciones derivadas de la Cuarta y la Quinta Enmienda en el marco de investigaciones y procesos penales.

Por ejemplo, el artículo 18 del Código de los Estados Unidos, artículo 2703(d), contenido en la Ley de Comunicaciones Almacenadas de 1986 (SCA[1]), (Título II de la Ley

[1] SCA: Sudden Cardiac Arrest

de Privacidad de las Comunicaciones Electrónicas de 1986 (ECPA)[2], faculta a las autoridades encargadas de la aplicación de la ley para acceder a prácticamente cualquier comunicación electrónica o datos de clientes almacenados por proveedores de servicios de internet mediante orden judicial.

Pueden obtener una de estas denominadas "órdenes 2703(d)" si logran demostrar hechos específicos y articulables que acrediten la existencia de motivos razonables para creer que la información solicitada es relevante y sustancial para una investigación penal en curso. Dado que la ley fue modificada por última vez hace casi tres décadas, en 1994, el artículo 2703(d) plantea serias preocupaciones en materia de debido proceso y privacidad en un contexto en el que los proveedores de servicios de internet (ISP) tienen acceso a grandes volúmenes de datos de usuarios altamente sensibles y de carácter estrictamente privado.

La Corte Suprema se ha mostrado notablemente reticente a pronunciarse sobre cuestiones de debido proceso relacionadas con esta normativa. El último caso relevante que abordó este tipo de problemáticas fue Carpenter contra Estados Unidos (2018), en el cual la Corte analizó la constitucionalidad del registro y la incautación sin orden judicial de información histórica de localización de estaciones celulares (CSLI)[3]. La CSLI permite determinar la ubicación de una persona en un radio aproximado de 50 metros cuadrados (alrededor de 530 pies cuadrados), y es generada por los proveedores de servicios de internet y telecomunicaciones cada vez que el teléfono celular de un usuario se conecta a una señal de red. Esto incluye tanto conexiones pasivas, como la recepción de mensajes de

[2] ECPA: Electronic Communications Privacy Act
[3] Cell Site Location Information

texto o llamadas, como conexiones activas, tales como el acceso a internet mediante datos móviles o la realización de llamadas.

Los ISP almacenan y analizan la CSLI con fines comerciales, lo que implica que estos registros pueden ser objeto de divulgación mediante una orden 2703(d). En Carpenter vs Estados Unidos (2018), el Buró Federal de Investigaciones (FBI) identificó los números de teléfono de varios sospechosos vinculados a una serie de robos a mano armada en tiendas RadioShack y T-Mobile, ocurridos en el sureste de Michigan y el norte de Ohio en 2011. (Carpenter vs Estados Unidos, 2018)

Los fiscales federales obtuvieron órdenes judiciales bajo la sección 2703(d) que obligaron a varios ISP a divulgar la CSLI de los sospechosos asociada a las llamadas telefónicas entrantes y salientes durante un período de cuatro meses. El peticionario Timothy Carpenter fue uno de esos sospechosos; sus proveedores de servicios de internet (MetroPCS y Sprint) proporcionaron a la fiscalía federal cerca de 13.000 puntos de datos de CSLI, recopilados a lo largo de 127 días.

Tras ser acusado de seis cargos de robo y seis cargos de portación de arma de fuego durante la comisión de un delito federal violento, Carpenter solicitó la exclusión de la CSLI como prueba, al considerar que el gobierno había vulnerado la Cuarta Enmienda al obtener dichos datos sin una orden judicial sustentada en causa probable. El Tribunal de Distrito negó la solicitud y Carpenter fue declarado culpable de once de los doce cargos, siendo posteriormente condenado a casi cien años de prisión federal. El Tribunal de Apelaciones de los Estados Unidos para el Sexto Circuito confirmó la condena, apoyándose principalmente en la “doctrina de la tercera parte” de la Cuarta Enmienda, tal como se establece en (Smith v. Maryland , 1979).

La doctrina de la tercera parte establece que la información divulgada a un tercero no está protegida por la Cuarta Enmienda, en la medida en que las personas renuncian a su expectativa de privacidad respecto de los datos que entregan voluntariamente a dichos terceros. Este razonamiento se sustenta en una construcción jurisprudencial previa desarrollada en (Katz v. United States , 1967), en la cual se establece que existe una violación de la Cuarta Enmienda cuando una actuación estatal vulnera la “expectativa razonable de privacidad” de una persona.

En (Smith v. Maryland , 1979) el Tribunal analizó si la policía había violado la Cuarta Enmienda al instalar sin orden judicial un dispositivo de registro en una compañía telefónica para capturar los números de entrada y salida del domicilio del demandante Michael Lee Smith. Aplicando el criterio de la expectativa razonable de privacidad, el Tribunal concluyó que "una persona no tiene una expectativa legítima de privacidad respecto de la información que entrega voluntariamente a terceros". (Smith v. Maryland , 1979). Antes de Carpenter, los tribunales federales habían interpretado ampliamente la doctrina de la tercera parte como una regla clara: si la información se transmite voluntariamente a un tercero, no está protegida por la Cuarta Enmienda. Punto final

Pero con la llegada de la era de los teléfonos inteligentes, el Tribunal tuvo que analizar si la doctrina de la tercera parte, aplicada tradicionalmente a herramientas analógicas como los registros de llamadas, seguía siendo adecuada en el contexto digital. Reconociendo que la información de localización generada por los teléfonos celulares es detallada, enciclopédica y se recopila de manera automática, el Tribunal matizó el alcance de dicha doctrina, estableciendo que las autoridades deben obtener una orden judicial basada en causa probable antes de acceder a la CSLI.

Pero a pesar de la importancia crucial que tuvo el caso Carpenter para frenar las intrusiones indebidas en las protecciones de la Cuarta Enmienda, no fue perfecto. Para empezar, (Carpenter vs Estados Unidos, 2018) no dudó en definir su estrechez: “Nuestra decisión de hoy es limitada. No expresamos una opinión sobre asuntos que no nos han sido sometidos y no alteramos la aplicación de Smith y Miller” Siendo justos, dadas las posibles implicaciones para la arraigada jurisprudencia del Tribunal en torno a la doctrina de la tercera parte, la cautela de la mayoría era comprensible.

Sin embargo, a lo largo de la opinión continúa siendo evidente que los fundamentos de décadas de la doctrina de la tercera parte han comenzado a debilitarse con la llegada de la era digital. En primer lugar, si la CSLI está sujeta a las protecciones de la Cuarta Enmienda porque, entre otras razones, es detallada, enciclopédica y se recopila sin esfuerzo, ¿por qué no habría de estarlo el historial de compras realizadas con tarjeta de débito o crédito de un usuario? Ciertamente, la Corte ha sido clara al sostener que los registros bancarios se encuentran inequívocamente sometidos a la doctrina de terceros; sin embargo, en una época en la que el uso de efectivo se encuentra en mínimos históricos y el uso de billeteras digitales continúa en aumento, los registros bancarios constituyen solo uno de los múltiples ámbitos en los que la era digital ha hecho prácticamente inevitable revelar información financiera personal a terceros.

Las encuestas realizadas por el Pew Research Center sugieren que una amplia mayoría de los estadounidenses considera imposible desenvolverse en la vida cotidiana sin que empresas privadas o el gobierno recopilen sus datos. Asimismo, la encuesta indica que cerca del 80% de los estadounidenses manifiesta preocupación por el uso de sus datos por parte de empresas privadas, mientras que aproximadamente el 64% expresa preocupación por el uso de datos privados por parte del gobierno. (Pew Researcj Center, 2015)

Si (Katz v. United States , 1967) aún mantiene vigencia, y “la Cuarta Enmienda protege a las personas, no a los lugares”, la Corte Suprema debería reconocer, sin lugar a dudas, que los consumidores poseen una expectativa de privacidad respecto de sus datos digitales, expectativa que, según consideran, está siendo vulnerada por empresas privadas y entidades gubernamentales.

Por otra parte, la CSLI constituye solo una de las múltiples categorías de información altamente sensible respecto de las cuales las autoridades policiales pueden solicitar órdenes de divulgación en virtud de la SCA. La Sección 2703(d) autoriza a las fuerzas del orden a obtener prácticamente cualquier comunicación electrónica o registro en posesión de los ISP, incluidos nombres de clientes, direcciones, registros de llamadas, direcciones de protocolo de internet (IP), números telefónicos, números de tarjetas de crédito e información de cuentas bancarias. Actualmente, los usuarios almacenan en sus teléfonos celulares grandes volúmenes de información especialmente sensible, mientras que los ISP poseen más datos de los usuarios que en cualquier otro momento.[20] A modo de ejemplo, la aplicación “Salud” de Apple permite registrar actividad física, medicamentos, datos relacionados con el sueño e incluso ciclos menstruales.[21] Del mismo modo, Apple proyecta lanzar una nueva aplicación de “diario” que analizará el comportamiento del usuario, su actividad cotidiana, su ubicación y hasta las personas con quienes comparte tiempo.[22]. Frente a este panorama, en algún momento el Congreso o los tribunales deberán establecer límites respecto del grado de accesibilidad que razonablemente pueden tener las fuerzas del orden sobre información de tal sensibilidad. Aunque, de manera provisional, los tribunales puedan asumir la tarea de resolver estos desafíos —considerando que el equilibrio entre la aplicación de la ley y los intereses de privacidad resulta delicado, particular y dependiente de cada caso[23], se trata de una cuestión que puede abordarse de

forma más adecuada mediante mecanismos legislativos, antes que a través de pruebas judiciales flexibles y multifactoriales.

No obstante, aun suponiendo que ni el Congreso ni la Corte Suprema tengan la intención de excluir la aplicabilidad de la doctrina de terceros respecto de los datos digitales o de la información sensible de los usuarios, persisten importantes interrogantes relacionados con la interpretación de la LCA. En particular, la LCA establece únicamente dos límites sustantivos para la emisión de órdenes 2703(d), permitiendo a los tribunales anularlas o modificarlas cuando resulten excesivamente amplias o impongan una carga desproporcionada a los proveedores.

El Congreso no proporciona a los tribunales directrices claras respecto de la aplicación prevista de estos criterios ambiguos. Hasta el momento, la Corte Suprema no ha interpretado el alcance de las cláusulas relativas a cargas inusualmente voluminosas o excesivas contenidas en la sección 2703(d), situación que deja abierta la posibilidad de que surjan múltiples dilemas jurídicos hipotéticos.

Uno de estos dilemas se relaciona con la cuestión de los datos cifrados. Entre 2008 y 2019, el Departamento de Justicia presentó más de sesenta solicitudes ante jueces y magistrados federales con el propósito de obligar a los proveedores de servicios de internet (ISP) a desarrollar software destinado a facilitar el descifrado de datos confidenciales de los usuarios. Debido a que numerosos ISP cifran la información de sus usuarios por razones de privacidad, las fuerzas del orden, en determinadas ocasiones, no cuentan con herramientas suficientes para descifrar los datos que ya se encuentran en su poder.

En otras palabras, la cuestión del descifrado involucra tanto aspectos de la Quinta Enmienda como de la Cuarta Enmienda. Las entidades gubernamentales pueden encontrarse en posesión legítima de un teléfono celular incautado mediante un registro

autorizado judicialmente, pero carecer de los medios necesarios para desbloquearlo. A ello se suma que, como lo estableció la Corte Suprema en el caso (Riley vs California, 2014), la policía, por regla general, no puede, sin una orden judicial, revisar información digital contenida en un teléfono celular incautado a una persona arrestada.

En consecuencia, el gobierno federal ha adoptado la práctica de solicitar órdenes judiciales destinadas a obligar a los ISP a desarrollar software especializado capaz de eludir las funciones de seguridad o descifrar los datos de los usuarios, con el fin de permitir el acceso de los investigadores a dicha información. Esta práctica generó una importante controversia pública en 2016, cuando Apple impugnó abiertamente una orden emitida en virtud de la Ley All Writs, promovida por el Departamento de Justicia (DOJ), mediante la cual se exigía a la compañía desarrollar software que permitiera a los investigadores federales acceder al iPhone del autor del atentado terrorista de San Bernardino, Syed Rizwan Farook (BBC News, 2016).

No obstante, la intensa disputa judicial tuvo una duración limitada, debido a que el FBI obtuvo, antes del inicio del litigio, un contrato privado que le permitió desbloquear el dispositivo. Aunque en el pasado los fiscales federales recurrían con frecuencia a la Ley All Writs para obligar a los ISP a colaborar en investigaciones penales, aprovechando el amplio alcance de sus disposiciones, el DOJ ha reconsiderado posteriormente su estrategia de exigencia de cooperación a los proveedores, especialmente después de enfrentar diversas derrotas significativas en litigios relacionados con dicha ley.

Sin perjuicio de que los fiscales federales procuren obligar al descifrado de los datos de los usuarios mediante la Ley All Writs o la SCA, los tribunales todavía no se han pronunciado de manera concluyente respecto de los límites del poder gubernamental para imponer este tipo de medidas. En la práctica, jueces y magistrados federales continúan

aprobando de forma regular las solicitudes presentadas por el Departamento de Justicia para obtener órdenes de descifrado bajo la Ley All Writs, mientras que los tribunales aún no han definido si la cláusula relativa a la carga indebida prevista en el artículo 2703(d) de la LCA restringe la emisión de este tipo de órdenes en el marco de dicha normativa.

Los principios fundamentales de la justiciabilidad establecen que un proveedor de servicios de internet (ISP) no puede invocar ante los tribunales los derechos de sus usuarios derivados de la Cuarta y Quinta Enmienda. En consecuencia, los ISP disponen de herramientas limitadas para controvertir órdenes de descifrado, en caso de que decidan hacerlo. Además, grandes proveedores como Google y Apple cooperan de manera constante con investigadores federales en el desarrollo de investigaciones penales. (BBC News, 2016)

En consecuencia, por razones prácticas, los ISP no se encuentran en capacidad de impugnar de manera razonable todas las órdenes judiciales, órdenes 2703(d), citaciones o solicitudes de descifrado que les son dirigidas. Entretanto, el Tribunal Supremo ha continuado absteniéndose de pronunciarse en diversos casos relacionados con la privacidad de datos, dejando en manos de los tribunales inferiores la resolución de estos complejos asuntos, pese a la ausencia de lineamientos o directrices nacionales claras por parte del máximo tribunal.

Por ahora, los usuarios se encuentran limitados en su capacidad para garantizar la privacidad de sus datos digitales. Mientras el Congreso o la Corte Suprema no adopten una posición definitiva, los tribunales continuarán enfrentando la compleja tarea de equilibrar los intereses contrapuestos entre la privacidad individual y la aplicación de la ley. No obstante, resulta indiscutible que ninguno de los intereses involucrados en dicho equilibrio

posee un carácter absoluto; por ello, se hace indispensable el desarrollo de normas nacionales claras y actualizadas en materia de privacidad de datos.

3.1.3. Cajar vs Colombia Corte Interamericana de Derechos Humanos

La Corporación de Abogados José Alvear Restrepo (CAJAR) constituye una reconocida organización de derechos humanos en Colombia. Durante más de dos décadas, sus integrantes fueron objeto de **vigilancia ilegal, hostigamientos y amenazas** por parte de organismos estatales de inteligencia, principalmente del extinto Departamento Administrativo de Seguridad (DAS).

Las prácticas denunciadas incluyeron:

- Interceptaciones telefónicas y electrónicas ilegales.
- Acceso indebido a correspondencia privada y documentos internos.
- Seguimientos y actos de hostigamiento contra miembros de la organización y sus familiares.
- Campañas de desprestigio mediante las cuales se les señalaba como colaboradores de grupos armados ilegales.
- Sustracción de información confidencial y realización de allanamientos encubiertos en sus oficinas.

Estas acciones tenían como finalidad debilitar su labor de denuncia frente a las violaciones de derechos humanos en Colombia y exponer a sus integrantes a elevados niveles de riesgo personal y profesional.

En este contexto, resultaba relevante analizar si el Estado colombiano vulneró los derechos fundamentales de los miembros de CAJAR al ejecutar prácticas ilegales de inteligencia y contrainteligencia en su contra, así como determinar en qué medida incurrió en responsabilidad internacional por no garantizar la protección de su intimidad, vida privada y labor como defensores de derechos humanos.

CAJAR y los representantes de las víctimas alegaron que el Estado colombiano implementó un sistema de hostigamiento sistemático que vulneró sus derechos a la vida privada, a la honra, a la libertad de asociación y a las garantías judiciales. De igual manera, sostuvieron que las actividades ilegales de inteligencia no constituían hechos aislados, sino una política institucionalizada del DAS.

Por su parte, el Estado colombiano reconoció parcialmente la existencia de actuaciones irregulares por parte del DAS; no obstante, sostuvo que estas correspondían a conductas realizadas por funcionarios aislados y no a una política estatal. Igualmente, argumentó que, tras la desaparición del DAS, se habían adoptado medidas correctivas.

A partir de ello, la Corte Interamericana de Derechos Humanos valoró las pruebas documentales, los testimonios y los peritajes que evidenciaban la sistematicidad de las labores de vigilancia, la ausencia de controles estatales efectivos y el riesgo permanente al que estuvieron expuestos los miembros de CAJAR.

La Corte IDH declaró a Colombia internacionalmente responsable por la vulneración de los derechos consagrados en la Convención Americana. Como resultado, ordenó la adopción de medidas de reparación, el reconocimiento público de responsabilidad y la implementación de garantías de no repetición, entre ellas, reformas a los sistemas de

inteligencia orientadas a asegurar controles democráticos efectivos. Asimismo, dispuso el establecimiento de garantías de protección y la adopción de protocolos claros para la recolección, uso y almacenamiento de información de inteligencia, así como la creación de mecanismos de control externo y judicial sobre las actividades de inteligencia estatal. Finalmente, la decisión consolidó el reconocimiento del derecho a la autodeterminación informativa dentro del Sistema Interamericano, particularmente en relación con las actividades de inteligencia desarrolladas por el Estado.

La sentencia constituye un hito en la protección de los defensores de derechos humanos en América Latina. Su principal aporte radica en la consolidación del derecho a la autodeterminación informativa, el cual impone a los Estados la obligación de regular y limitar el uso de tecnologías de vigilancia.

La decisión resulta acertada en la medida en que reconoce la responsabilidad estructural del Estado, y no únicamente la de funcionarios individuales; además, establece estándares más rigurosos de control judicial sobre las actividades de inteligencia y fortalece el marco regional de protección del derecho a la intimidad en contextos digitales y de vigilancia. No obstante, también plantea importantes desafíos, entre ellos, la implementación efectiva de los controles ordenados y la necesidad de transformar las culturas institucionales de seguridad presentes en los Estados.

3.2.Jurisprudencia nacional

3.2.1. Corte Constitucional Sentencia T-043/ 2020

Antecedentes del caso. La sentencia T-043/2020 tuvo origen en el marco de un proceso penal, en el cual una de las partes aportó como prueba capturas de pantalla de conversaciones de WhatsApp. Dichos documentos buscaban acreditar determinadas actuaciones de la contraparte. En este contexto, los jueces debieron analizar si las impresiones del contenido visualizado en pantalla poseían el mismo valor probatorio que los archivos digitales originales.

La demandante argumentó que las capturas de pantalla eran auténticas, debido a que habían sido obtenidas directamente desde su teléfono móvil. Igualmente, señaló que los mensajes resultaban determinantes para el resultado del proceso. Por su parte, la contraparte cuestionó la autenticidad de dichos documentos, al sostener que las capturas de pantalla podían ser fácilmente manipuladas mediante programas de edición fotográfica.

Esta controversia evidencia una problemática ampliamente extendida: aunque las comunicaciones digitales son de fácil acceso, con frecuencia no existe un procedimiento estandarizado que permita garantizar su autenticidad. En ausencia de metadatos, códigos hash o registros de verificación, persiste el riesgo de que los tribunales admitan pruebas defectuosas o potencialmente manipuladas.

El problema jurídico surge al intentar determinar si ¿las capturas de pantalla de conversaciones de WhatsApp pueden considerarse prueba electrónica con pleno valor probatorio o si, por el contrario, deben entenderse únicamente como prueba circunstancial que requiere ser valorada conjuntamente con otros elementos probatorios?

Esta cuestión jurídica incide directamente en la aplicación de la Ley de Procedimiento Penal colombiana (Ley 906 de 2004), la cual, aunque autoriza el uso de prueba electrónica, no establece disposiciones específicas respecto de las capturas de pantalla. Del mismo modo, compromete derechos fundamentales como el derecho al debido proceso, las garantías de un juicio justo y el principio de igualdad de armas.

Tras realizar un análisis exhaustivo, la Corte llegó a varias conclusiones relevantes. Una de las principales consistió en establecer la diferencia entre la prueba electrónica y la prueba circunstancial. En ese sentido, los jueces precisaron que las capturas de pantalla impresas no pueden ser aceptadas automáticamente como prueba electrónica, debido a que esta última exige que el archivo se conserve en su formato original y que su integridad pueda ser verificada. En contraste, una impresión elimina información técnica esencial para comprobar su autenticidad. Por esta razón, las capturas de pantalla únicamente pueden considerarse, en el mejor de los casos, como prueba circunstancial orientada a demostrar determinados hechos, cuyo valor probatorio dependerá de otros elementos de corroboración.

Segundo, la Corte se pronunció sobre los requisitos de autenticidad e integridad de la prueba digital. Respecto de la autenticidad, señaló que esta exige demostrar que la evidencia proviene efectivamente de la fuente que se afirma. Por su parte, la integridad implica acreditar que el contenido no ha sido alterado. El tribunal enfatizó que, tratándose de pruebas digitales, dichos requisitos únicamente pueden verificarse de manera confiable mediante procedimientos técnicos especializados, tales como el análisis de metadatos o la intervención de peritos.

Tercero, la Corte analizó la carga de la prueba y señaló que la parte que aporta un documento digital tiene la responsabilidad de demostrar su autenticidad. No obstante, ello

no implica que la contraparte quede en estado de indefensión, ya que conserva el derecho de controvertir la autenticidad de la prueba y presentar elementos de contradicción o contrapruebas.

Cuarto, respecto del derecho de objeción y defensa, los jueces enfatizaron la importancia del derecho de contradicción. En este sentido, señalaron que las pruebas que no puedan ser verificadas de manera suficiente no pueden constituir el único fundamento de una decisión judicial, ya que ello vulneraría el derecho de defensa.

Quinto, en relación con la relevancia internacional, se expuso que la decisión también hizo referencia a principios internacionales, entre ellos las Leyes Modelo de la CNUDMI sobre Prueba Electrónica, las cuales igualmente destacan la importancia de la autenticidad y la integridad de la evidencia digital. Esta sentencia generó un impacto significativo, debido a que el tribunal determinó que las capturas de pantalla de mensajes de WhatsApp no constituyen prueba electrónica plenamente válida, sino que deben considerarse únicamente como prueba circunstancial. En consecuencia, pueden complementar un conjunto probatorio, pero no pueden servir, de manera aislada, como fundamento exclusivo de una condena o de una decisión judicial.

Impacto en el Derecho Penal. El Tribunal Constitucional estableció que las capturas de pantalla de mensajes de WhatsApp no constituyen prueba electrónica plena, sino que deben ser consideradas como prueba circunstancial. Aunque pueden contribuir a ilustrar los hechos objeto de debate, no pueden emplearse como fundamento único para emitir una condena penal.

Primero: Importancia para la valoración de la prueba. En los procesos penales se aplica el principio *in dubio pro reo*, según el cual el beneficio de la duda favorece al acusado. Debido a que las capturas de pantalla pueden ser manipuladas con facilidad y su

autenticidad no puede garantizarse sin mecanismos técnicos de verificación, el tribunal concluyó que estas no pueden constituir una base suficiente para imponer sanciones penales. Por tal motivo, dichas pruebas deben estar acompañadas de otros elementos de convicción, tales como informes forenses, declaraciones testimoniales o la obtención de los archivos digitales originales.

Segundo: Impacto en las autoridades investigadoras. Para la policía y la fiscalía, esta decisión implica la necesidad de adoptar medidas más rigurosas para la protección y recolección de comunicaciones digitales. En consecuencia, la simple presentación de capturas de pantalla impresas deja de ser suficiente como medio probatorio. Por el contrario, resulta indispensable la obtención de los archivos originales, la adecuada documentación de la cadena de custodia y, cuando sea necesario, la intervención de expertos en informática forense, con el fin de garantizar la admisibilidad de la prueba ante el tribunal.

Tercero: Protección de los derechos de la defensa. La decisión fortalece las garantías del acusado, debido a que el uso de capturas de pantalla como prueba principal, sin una verificación adecuada, podría conducir a errores judiciales. En este sentido, su clasificación como prueba circunstancial asegura que el acusado tenga la posibilidad de controvertir de manera efectiva la autenticidad de dichos documentos.

Cuarto: El efecto preventivo. Finalmente, la decisión también produce un efecto preventivo, en la medida en que advierte a todas las partes involucradas en el proceso que la prueba digital en materia penal exige el mayor grado de cuidado y rigurosidad. De esta manera, contribuye al mejoramiento de la calidad de las investigaciones y al fortalecimiento de la confianza en la administración de justicia.

3.2.2. Corte Constitucional Sentencia SP248/2025

Los antecedentes del caso se originan con el asesinato de Édgar Quintero, periodista del municipio de Palmira (Valle del Cauca), ocurrido el 2 de marzo de 2015. Los hechos tuvieron lugar en la panadería “Pan Caliente”, establecimiento que frecuentaba de manera habitual. Quintero desarrollaba labores periodísticas relacionadas con denuncias sobre la administración municipal, actuaciones de la policía y actividades de microtráfico, circunstancias que lo situaban en un contexto de riesgo. Este aspecto ha sido señalado en análisis de terceros que retoman lo expuesto en la sentencia.

El acusado John Freyder Caicedo Popo, alias “Chocolate”, es acusado de ser quien disparó contra Quintero, asesinándolo.

Para sustentar la acusación, se tuvieron en cuenta los siguientes elementos materiales probatorios:

a. Fotografías extraídas de una memoria Micro SD perteneciente a un teléfono celular marca Vodafone, encontrado en el lugar de los hechos.
b. Archivos almacenados en un disco duro externo marca Buffalo.
c. Intervención de los investigadores Sandra Julieth Enríquez, quien obtuvo evidencias en el lugar de los hechos; William Antonio Saldarriaga Zúñiga, encargado del análisis de informática forense y de la extracción de imágenes de la memoria Micro SD; y Leydi Judith Orejuela Gutiérrez, investigadora que realizó la impresión de las fotografías y participó en su incorporación al juicio.
d. Declaraciones juradas rendidas con anterioridad al juicio por los testigos presenciales Luis Orlando Mosquera Llanos y Miguel Ángel Murillo Hurtado,

quienes realizaron un reconocimiento fotográfico del acusado, identificándolo como autor del homicidio.

e. Durante el juicio, dichos testigos se retractaron o modificaron su versión inicial, argumentando razones relacionadas con miedo, amenazas e inseguridad. Adicionalmente, comparecieron como testigos de cargo Clara Luz y Lina María López Correa, empleadas de la panadería, quienes manifestaron haber sido objeto de amenazas; incluso, al menos una de ellas tuvo que ser conducida al juicio debido al estado de nerviosismo que presentaba.

El A quo profirió fallo condenatorio, al considerar que la prueba digital —particularmente las fotografías aportadas— resultaba válida, que los testigos de cargo presentaban versiones coherentes y que las retractaciones efectuadas durante el juicio no cumplían con los requisitos necesarios para desvirtuar las declaraciones rendidas previamente. En consecuencia, se otorgó credibilidad a los testimonios iniciales.

El *ad quem*, correspondiente al Tribunal Superior de Buga, absolvió al acusado al considerar que existía duda razonable. Para ello, excluyó las seis fotografías extraídas de la memoria Micro SD, argumentando un inadecuado manejo de la cadena de custodia y cuestionando su legalidad y autenticidad, entre otros aspectos, por la ausencia de código hash y porque el dispositivo físico no fue incorporado al juicio. De igual manera, otorgó mayor credibilidad a las retractaciones efectuadas por los testigos durante el juicio que a las entrevistas y declaraciones rendidas con anterioridad.

Posteriormente, con ocasión de la interposición del recurso de casación, la Fiscalía acudió ante la Corte Suprema de Justicia argumentando que la absolución había sido

improcedente. Sostuvo que las pruebas fotográficas no debieron ser excluidas y que el Tribunal incurrió en errores de valoración probatoria al otorgar mayor credibilidad a las retractaciones realizadas en juicio, sin considerar adecuadamente el contexto de amenazas ni las declaraciones rendidas previamente por los testigos.

La Corte, en la sentencia SP248-2025, abordó diversos aspectos jurídicos de especial relevancia. Entre los más importantes se encuentran los siguientes:

Legalidad vs. Ilícito de la prueba, la cláusula de exclusión:

La Corte reiteró que la Constitución establece que toda prueba obtenida con vulneración de garantías fundamentales carece de validez de pleno derecho, conforme a lo dispuesto en el artículo 29 de la Constitución Política y el artículo 23 de la Ley 906 de 2004. Asimismo, diferenció los conceptos de prueba ilícita y prueba ilegal: la primera se configura cuando existe una afectación directa de derechos fundamentales, mientras que la segunda surge por el incumplimiento de formalidades legales en la obtención o incorporación de la prueba.

En el caso concreto, la Corte consideró que la evidencia fotográfica digital no fue obtenida mediante una vulneración sustancial de normas que justificara su exclusión. Asimismo, reconoció que sí se realizó el control posterior en los términos previstos por la ley y que existió descubrimiento probatorio, circunstancia que permitió a la defensa conocer oportunamente dichas pruebas. En consecuencia, concluyó que el Tribunal no podía excluir de manera automática las fotografías aportadas.

1. Prueba digital, autenticidad y cadena de custodia.

No se exige la existencia de un código hash como requisito indispensable para la validez de una prueba digital, aunque dicho mecanismo constituye una buena práctica para garantizar su integridad. Lo verdaderamente relevante es que la autenticidad de la evidencia pueda acreditarse mediante otros medios idóneos, tales como peritajes técnicos o las declaraciones de las personas encargadas de recolectar, extraer, almacenar e imprimir las imágenes.

El dispositivo original no necesariamente debe estar presente en el juicio oral cuando ello resulte impracticable, por ejemplo, en situaciones en las que existan miles de archivos, siempre que se garantice que el material presentado (como las imágenes impresas en este caso) corresponda fielmente a la información extraída mediante procedimientos confiables.

Se reconoció que la Fiscalía realizó el debido descubrimiento probatorio, al informar a la defensa sobre la existencia del disco duro y de las fotografías, lo que permitió el ejercicio del debate probatorio. En este sentido, la ausencia del código hash o del dispositivo físico completo no constituyó, por sí sola, un motivo suficiente para excluir la prueba, dado que no se demostró que dicha omisión implicara una vulneración sustancial del debido proceso.

2. Valoración de testimonios, retractaciones, y sana crítica

La Corte analizó si el Tribunal de segunda instancia aplicó correctamente los principios de la sana crítica al valorar las retractaciones realizadas por los testigos. A partir de ello, concluyó que dicho tribunal incurrió en un falso raciocinio, al otorgar mayor credibilidad a las retractaciones que a las declaraciones iniciales, sin una motivación

suficiente y sin ponderar adecuadamente el contexto de amenazas, miedo y vulnerabilidad en el que se encontraban los testigos.

Se invocaron ejemplos relacionados con el temor manifestado por las testigos, entre ellos, amenazas como “usted tiene hijo, escóndase”, el estado de nerviosismo que presentaban y el contexto regional de violencia, circunstancias que podían influir en sus declaraciones durante el juicio. El Tribunal, al descartar sin mayor análisis las declaraciones previas y otorgar mayor peso a las retractaciones, no realizó una valoración integral de los medios de prueba, ni contrastó de manera suficiente las versiones iniciales y posteriores, ni examinó adecuadamente si dichas retractaciones podían estar justificadas por el miedo o las amenazas sufridas por las testigos.

3. Falso juicio de legalidad del Tribunal en cuanto a la exclusión de las fotografías

La Corte consideró que el Tribunal incurrió en un “falso juicio de legalidad” al excluir las fotografías sin que se hubiera acreditado de manera clara la existencia de una vulneración sustancial que justificara dicha exclusión. Esta determinación se sustentó principalmente en aspectos formales, como la ausencia del dispositivo físico completo o la inexistencia de un código hash, en lugar de realizar un análisis de fondo sobre si la prueba afectaba garantías como el derecho de defensa, la contradicción o la igualdad procesal.

La Corte concluyó que debía casarse la sentencia absolutoria dictada en segunda instancia. En consecuencia, anuló dicha decisión para que prevaleciera la condena proferida en primera instancia. Asimismo, confirmó la responsabilidad penal de John Freyder Caicedo Popo por el homicidio del periodista Édgar Quintero, con fundamento en la

valoración conjunta de las pruebas, incluidas la prueba digital, las declaraciones previas de los testigos y el contexto de amenazas existente.

Esta sentencia tiene relevancia jurídica porque abordó aspectos como:

Primero, la flexibilidad probatoria con estándares claros, la sentencia refuerza la idea de que la incorporación y valoración de la prueba digital no pueden depender exclusivamente de formalismos estrictos, como la existencia de un código hash o la presencia física del dispositivo, cuando la autenticidad puede acreditarse mediante otros mecanismos idóneos. De esta manera, se abre paso a una aplicación más moderna de los estándares probatorios frente a las evidencias tecnológicas.

Segundo, la protección del debido proceso en contextos de violencia y amenazas, la sentencia reconoce que factores como el miedo, las amenazas y la vulnerabilidad pueden influir en las declaraciones de los testigos, razón por la cual las retractaciones no deben recibir automáticamente mayor credibilidad que las versiones iniciales. En consecuencia, se exige un análisis contextual debidamente motivado, lo que fortalece garantías fundamentales como el derecho de defensa, la igualdad y la contradicción.

Tercero, la clarificación de los conceptos de prueba ilegal, prueba ilícita y formalidades no esenciales, la Corte delimita los supuestos en los cuales el incumplimiento de determinadas formalidades conduce a la exclusión de la prueba y aquellos en los que esta puede ser admitida, siempre que no exista una afectación sustancial al debido proceso.

Cuarto, la importancia del descubrimiento probatorio, la sentencia enfatiza que la defensa debe ser informada oportunamente sobre las pruebas existentes, con el fin de garantizar un debate probatorio pleno, aspecto esencial para la legitimidad del proceso.

Quinto, el criterio de valoración conjunta de las pruebas, la sentencia destaca que no resulta suficiente analizar de manera aislada cada elemento probatorio, sino que es necesario valorar el acervo probatorio en su conjunto, confrontando fotografías, declaraciones iniciales, retractaciones, pruebas periciales y demás elementos, con el propósito de establecer la certeza más allá de toda duda razonable.

CAPÍTULO IV:

Tensiones entre el manejo procesa de las pruebas digitales, el derecho al debido y el derecho a la defensa.

4.1.Obtención de la prueba digital desde el celular

Los precedentes norteamericanos plantean una cuestión esencial que aún no ha sido suficientemente abordada: ¿por qué existen protocolos tan rigurosos para la práctica de allanamientos físicos, mientras que en materia de dispositivos digitales no se exigen estándares equivalentes? Cuando el apoderado realiza el control de legalidad de un allanamiento, se verifican los motivos fundados de la diligencia y si el fiscal especificó los lugares concretos sobre los cuales recaería la intervención, así como los elementos que pretendía encontrar. En ese contexto, debe justificarse la necesidad de ingresar a una habitación determinada; por ejemplo, si la hipótesis investigativa sostiene que la droga se encuentra en la cochera o en el garaje del vehículo no existiría razón para ingresar a las habitaciones de la vivienda, esta lógica de delimitación y motivación específica debería extenderse igualmente a la obtención de prueba digital contenida en teléfonos celulares y otros dispositivos electrónicos.

En contraste, pareciera existir una especie de autorización ilimitada respecto del acceso al celular. En muchos casos, cuando un ciudadano es capturado y porta un teléfono móvil, se asume que la orden de captura incluye automáticamente la revisión integral del dispositivo, como consecuencia, este es inspeccionado y descargado en su totalidad, incluso, en situaciones donde el celular cuenta con sistemas de reconocimiento facial, algunos funcionarios desbloquean el dispositivo utilizando el rostro de la persona sin solicitar previamente su autorización. Esta práctica genera cuestionamientos relevantes,

especialmente porque evidencia la ausencia de los mismos requisitos y controles que se exigen frente a otras intromisiones en la intimidad y la privacidad. Por ello, los estándares relacionados con los motivos fundados y la delimitación de la intervención deberían aplicarse igualmente al acceso y revisión de teléfonos celulares.

De esta manera, cuando se pretenda acceder a un teléfono celular, debe existir una orden judicial sometida a su respectivo control. Además, dicha autorización debería especificar de manera razonable las razones por las cuales se ingresará a determinados contenidos del dispositivo, como la galería de fotografías, las conversaciones de WhatsApp, el correo electrónico, el registro de llamadas o cualquier otro componente del amplio universo de información almacenada en el celular.

Por ejemplo, si se incautara el celular de un abogado, podría ocurrir que este contenga acceso a plataformas como Dropbox o bases de datos con carpetas que almacenen información confidencial relacionada con los casos que adelanta dicha persona, así como fotografías, conversaciones, evidencias y procesos reservados a los cuales tiene acceso precisamente por el ejercicio de su profesión.

La realidad es que en Colombia aún existe una mora en asumir con seriedad la importancia que tiene actualmente el teléfono celular. Por ello, resulta particularmente interesante la metáfora desarrollada en la jurisprudencia norteamericana, según la cual el celular puede entenderse como una extensión de la anatomía humana. En ese sentido, el dispositivo representa una prolongación de la intimidad, de la memoria y de los derechos fundamentales de la persona, razón por la cual su intervención no puede considerarse una intromisión menor.

La realidad actual demuestra que la importancia atribuida al teléfono celular exige un tratamiento de privacidad equivalente al que se otorga al ingreso a una vivienda en el

contexto de un allanamiento, incluso, existen casos en los que personas han sido condenadas por espiar el celular de su pareja, aun cuando la relación conyugal representa uno de los mayores espacios de intimidad compartida. Si en ese ámbito se reconocen límites respecto al acceso a los datos y a la información personal, surge entonces el cuestionamiento de por qué esos mismos límites no se imponen con igual rigor al Estado dentro de una causa penal, especialmente cuando este actúa, en últimas, como contraparte del investigado, resulta necesario avanzar hacia estándares más estrictos de protección, y en ese propósito las propuestas formuladas por los litigantes pueden ser de gran utilidad para promover este tipo de debates.

De todas maneras, un elemento material probatorio como una fotografía obtenida mediante el acceso arbitrario al celular por parte de funcionarios investigadores o incluso de la policía durante una requisa difícilmente superaría una audiencia preparatoria frente a un cuestionamiento por ilegalidad. Esto ocurre porque existe una confrontación directa con el derecho constitucional a la intimidad, discusión que incluso podría conducir a considerar la prueba como ilícita.

4.2.Colaboración de las plataformas digitales con la investigación penal colombiana

Cuando un mensaje de datos se encuentra encriptado o simplemente no se puede tener acceso a él por múltiples motivos, como por ejemplo que el dato se encuentre en un dispositivo que no pertenece al poderdante que se está representando, entonces es necesario recordar que existen acuerdos de colaboración, entre ellos la Convención de Budapest del año 2001, mediante los cuales las autoridades pueden prestarse asistencia. Sin embargo, el problema surge precisamente cuando una comunicación entre emisores y receptores se

encuentra debidamente encriptada, ya que ni siquiera WhatsApp puede acceder a su contenido, porque únicamente los dispositivos de los participantes de la conversación poseen el código necesario para acceder a esa información.

Sin embargo, muchas personas cuentan con copias de seguridad en la nube y podría accederse a ellas a través del dispositivo, aun así, actualmente no existe al menos de manera lícita ningún mecanismo que permita interceptar una comunicación en medio de su transmisión y desencriptarla ya que lo único que se obtendría serían datos imposibles de leer, circunstancia que otorga cierto nivel de confiabilidad al sistema.

Lo que sí podría hacerse es acudir a softwares maliciosos; sin embargo, al tratarse de este tipo de herramientas difícilmente superarían un análisis de legalidad en sede de audiencia preparatoria ya que graban subrepticiamente toda la información contenida en el celular, algo similar ocurre con el desbloqueo del dispositivo mediante el reconocimiento facial de la persona.

Sin embargo, sí existen plataformas utilizadas por la Fiscalía General de la Nación para la recopilación de evidencia digital:

> En la Dirección Especializada contra los Delitos Informáticos se han utilizado herramientas tecnológicas avanzadas con el propósito de optimizar procesos y obtener resultados concluyentes en los análisis forenses. Entre las herramientas empleadas se encuentran IBM Watson Explorer, IBM i2 Notebook, Chainalysis, Ghidra, Magnet Axiom y Cellebrite Physical Analyzer. Asimismo, se han implementado estrategias orientadas a articular esfuerzos para el desarrollo efectivo de las investigaciones, destacándose la colaboración con la Policía Nacional, el Ejército Nacional, ASOBANCARIA y FASECOLDA, entre otras entidades. (Fiscalia General de la Nacion, 2025, pág. 7)

4.3.Aspectos técnicos que se deben tener en cuenta para presentar pruebas de redes sociales.

Lo ideal es realizar una copia de las conversaciones; sin embargo, también surge otro problema, ya que muchas interacciones no se encuentran disponibles de esa manera, como ocurre con los comentarios en muros, publicaciones en Twitter o mensajes intercambiados entre usuarios. En esos casos, por ejemplo, en Twitter, no resulta recomendable limitarse a tomar un pantallazo lo adecuado es ingresar directamente a la publicación, ampliarla y copiar la URL disponible, pues cada trino cuenta con una dirección electrónica propia que permite identificarlo de manera individual.

Existen herramientas en internet de fácil acceso en las que se pega el enlace y estas certifican que dicho link corresponde efectivamente a una determinada página lo que permite otorgar mayor credibilidad a la información presentada. Aunque en muchos procesos relacionados con amenazas en redes sociales y situaciones similares todavía se utilizan pantallazos, lo que se propone es avanzar un poco más allá de ese mecanismo.

Las cortes también deberán fijar límites más claros frente al uso de capturas de pantalla debido a que estas pueden prestarse para abusos probatorios difíciles de controlar. Por ello, resulta necesario mejorar las prácticas de recolección y preservación de evidencia digital. Sin embargo, esto también plantea dificultades porque en últimas una persona advertida del proceso podría cuestionar quién garantiza que la evidencia no fue manipulada antes de ser presentada.

La discusión se vuelve aún más compleja con el uso indebido de herramientas de inteligencia artificial capaces de alterar o fabricar contenidos digitales, todo esto demuestra

que se trata de un escenario altamente complejo que requiere avances tanto jurisprudenciales como normativos para construir mayores bases procesales y ofrecer garantías efectivas tanto a la persona investigada como a la víctima.

4.4. Perito.

En un procedimiento pericial, lo primero que debe realizarse sobre una base de computador es la denominada prueba espejo pues constituye el protocolo técnico inicial, si no se practica dicha copia espejo el dictamen rendido por el perito podría ser objeto de contradicción. No obstante, la prueba espejo no es el único mecanismo para garantizar la fiabilidad de un elemento probatorio, su utilización dependerá del tipo de información que se pretenda fijar y de la herramienta empleada para ello ya que existen documentos o contenidos digitales que no pueden ser copiados de manera íntegra bajo este método debido a que no siempre se encuentran disponibles para ese tipo de extracción.

> Una copia espejo en el ámbito digital se refiere a una imagen forense o clon forense, que es una copia exacta, bit a bit, de un dispositivo de almacenamiento como un disco duro o un teléfono celular. Este proceso, también llamado clonado forense, es crucial para la informática forense porque crea una réplica bit a bit del dispositivo original, preservando toda la información, incluyendo datos visibles, eliminados y no asignados, sin alterar la evidencia. La integridad de la copia se verifica mediante un código hash, como SHA256 o MD5, comparando el valor hash del original con el de la copia. (Tamayo, 2024, pág. 1)

Una situación distinta se presenta cuando la información efectivamente se encuentra almacenada de manera local en el celular pues en ese caso puede realizarse una copia espejo del dispositivo, por ello, muchas veces resulta fundamental conservar el aparato donde se encuentra la información como ocurre con los teléfonos móviles ya que ello permite efectuar una extracción íntegra de los datos.

El problema surge cuando la información se encuentra almacenada en la infraestructura o propiedad de un tercero porque en esos casos nunca se obtiene realmente una copia espejo del archivo original, lo único que existe es acceso a determinada información alojada externamente. En consecuencia, lo que debe garantizarse mediante herramientas informáticas es que el protocolo de extracción utilizado haya sido válido y confiable.

En la medida de lo posible el procedimiento debe realizarse sobre el mismo elemento donde se encuentra la información, así si resulta viable puede abrirse directamente ante el juez la conversación de WhatsApp en el celular de la persona y mostrarla desde la propia aplicación, posteriormente esa conversación puede exportarse desde el mismo dispositivo y enviarse mediante las herramientas que ofrece la plataforma.

Obviamente, todo esto también admite múltiples discusiones especialmente porque no existe un rito expresamente descrito en una norma para este tipo de procedimientos, la situación ideal se presenta cuando se cuenta con el archivo completo en un dispositivo propio, es decir, perteneciente al titular de la fuente. Sin embargo, el escenario cambia cuando una persona es titular del dato, pero no de la fuente donde este se encuentra almacenado, situación que actualmente ocurre con gran parte de la información digital.

4.5.Firma digital.

Sobre la firma digital, resulta importante abordar la manera correcta de presentar un documento como prueba legal y válida especialmente porque durante la pandemia el derecho mantuvo una visión altamente ritualista frente a este tema, en ese contexto, comenzó a discutirse con mayor frecuencia la diferencia entre firma electrónica y firma digital, así como diversos aspectos técnicos que suelen ser considerados por los notarios. En la práctica una de las soluciones más utilizadas ha sido el envío de documentos con una firma que realmente no corresponde ni a una firma digital ni a una firma electrónica, sino simplemente a una imagen pegada de la firma manuscrita, mecanismo que además resulta altamente falsificable. Por ello, para garantizar que un contrato sea auténtico y efectivo, lo que suele verificarse es la trazabilidad de la comunicación a través del correo electrónico, permitiendo construir una valoración indiciaria sobre la autenticidad del documento.

También, puede acudirse a sistemas de certificación prestados por agencias especializadas que ofrecen servicios de validación electrónica, estas entidades toman fotografías, verifican la identidad del usuario y garantizan que la firma electrónica fue efectivamente realizada por la persona correspondiente. Varias plataformas utilizan actualmente este tipo de mecanismos en los cuales el usuario ingresa virtualmente se le toma una fotografía en tiempo real y se aplican procedimientos de verificación similares a los utilizados para tarjetas de crédito como el reconocimiento biométrico facial, el escaneo de la cédula y la comparación de datos.

Todo ello evidencia que el panorama se vuelve cada vez más complejo, porque ya no es posible pretender que la realidad tecnológica avance al ritmo del modelo probatorio

ortodoxo; por el contrario, es el derecho probatorio el que debe adaptarse y alcanzar las nuevas dinámicas digitales.

> En Colombia, las agencias de certificación de firma digital acreditadas por el Organismo Nacional de Acreditación (ONAC) incluyen a Camerfirma Colombia, Viafirma Colombia y Certicamara, entre otras que ofrecen soluciones para personas naturales y jurídicas. Estas entidades garantizan la seguridad y validez jurídica de los documentos firmados electrónicamente mediante la emisión de certificados digitales. (Viafirma, 2025, pág. 1)

Lo cual se va complejizando aún más, puesto que ya no es posible avanzar al ritmo del mundo probatorio "ortodoxo"; por el contrario, es el derecho probatorio el que debe adaptarse y alcanzar las dinámicas tecnológicas actuales. En cada caso será necesario analizar la fiabilidad del elemento presentado pero lo cierto es que la firma plasmada en un documento ya no posee la misma fuerza probatoria que tenía en el pasado.

En consecuencia, resulta necesario acompañarla de otros elementos que permitan inferir que realmente existió la intención de la persona de suscribir el documento. Actualmente, tomar la firma de cualquier archivo mediante un screenshot o una imagen es relativamente sencillo de duplicar razón por la cual adquieren mayor relevancia los servicios internacionales de certificación de firmas electrónicas.

4.6.Correo electrónico como prueba.

El correo electrónico constituye una de las pruebas digitales por excelencia, sin embargo, con frecuencia sigue aportándose innecesariamente mediante simples pantallazos

pese a que muchos proveedores permiten acceder a las propiedades del mensaje y guardarlo de forma completa. En esos casos, normalmente se genera un archivo PDF; no obstante, dicho documento continúa siendo plenamente vulnerable ya que puede adulterarse, modificarse o alterarse con relativa facilidad.

Hasta ahora se ha permitido un procedimiento consistente en que el testigo abra directamente su propio correo electrónico durante el juicio y desde allí reenvíe el mensaje al correo del despacho judicial, este mecanismo no ha encontrado mayores obstáculos en la práctica ya que permite conservar la trazabilidad de los correos enviados y, además, brinda al juez mayores garantías de que la prueba no fue vulnerada o alterada.

Esto demuestra que también se requiere innovación en los procesos judiciales especialmente porque lo importante es transmitirle al juez seguridad sobre el elemento probatorio dentro del contexto de la evidencia digital caracterizada precisamente por su volatilidad y vulnerabilidad, una de las formas de lograrlo es mediante este tipo de prácticas.

4.7.Facultades de la víctima en el recaudo de la prueba digital.

Debe entenderse que tanto el papel de la víctima como el de la defensa responden a intereses antagónicos, pero necesarios dentro de la construcción del proceso penal siempre que no se desborden las facultades de cada una de las partes, la víctima cuenta con facultades probatorias; sin embargo, debe tener presente que, a partir de la audiencia preparatoria y especialmente durante el juicio, estas deben canalizarse a través de la Fiscalía.

Mientras se mantenga ese límite, conforme al cual la práctica e incorporación de la prueba en juicio corresponde únicamente a la Fiscalía resulta acertado que el código le permita previamente amplias facultades a la víctima para recolectar y descubrir elementos probatorios pues en últimas es la principal afectada por la conducta delictiva. (Fiscalia General de al Nacion, 2025)

Permitir este tipo de facultades a la víctima también contribuye a descongestionar la actividad estatal lo cual resulta necesario en muchos casos, por ejemplo, una compañía podría alegar que fue víctima del hurto de información almacenada en sus servidores; en ese escenario, la empresa puede contar con los recursos suficientes para contratar una experticia externa, acudir a ingenieros altamente capacitados, recopilar la información y presentarla debidamente organizada. En ese contexto, no siempre resulta necesario que toda la carga técnica recaiga exclusivamente sobre la Fiscalía y sus investigadores. Por ello, es razonable reconocer amplias facultades de recaudo a la víctima, siempre que se garantice que la información no fue adulterada durante su obtención. Naturalmente, esas cuestiones deberán ser objeto de valoración posterior dentro del proceso penal.

Por consiguiente, la víctima sí debe contar con facultades probatorias, siempre que se mantenga el límite correspondiente dentro del juicio en el sentido de que la práctica e incorporación de la prueba debe realizarse a través de la Fiscalía, quien es en últimas la titular de la pretensión punitiva del Estado.

CONCLUSIONES

La presente investigación logró poner en evidencia que la prueba digital, actualmente, se afianzó como un elemento crucial, uno esencial dentro del proceso penal moderno. Esto es por el gran impacto que tienen las tecnologías de la información en nuestra vida diaria, e inclusive en la creación de pruebas. A pesar de esto, su inclusión en el sistema jurídico colombiano todavía revela deficiencias normativas, originando dudas sobre su admisión, su autenticidad, y también la forma de valorar esas evidencias (Parra J. , 2019)

Además, durante este estudio se observó que, aunque la doctrina haya buscado asemejar la prueba digital a la documental mediante el principio de equivalencia funcional, semejante postura es deficiente ante las características técnicas específicas de la evidencia electrónica. Esto debido a factores como su fugacidad, la facilidad para ser alterada, y la imprescindible necesidad de herramientas tecnológicas para su interpretación (Chaia R. , 2024)En consecuencia, se manifiesta la necesidad imperiosa de promover una comprensión más independiente de la prueba digital en el ámbito del derecho probatorio.

Es pertinente resaltar que la jurisprudencia colombiana, basada en la Ley 527 de 1999 y el Código de Procedimiento Penal (Ley 906 de 2004), reconoce validez probatoria a la evidencia digital si se garantiza su autenticidad e integridad. La Corte enfatiza la cadena de custodia y la pericia técnica para su admisibilidad, admitiendo representaciones físicas o digitales una vez autenticadas es importante que la normativa colombiana, especialmente la Ley 1273 de 2009, proporciona el marco para la protección de la información y los datos, fundamental para el manejo de evidencia digital en investigaciones penales.

De igual modo, se consiguió concretar que la evaluación de la prueba digital ha de efectuarse conforme los preceptos de la sana crítica, la libertad probatoria y el derecho a la

contradicción. Tales fundamentos facultan al juzgador a examinar esta clase de evidencia empleando criterios lógicos, científicos, y técnicos. Empero, la carencia de directrices precisas es capaz de acarrear peligros al debido proceso y al derecho a la defensa, más aún, cuando no se salvaguarda a cabalidad la autenticidad e integridad de la información digital como lo menciona (Taruffo, 2012).

De otra manera, se detectó que la cadena de custodia en la evidencia digital, toma una trascendencia particular, ya que, no solamente concierne a la preservación material del elemento probatorio, sino también, la seguridad de su integridad y trazabilidad desde el instante de su adquisición hasta su inclusión en el proceso. Dentro de éste marco, la escasez de protocolos técnicos homogéneos pudiera socavar la confiabilidad de éste tipo de prueba.

Dado el talante exploratorio que informa esta indagación, el objetivo no reside en la formulación de conclusiones taxativas. Más bien, aspiramos a ofrecer perspectivas analíticas que faciliten la comprensión de los retos prominentes asociados al empleo de la evidencia digital en el ámbito penal colombiano. En este contexto, se exponen patrones y retos que resaltan la imperiosa necesidad de reforzar la reglamentación legal y los criterios emanados de la jurisprudencia en esta esfera.

Por consiguiente, se deduce que el escrutinio de la prueba digital amerita una aproximación multidisciplinaria que entrelace el derecho, la tecnología y la ciencia forense. Esto con el propósito primordial de asegurar un balance apropiado entre la efectividad probatoria y la salvaguarda de los derechos fundamentales, particularmente el debido proceso, la privacidad y el derecho a la defensa.

BIBLIOGRAFÍA

Agencia Nacional de Defensa Juridica del Estado. (2022). *Mensaje de datos como medio de prueba*. Obtenido de https://www.defensajuridica.gov.co/docs/BibliotecaDigital/Documentos%20compartidos/0729.pdf

Arellano, L., & Castañeda, C. (2012). *La Cadena de Custodia Informático-forense.* medellin: Tecnologico de antioquia institucion universitaria.

Bautista, F., Mosquera, A., Obando, A., & Rios, D. (2021). *Ecidencia digital. Aspectos generales.* Bogotá: Escuela Judicial Rodrigo Lara Bonilla.

BBC News. (29 de 03 de 2016). *¿Cómo logró el FBI desbloquear el iPhone del atacante de San Bernardino y de paso frustrar a Apple?* Obtenido de https://www.bbc.com/mundo/noticias/2016/03/160329_tecnologia_fbi_como_desbloqueo_iphone_san_bernardino_apple_ch

Bigot, M. (2010). *El enfoqe dicotomico del estudio de la lengua.* Buenos Aires: Universidad Nacional de Rosario.

Bujosa, M., Bustamante, M., & Toro, L. (2021). *La prueba digital producto de la vigilancia secreta:obtención, admisibilidad y valoración en el proceso penal en España y Colombia.* Medellin: Universidad de Medellin.

Carpenter vs Estados Unidos, 16-402 (Supreme Court of the Unite States 22 de 06 de 2018).

Chaia, R. (2024). *La prueba digital, T.1 Principios y garantias constitucionales para s aplicacion en el proceso penal en la era digital.* Hammurabi.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia (Convenio de Budapest). ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/18

Constitución Política de Colombia. (1991). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Corte Interamericana de Derechos Humanos. (2024). *Caso Miembros de la Corporación de Abogados José Alvear Restrepo (CAJAR) vs. Colombia. Sentencia de 17 de noviembre de 2024.* San José: Corte IDH

Corte Constitucional de Colombia. (2 de noviembre de 2016). M.P: L. Vargas. *C-604/16:* https://www.corteconstitucional.gov.co/relatoria/2016/c-604-16.htm

Corte Constitucional de Colombia. (12 de marzo de 2021). *M.P : J. Reyes. SU-060 de 2021*. https://www.corteconstitucional.gov.co/relatoria/2021/su060-21.htm

Corte Constitucional de Colombia. (9 de julio de 2005). *M.P : C.Vargas. C-591 de 2005*. https://www.corteconstitucional.gov.co/relatoria/2005/c-591-05.htm

Corte Constitucional de Colombia. (9 de mayo de 2007). *M.P : J. Cordoba. C-336 de 2007*. https://www. https://www.corteconstitucional.gov.co/relatoria/2007/c-336-07.htm

Corte Suprema de Justicia, Sala de Casación Penal. (2025, 29 de enero). *Sentencia SP248-2025 (Rad. 58275)*. Obtenido el 23 de septiembre del 2025. https://archivodigitalapi.cortesuprema.gov.co/share/2025/3/Boletines/SP248-2025%2858275%29.pdf

Constitution. amend. IV. (1791) obtenido el 23 de septiembre del 2025. https://constitution.congress.gov/constitution/amendment-4/

Constitution. amend. V. (1791) obtenido el 23 de septiembre del 2025. https://constitution.congress.gov/constitution/amendment-5/

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523 (1986) United States. Obtenido el 23 de septiembre del 2025. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Fiscalia General de al Nacion. (2025). *Derechos de las Victimas* . Obtenido de https://www.fiscalia.gov.co/colombia/justicia-transicional-2/derechos-de-las-victimas/

Fiscalia General de la Nacion. (2018). *Manual del sistema de cadena de custodia.* Bogotá: Fiscalia General de la Nacion.

Fiscalia General de la Nacion. (2025). *Informe de Gestion 2024-2025.* Bogotá: Fiscalia General de la Nacion.

Gonzalez, J. (2021). *Corte Constitucional aclaró que los pantallazos impresos de WhatsApp tienen el valor de prueba indiciaria*. Obtenido de Instituto colombiano de derecho procesal: https://icdp.org.co/corte-constitucional-aclaro-que-los-pantallazos-impresos-de-whatsapp-tienen-el-valor-de-prueba-indiciaria/

IBM. (07 de 08 de 2025). *interfaces del usuario*. Obtenido de https://www.ibm.com/docs/es/i/7.5.0?topic=applications-user-interfaces

Katz v. United States , 389 U.S. 347 (Supreme Court of the Unite States 18 de 12 de 1967).

Ochoa, P. (2018). *El tratamiento de la evidencia digital, una guia para adquision y/o recopilacion.* Ecuador: Universidad de Cuenca .

Parra, D. (2019). *requisitos juridicos para la validez juridica de la prueba digital.* Bogotá : Universidad Catolica de Colombia.

Pew Researcj Center. (20 de 05 de 2015). *Opiniones de los estadounidenses sobre la recopilación y seguridad de datos*. Obtenido de

https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Riley vs California, 13-132 (Supreme Court of the Unite States 25 de junio de 2014).

Sanabria, R. (7 de 03 de 2021). *Prueba digital en el proceso penal: exclusion de la cadena de custodia*. Obtenido de https://rsanabria.co/2025/03/07/prueba-digital-en-el-proceso-penal-exclusion-cadena-de-custodia-y-la-validez-de-la-version-impresa-sin-codigo-hash/

Silva, J. (2020). La prueba electrónica en el proceso penal acusatorio. *Revista Colombiana de Derecho Procesal*, 15(1), 201-230.

Smith v. Maryland , 442 U.S. 735 (U.S. Supreme Court 20 de 06 de 1979).

Tamayo, L. (01 de 01 de 2024). *Clonado forense y volcado forense de evidencias digitales. importancia del hash en su preservacion.* Obtenido de https://www.linkedin.com/pulse/clonado-forense-y-volcado-de-evidencias-digitales-del-jos%C3%A9-luis-tdqhc/

Universidad de Alcala. (20 de febrero de 2020). *Seminario "tegnologia de la imagen aplicada a la escena del delito" Instituto Universitario de Investigación en Ciencias Policiales*. Obtenido de Universidad de Alcala: https://congresosalcala.fgua.es/imagendelito

Viafirma. (04 de 06 de 2025). *Entidades autorizadas para emitir certificados digitales en Colombia.* Obtenido de https://www.viafirma.com/es/entidades-certificadoras-en-colombia/