Barreras legales, técnicas e institucionales en la judicialización de los delitos informáticos en Colombia A partir de la Ley 1273 del 2009

Isabella Torres Moreno

Mariana Vélez Muñoz

Universidad Autonoma Latinoamericana

Medellín, Antioquia

2025

Universidad Autonoma Latinoamericana

Facultad de derecho

Area Derecho Penal - Monografía de Investigación

Rector: Dr. Jose Rodriguez Florez Ruiz

Decana de la Facultad de Derecho: Dr. Ramón Elejalde Arbelaez

Director de Tesis: Dra. Ana Maria Mesa Elneser

Examinadores:

TABLA DE CONTENIDOS

Agradecimientos de Isabella Torres Moreno

Quiero expresar mi más profundo agradecimiento a quienes han sido parte especial de este camino. Este logro es mío y de todos aquellos que han dejado huella en mi vida porque en cada página está reflejado el amor, el apoyo y la inspiración que me dieron.

A mi mamá, el pilar más grande de mi vida. Su amor incondicional ha sido la fuerza que me sostuvo en cada paso. Con su ejemplo de esfuerzo, entrega y valentía me enseñó que no hay sueño imposible cuando se lucha con el corazón. Todo lo que soy y este logro que hoy celebro se lo debo, en gran medida, a ella, porque en cada página de este camino está reflejado su amor inmenso y el mío hacia ella.

A mi papá, cuya confianza y amor marcaron profundamente mi vida. Sus palabras llenas de aliento y su manera de acompañarme me enseñaron que la verdadera riqueza está en el apoyo sincero y en caminar juntos. Este logro también es suyo, porque en mi corazón y en cada paso de este camino está grabado mi amor hacia él.

Al padre que encontré en la vida y que hoy me acompaña desde el cielo. Toda esta carrera se la debo a él, porque su recuerdo y su ejemplo han sido la fuerza que me impulsó y la inspiración más profunda para no rendirme. Su amor y su presencia viven en mí, y este logro es también suyo, porque cada paso que di lo hice con él en mi corazón.

A mi hermana, por ser compañía en este camino e inspiración. Su pasión en todo lo que hace y la forma en que enfrenta los retos me mostraron que los sueños se cumplen con entrega y valentía. Este logro también es suyo, porque en cada paso sentí su amor, su apoyo y la motivación que me regaló con su ejemplo.

A mi hermano de vida, quien fue compañero en esta carrera. Gracias por caminar a mi lado, compartir alegrías, retos y aprendizajes; su apoyo constante hizo que este proceso fuera mucho más significativo.

A mi tía, mi mejor amiga, porque ha sido una inspiración constante en mi vida. Sus palabras y su apoyo han dejado una huella imborrable en mi formación académica y personal, y gran parte de este logro también se lo debo a ella.

A mi novio, porque siempre caminó a mi lado en este proceso. Su paciencia, sus palabras de aliento cuando sentía que no podía más, y su alegría en cada logro hicieron de este camino una experiencia más llevadera. Él ha sido mi apoyo emocional, recordando con su amor que los sueños compartidos se viven con más fuerza. Gracias por creer en mí incluso en mis dudas.

A Frida, mi perrita, porque ha llenado mis días de calma y felicidad. Ella me enseñó que la fidelidad de un compañero de cuatro patas puede convertirse en la fuerza más pura para seguir adelante

A la Doctora Ana María Mesa Elneser, por su orientación y dedicación para dar forma a este proyecto y a todas las personas que compartieron su tiempo y conocimiento a través de entrevistas, cuyos valiosos aportes enriquecieron profundamente este trabajo.

Y, sobre todo, a Dios, por darme la vida, la sabiduría, la fortaleza y la oportunidad de llegar hasta aquí, confiándome la misión de crecer y de soñar en grande.

Agradecimientos de Mariana Velez Muñoz

Dios, fuente de vida, fortaleza y claridad, por iluminar cada paso de este camino, su presencia silenciosa ha sido constante, me dio claridad en momentos de oscuridad y esperanza en los momentos de cansancio y dudas.

A mi familia, por ser raíz, sostén y refugio, Gracias por acompañarme con su amor incondicional y creer en mí incluso cuando yo dudaba. De manera especial a mi madre quien con su entrega y valentía me han enseñado que los sueños se alcanzan con esfuerzo, constancia y fe. Cada palabra fue energía para continuar y cada gesto muestra de su amor infinito.

A mi abuelo, mi ángel guardián, su recuerdo ha sido compañía silenciosa en los momentos de cansancio, y su amor se logró transformar en fuerza invisible. Celebrando desde el cielo este logro, porque parte de lo que soy es parte de su legado, Él es y seguirá siendo la luz eterna que guía mis pasos recordando que el amor trasciende tiempo y distancia.

A mi novio, por su compañía paciente y silenciosa fueron bálsamo en medio de la presión y el cansancio.

A mis maestros de luz, Tobby y Grecia, que con sus miradas sinceras y la nobleza de su compañía me recuerdan la importancia de las pequeñas cosas, que la vida se alimenta de sencillez, su silencio se convirtió en refugio y sus miradas llenas de amor, fueron fuerzas para continuar en los dias mas dificiles.

A la doctora Ana María Mesa, directora de este trabajo, por su guía sabia, fortaleciendo el contenido académico de esta investigación, por disposición y compromiso para que este proyecto pudiera culminar con éxito y a las personas que participaron en las entrevistas aportando voces y perspectivas que dieron vida y sentido a este trabajo.

Este logro no es solo mío, es el reflejo de amor infinito de presencias visibles e invisibles que me acompañaron con amor y esperanza, cada gesto se convirtió en una fuerza que me permitió llegar hasta aquí. A todos ellos gracias por ser parte de este viaje. Este logro. es tan mío como de ustedes.

INTRODUCCIÓN

A lo largo de la historia, el ser humano ha experimentado una constante evolución, desarrollando ideas e inventos que han transformado la forma en que vivimos. Estos avances han tenido como propósito principal facilitar las actividades cotidianas y mejorar la calidad de vida. Sin embargo, no todos los inventos se utilizan exclusivamente para fines positivos; en algunos casos, su mal uso puede poner en peligro la integridad humana, y no es una excepción la informática, el internet y los avances tecnológicos que ocurren día a día.

En el ámbito de los sistemas informáticos, este fenómeno no es diferente. Cada día, estamos más inmersos en la tecnología, lo que ha transformado profundamente nuestras dinámicas sociales. La convivencia familiar ha disminuido, los niños han dejado de jugar en las calles, y muchas personas pasan gran parte de su tiempo frente a una pantalla. Aunque la tecnología ha facilitado innumerables aspectos de nuestra vida, también ha generado desafíos en nuestras relaciones y en la forma en que nos conectamos como sociedad, desde temprana edad los niños saben manipular aparatos electrónicos ¿pero sabrán estos darles un buen uso y ser consciente del impacto de la tecnología en la era digital?

En este contexto, durante la Guerra Fría, una época marcada por la competencia tecnológica y militar entre Estados Unidos y lo que era la antigua Unión Soviética, nació uno de los avances más significativos: ARPANET. El 1 de diciembre de 1969, la Advanced Research Projects Agency (ARPA), perteneciente al Departamento de Defensa de los Estados

Unidos, materializó este proyecto con el objetivo de facilitar el intercambio de información entre agentes involucrados en misiones estratégicas.

Para garantizar la eficiencia de ARPANET, se planteó la necesidad de desarrollar un sistema operativo que permitiera el acceso remoto desde cualquier parte del mundo. Esto condujo a la idea de implementar una red inalámbrica, la cual permitiría un acceso más ágil y versátil, ampliando significativamente su alcance y utilidad, pero a su vez está idea permitía a los ciberdelincuentes a acceder a estas redes con mayor facilidad.

Pero no todo fue como se tenía planeado, en 1988 fue liberado el gusano morris, el primer gusano informático de la historia creado por Robert Tappan Morris este era un estudiante de Cornell este gusano atacó a 6.000 computadoras las cuales estaban conectadas a ARPANET están estuvieron infectadas por más de 72 horas, Según su creador Robert Tappan Morris el objetivo de este gusano el cual lleva por nombre su apellido era comprobar el tamaño de la internet, usando técnicas, su sistema operativo buscaba usar técnicas que lograra descifrar contraseñas con el fin de buscar fallas en los sistemas operativos. (Jesús Audelo González, Héctor Pérez Meana y Pedro Guevara López, 2015)

En Colombia este contexto no es desconocido, si bien no se tiene un registro exacto de cuál fue el primer ataque cibernético que sufrió ya que no hay un registro detallado y completo del inicio de la era digital; Uno de los más recientes informes de Fortinet que es una empresa de ciberseguridad originada en los estados unidos con sede en california, informa que en el primer semestre de 2023 se presentaron más de 5.000 millones de intentos de ciberataque ,o que la ubica a nivel Latinoamérica en el cuarto país con más problemas de seguridad a nivel informático. En el estudio de ciberseguridad realizado por Fortinet se

registra que cada 8 minutos se presenta la denuncia de delitos contenidos en la ley 1273 de 2009.

Estos datos evidencian que, si bien la tecnología ha representado a lo largo de la historia una herramienta invaluable en materia de comunicación, optimización de procesos y eficiencia laboral, su uso no siempre se enmarca en principios éticos y legales. La indebida utilización de los avances tecnológicos por parte de ciertos individuos o grupos pone de manifiesto la necesidad imperiosa de fortalecer los marcos normativos y los mecanismos de control que regulan su implementación, con el fin de mitigar riesgos asociados a su uso indebido.

En este panorama, se evidencia que la rápida expansión de los delitos informáticos ha superado la capacidad de respuestas del sistema jurídico colombiano y que pese a la existencia de la Ley 1273 de 2009 que fue agregado al marco jurídico establecido en la ley 906 de 2004, la judicialización de este tipo de conductas enfrenta múltiples obstáculos que va desde lo técnico hasta lo legal por la alta complejidad técnica en la evidencia digital, especialización de operadores jurídicos. Reflejando un problema técnico-jurídico vulnerando derechos fundamentales. que va desde la vulneración a los datos personales hasta afectación en el patrimonio económico, lo cual exige respuestas más efectivas por parte del estado.

Desde la perspectiva académica, este estudio se enmarcará en el Derecho penal contemporáneo, que enfrenta un reto de adecuar sus criterios dogmáticos, procesales y sustanciales para adaptarse a las nuevas formas de criminalidad.

PLANTEAMIENTO DEL PROBLEMA

La criminalidad informática o también conocido como el cibercrimen ha evolucionado de una manera abismal ya que la tecnología está en constante crecimiento; esto ha generado desafíos para los sistemas jurídicos adaptándose a contextos actuales, En Colombia la ley 906 de 2004 se adopta al sistema penal acusatorio, este sistema penal acusatorio se ha regido por principios bases como la oralidad, inmediación y contradicción estos son los que van a regir la actuación penal; No obstante, en la vida cotidiana las víctimas del cibercrimen se enfrentan con obstáculos jurídicos que no les permitan logran que las denuncias lleguen a la etapa de juicio oral ya sea para obtener una sentencia condenatoria o absolutoria.

Uno de los principales obstáculos a los que se enfrentan es el alto nivel de complejidad probatoria que es inherente a este tipo de delitos; una primera barrera es la identificación y judicialización de los responsables ya que la misma se ve obstaculizada por la naturaleza misma de estos delitos a diferencia del resto de tipos penales, en los que el agresor suele tener una identidad visible en el ámbito digital el victimario no siempre posee una cara visible. El anonimato, es un ente característico de estas agresiones; adicionalmente la admisibilidad de los elementos materiales probatorios se ven en peligro ya que la misma está sujeta a modificaciones y la verificación de la autenticidad de la misma, lo que puede comprometer su incorporación al proceso.

A esta problemática se le suma la falta de personal especializado materia de delitos informáticos dentro de la rama judicial los entes encargados de la investigación y posterior judicialización de los posibles responsables de estas agresiones redunda en las falencias en recopilación, análisis y posterior incorporación de la prueba digital a los procesos judiciales

La dilatación de las etapas procesales, la congestión judicial en la que se encuentra Colombia y la priorización de otros delitos con “MAYOR RELEVANCIA SOCIAL”

terminan agravando el problema, generando impunidad y desconfianza por parte de las víctimas de estos delitos respecto a la justicia penal.

En este contexto, resulta imperativo analizar de manera crítica cuáles son las principales dificultades técnicas, legales e institucionales que enfrentan las víctimas de delitos informáticos en Colombia para que sus denuncias sean efectivamente judicializadas y culminen en la etapa de juicio oral con una sentencia, en el marco del procedimiento establecido por la Ley 906 de 2004.

PREGUNTA DE INVESTIGACIÓN: ¿Cuáles son las causas técnicas y legales que evidencian las dificultades en el proceso penal en primera instancia para la investigación y judicialización de los delitos informáticos a partir de la ley 906 de 2004?

OBJETIVO GENERAL: Establecer las dificultades legales y técnicas que enfrentan las víctimas de delitos informáticos en Colombia, para la investigación y judicialización del delito desde la presentación de la denuncia hasta la etapa de sentencia en el juicio oral de primera instancia.

OBJETIVOS ESPECÍFICOS:

1. Describir las etapas del proceso penal aplicable a los delitos informáticos en Colombia con miras a establecer las dificultades legales que surgen en el desarrollo de la investigación y judicialización.
2. Identificar y describir las herramientas técnicas y jurídicas actualmente admisibles en el ordenamiento colombiano para la recolección, preservación y análisis de evidencia digital en la investigación penal de delitos informáticos, con base en la Ley 906 de 2004 y los estándares internacionales aplicables.

3. Establecer, desde la perspectiva de los actores del proceso penal —jueces, fiscales, defensores e investigadores—, las principales dificultades técnicas, jurídicas, institucionales y de recurso humano que afectan la etapa de investigación y el juicio oral en los delitos informáticos, evidenciando las coincidencias y tensiones que emergen entre sus roles, prácticas y comprensiones del fenómeno delictivo en entornos digitales.

MARCO TEÓRICO

Delitos informáticos y su impacto en la sociedad

Los delitos informáticos han evolucionado rápidamente, causando impacto tanto en personas como en empresas y entidades gubernamentales. Para hacer frente a esta problemática, Colombia incorporó a su Código Penal diversas conductas delictivas relacionadas con el uso indebido de las tecnologías de la información y las comunicaciones a través de la Ley 1273 de 2009. Con esta normativa, se buscó responder al crecimiento de la ciberdelincuencia y establecer un marco legal que permitiera su persecución y sanción.

Entre estas se encuentran el acceso abusivo a sistemas informáticos, la violación de datos personales, la interceptación de datos y la suplantación de identidad (Congreso de la República de Colombia, 2009).

La dimensión transnacional del fenómeno ha impulsado la adopción de marcos internacionales de cooperación; la Convención de Budapest sobre Ciberdelincuencia (Council of Europe, 2001) establece parámetros para la tipificación, la preservación de evidencia digital y la cooperación judicial entre estados, lo que obliga a los países a armonizar prácticas y procesos para enfrentar ataques que suelen trascender jurisdicciones. (Council of Europe, 2001).

Diferentes estudios han intentado clasificar estos delitos. Por ejemplo, Gómez Restrepo y Bermúdez Durana (2010) los separan en dos categorías: aquellos que atentan directamente contra la seguridad informática y aquellos en los que la tecnología es un medio para cometer otros delitos, como la estafa en línea. Sin embargo, con el paso del tiempo, actualmente esta clasificación ha evolucionado y ha tenido que adaptarse a riesgos emergentes, como el ciberacoso, la sextorsión y el fraude digital.

Uno de los casos más impactantes de delitos cibernéticos en Colombia fue el de Los Troyanos, una organización delictiva desmantelada en noviembre de 2021. Este fue un grupo que logró infiltrarse en los sistemas informáticos de 41 alcaldías de distintas regiones del país, desviando más de 12.000 millones de pesos a través de transferencias fraudulentas. Usando software malicioso y técnicas avanzadas de acceso no autorizado, burlaron los controles de seguridad y operaron sin ser detectados durante un largo tiempo.

Lo más preocupante de este caso no fue solo la magnitud del hurto, sino la facilidad con la que lograron vulnerar los sistemas financieros de instituciones públicas. Durante meses, fondos destinados a infraestructura, salud y programas sociales fueron desviados sin que las víctimas advirtieran el fraude a tiempo.

La investigación de la Fiscalía permitió la captura de 29 de los 52 integrantes en operativos simultáneos en Bogotá, Valledupar, Cesar y La Guajira. Sin embargo, el caso expuso la falta de protocolos de ciberseguridad en las entidades estatales y las dificultades para rastrear y judicializar este tipo de delitos en el país.

Protección de las víctimas en el marco normativo colombiano

En Colombia, además de la Ley 1273 de 2009, existen más normativas con el fin de proteger a las víctimas de delitos informáticos. Un ejemplo de esto es la Ley 1581 de 2012,

que regula el tratamiento de datos personales y permite a los ciudadanos solicitar la rectificación o eliminación de su información en caso de uso indebido.

A pesar de estos avances, Dávila Suancha (2021) manifiesta y advierte que una de las más grandes dificultades en cuanto a la persecución de estos delitos es lo complicado que se hace identificar a los responsables, especialmente cuando actúan desde otros países o emplean técnicas sumamente avanzadas para ocultar su identidad. Esto nos permite identificar la importancia de reforzar la cooperación internacional y fortalecer la capacidad técnica de las autoridades para rastrear y judicializar a los ciberdelincuentes.

Un problema recurrente es la baja tasa de denuncias por parte de las víctimas. Una gran cantidad de personas que han sido afectadas por delitos como el robo de identidad o la difusión no autorizada de contenido íntimo no acuden a las autoridades por desconocimiento de cómo funcionan los procedimientos o por miedo a consecuencias como hostigamiento o que su privacidad se vea vulnerada nuevamente. Lo que sugiere que, además de mejorar el marco legal, se requiere una difusión mucho mayor de información sobre los derechos de las víctimas y los canales de denuncia disponibles en el país.

Consecuencias de los delitos informáticos en las víctimas

Las afectaciones a las víctimas respecto a estos delitos pueden ser económicas, psicológicas y sociales, resultando en muchos casos igual o incluso más graves que en otros delitos debido a la permanencia y el alcance de los crímenes informáticos. A diferencia de un delito común, sus efectos en la mayoría de los casos suelen ser inmediatos y localizados, mientras que los delitos cibernéticos pueden prolongarse en el tiempo. Además, en el ámbito emocional, Castañeda (2019) señala que muchas víctimas de ciberacoso o sextorsión sufren altos niveles de estrés, ansiedad e incluso depresión. Siendo tan grandes en los casos más

graves que puede llevar al aislamiento social o, en situaciones extremas, a intentos de autolesión.

En el ámbito financiero, el fraude digital y el robo de identidad pueden tener consecuencias devastadoras. López y Suárez (2021) señalan que muchas personas han visto comprometidos sus ahorros y su estabilidad económica debido a ataques cibernéticos, sin que las instituciones bancarias siempre ofrezcan respuestas de manera rápida o lo suficientemente eficaces.

A nivel reputacional, la difusión no autorizada de información personal o imágenes íntimas puede tener consecuencias devastadoras para las víctimas, incluyendo discriminación laboral, estigmatización social e incluso amenazas contra su integridad (Ministerio de Tecnologías de la Información y las Comunicaciones, 2021). El caso de Mariana González evidencia esta problemática. Ella, una comunicadora social y periodista de Bogotá, decidió probar una aplicación de citas para conocer nuevas personas. Allí entabló conversación con un hombre que, tras ganarse su confianza, la manipuló para obtener material íntimo. Después, comenzó a amenazarla con compartir este contenido y creó perfiles falsos en redes sociales para enviarlo a sus contactos y familiares. La situación escaló hasta el punto de recibir amenazas de muerte, demostrando el profundo impacto que estos delitos pueden tener en la vida de las víctimas.

Derechos fundamentales y la lucha contra la ciberdelincuencia

Un aspecto complejo respecto a la prevención y persecución de los delitos informáticos es lograr establecer un equilibrio entre la seguridad y la protección de los derechos fundamentales. Siendo la privacidad y la libertad de expresión fundamentales teniendo en cuenta que deben garantizarse de manera conjunta.

A nivel internacional, la Convención de Budapest sobre Ciberdelincuencia brinda un marco para que los países trabajen juntos en la investigación y persecución de estos delitos sin afectar derechos fundamentales (Consejo de Europa, 2001). En línea con este compromiso, Colombia ha adoptado diversas estrategias para mejorar la identificación y judicialización de los ciberdelincuentes (OEA, 2022).

Etapas procesales en la judicialización de los delitos informáticos en Colombia

La persecución judicial de los delitos informáticos en Colombia se enfrenta con múltiples obstáculos en cada una de las etapas del proceso penal que se encuentran reguladas por la ley 906 de 2004, desde la formulación de la denuncia las víctimas se encuentran con un principal obstáculo la individualización y la tipicidad del delito, en la investigación existe la gran brecha que es la individualización de la presunta persona que comete el delito ya que estos delitos se cometen desde el anonimato adicionalmente estos delitos son transnacionales lo que exige una cooperación internacional que al día de hoy no es suficiente, pero los obstáculos continúan; en la imputación no se logra imputar de manera adecuada el tipo penal sin todavía mencionar la evidencia que puede ser debatida por la defensa ya que este tipo de elementos materiales probatorios cuentan con una alta complejidad para que conserve su autenticidad, Posteriormente en la audiencia de acusación y las audiencias preparatorias la fiscalía debe sustentar la teoría del caso ya que en ocasiones carece de elementos materiales probatorios por la falta de capacitación a los auxiliares de la justicia, finalmente ya nos encontramos en la etapa del juicio oral en donde la valoracion de la prueba enfrenta grandes cuestionamientos debido a la naturaleza de la misma lo que podria debilitar la carga probatoria debido a la falta o conservacion de autenticidad de la misma; En consecuencia, la falta de especialización en cibercriminalidad, la insuficiencia de herramientas tecnológicas y

la alta carga procesal limitan el acceso efectivo a la justicia para las víctimas de estos delitos (Ley 906 de 2004).

DISEÑO METODOLÓGICO

Esta investigación cuenta con un enfoque mixto, combinando el análisis cualitativo y cuantitativo para comprender el marco legal colombiano sobre delitos informáticos y su efectividad en la protección de las víctimas. Se trata de un estudio descriptivo y exploratorio que examina la normativa vigente y, al mismo tiempo, analiza las dificultades que enfrentan las víctimas al denunciar estos delitos y acceder a la justicia.

Además, se consultarán fuentes secundarias como artículos académicos, informes de organismos internacionales entre ellos la OEA e INTERPOL y estudios previos sobre la protección de las víctimas de delitos cibernéticos en Colombia y otros países.

El estudio incorpora un análisis cuantitativo de las denuncias presentadas, utilizando las cifras disponibles en los datos abiertos de la Fiscalía General de la Nación. Esto permitirá identificar patrones en la judicialización de los delitos informáticos y también evaluar qué tan lejos se logra avanzar estos casos dentro del sistema de justicia.

Para tener una visión más clara y cercana a la realidad, se examinará el proceso judicial por etapas procesales, desde el momento en que la víctima interpone la denuncia hasta la posible sanción del responsable. Se prestará especial atención a las dificultades que enfrentan las víctimas en cada fase, con el propósito de entender cómo funciona realmente el

sistema para ellas y hacer visibles las barreras que pueden impedirles acceder a la justicia y recibir una protección efectiva.

CAPÍTULO I

ETAPAS DEL PROCESO PENAL ACUSATORIO Y EVOLUCIÓN ESTADÍSTICA DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

1.1 Introducción

Este capítulo examinará cómo se comporta el proceso penal acusatorio en Colombia frente a los delitos informáticos, considerando las particularidades de esta criminalidad en cada una de sus fases procesales. A partir del marco normativo previsto en la Ley 906 de 2004, abordando los momentos clave del procedimiento para identificar los puntos donde surgen barreras jurídicas, operativas e institucionales que afectan el curso de las investigaciones y la posibilidad de avanzar hacia una decisión judicial.

Enfocándonos en observar cómo las exigencias técnicas propias de este tipo de delitos y las limitaciones estructurales del sistema, impactan la aplicación práctica del modelo procesal. Cada etapa es estudiada desde una perspectiva normativa, pero también se expone su aplicación en la práctica a partir de las estadísticas disponibles para delitos y una lectura jurídica y también cuantitativa, que permite observar tendencias, estancamientos y retrocesos en la trazabilidad procesal de las denuncias.

Los gráficos procesales muestran cómo, en la mayoría de los casos, las investigaciones por delitos informáticos se concentran en la etapa preliminar sin avanzar significativamente hacia fases más decisivas como la investigación formal, el juicio oral o la ejecución de la pena. Lo cual permite observar la existencia de patrones persistentes de ineficacia procesal, que obstaculizan la judicialización efectiva y que, en muchos casos, dejan a las víctimas sin respuestas jurídicas de fondo.

A nivel regional, investigaciones recientes demuestran que la problemática colombiana no es un caso aislado. En varios países latinoamericanos los delitos informáticos también muestran tasas bajas de judicialización, influenciadas por factores tecnológicos, regulatorios y sociales que limitan la capacidad de respuesta estatal (Variables asociadas a los delitos informáticos en Latinoamérica, 2024).

Por tanto, se ofrece una radiografía crítica de las limitaciones que enfrenta el sistema penal cuando se enfrenta a conductas delictivas cometidas mediante tecnologías de la información buscando evidenciar las etapas del proceso y los puntos de ruptura donde se debilita la ruta hacia una sentencia condenatoria. Así, se sientan las bases para una reflexión más profunda sobre la necesidad de adaptar el aparato judicial a lo que plantea el cibercrimen en Colombia, en función de garantizar el acceso efectivo a la justicia.

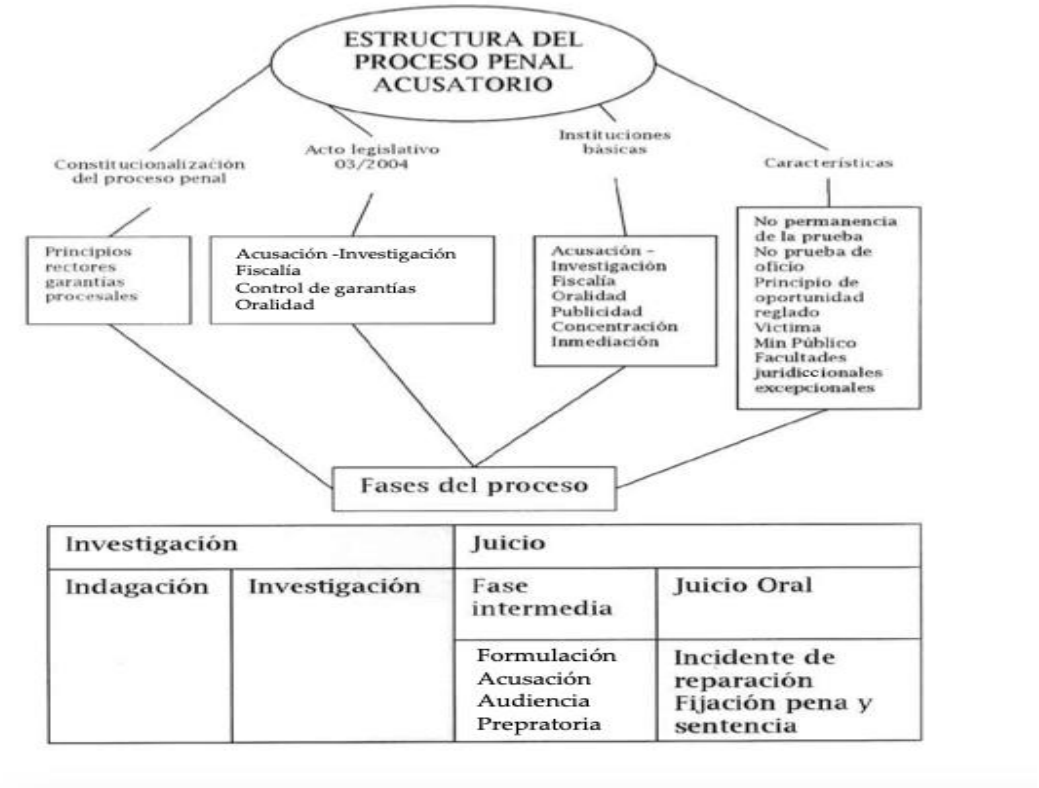
El proceso penal en Colombia enmarcado en la ley 906 del 2004 también conocido como el código de procedimiento penal colombiano, es un sistema penal acusatorio establecido por el acto legislativo No 03 del 19 de diciembre del 2002; en el cual este hace referencia

> *El nuevo modelo acusatorio es un sistema de partes, según el cual, el imputado ya no es un sujeto pasivo en el proceso, como lo era bajo el modelo inquisitivo, sino que demanda su participación activa, incluso desde antes de la formulación de la*

> *imputación de cargos. Por lo que, sin considerar una inversión de la presunción de inocencia, las cargas procesales se distribuyen entre la Fiscalía y el investigado, imputado o procesado a quien le corresponde aportar elementos de juicio que permitan confrontar los alegatos del acusador, e inclusive los aportados por la víctima a quien también se le permite la posibilidad de enfrentar al imputado.* (Corte Constitucional de Colombia, 2005)

Hace 25 años el derecho penal fue reformado de una manera estructural que correspondía a nuevas teorías del derecho germano aplicando un positivismo naturalista; uno de los cambios más significativos fue cambiar el derecho penal de autor por el derecho penal de acto; El sistema penal acusatorio nos divide el proceso en dos etapas; la etapa de investigación que se encuentra subdividida en la etapa de indagación e investigación y la etapa del juicio subdividida en la fase intermedia y el juicio oral; cada una de estas etapas tienen un objetivo diferente pero que todas conducen a un mismo fin que es dar por finalizado un proceso con una sentencia condenatoria o absolutoria.

Figura 1.



Fuente: Fiscalía General de la Nación, Estructura del proceso penal acusatorio.

l.2 Etapa de investigación

1.2.1. Indagación

La fase de indagación, también denominada etapa preliminar del proceso penal, tiene como finalidad verificar la existencia de elementos materiales probatorios, evidencia física o información legalmente obtenida que permitan inferir razonablemente la comisión de una conducta punible y, así mismo, identificar a los posibles autores o partícipes; esta etapa, por disposición legal y constitucional, es de competencia de la Fiscalía General de la Nación, que la dirige y coordina con el apoyo funcional de los cuerpos de Policía Judicial. Se distingue por su carácter reservado, no contradictorio y estrictamente preliminar, en tanto se encuentra orientada a la verificación de los hechos sin que aún exista una imputación formal.

Esta fase procesal se activa con la recepción de una noticia criminal, la cual puede ser conocida a través de distintos medios tales como la querella, la petición especial o de manera oficiosa. Una vez se tenga conocimiento de dicha noticia, debe registrarse su iniciación de

forma inmediata y a través de un medio expedito, momento en el cual el fiscal del caso asumirá la dirección, coordinación y control jurídico de la actuación procesal.

En desarrollo de esta fase, se adelantan diversas diligencias investigativas como entrevistas a testigos, inspecciones judiciales, informes periciales, análisis forenses, así como interceptaciones de comunicaciones, entre otros actos de investigación. Es importante destacar que ciertas diligencias requieren control judicial, ya sea previo o posterior, dependiendo de la naturaleza del acto. Este control es competencia exclusiva del juez de control de garantías.

Dentro de las primeras treinta y seis (36) horas siguientes al inicio de la actuación, el fiscal deberá elaborar un informe ejecutivo, en el cual se consignen los resultados preliminares de las diligencias practicadas y el estado inicial del caso.

La trascendencia jurídica de esta etapa radica en determinar la viabilidad de formular imputación, conforme a los elementos que han sido recaudados. La duración de la indagación estará sujeta a la obtención de elementos probatorios suficientes que permitan sustentar una inferencia razonable de autoría o participación. En caso de que la actividad investigativa no arroje un nivel mínimo de persuasión jurídica, la actuación podrá prolongarse hasta tanto no opere la prescripción de la acción penal.

Finalmente, es de advertir que, en la etapa de indagación, la competencia para el ámbito de delitos informáticos se encuentre delegada en un fiscal especializado, quien asume la dirección y coordinación de todas las funciones y actividades que realizarán la Policía Judicial. Está, a su vez, se encuentra delegada de manera permanente en la Policía Nacional

La estructura que respalda la investigación de los delitos informáticos está compuesta por diversas dependencias de la Fiscalía General de la Nación, entre las cuales se destacan: La Fiscalía Delegada contra la Criminalidad Organizada, La Dirección Especializada contra los Delitos Informáticos, La Dirección Especializada contra las Organizaciones Criminales, La Fiscalía Delegada para las Finanzas Criminales, La Dirección de Apoyo a la Investigación y Análisis contra la Criminalidad Organizada, Las Fiscalías de Investigaciones Priorizadas, adscritas a la Dirección del Cuerpo Técnico de Investigación (CTI), La Unidad de Fiscalía

para la Protección de Datos Personales, Las Fiscalías de Estructura de Apoyo. (Fiscalía general de la nación, 2021)

En cuanto a la articulación con los organismos de Policía Judicial, intervienen los siguientes grupos y funcionarios especializados: Grupos Investigativos contra los Delitos Informáticos, Grupos Investigativos contra los Delitos Informáticos adscritos a la Dirección del Cuerpo Técnico de Investigación (CTI), Funcionarios de la Policía Judicial adscritos a la Seccional de Investigación Criminal (SIJIN), Funcionarios de la Policía Judicial (DIJIN), Miembros de la Policía Nacional destacados en las estructuras de apoyo, Funcionarios asignados a las estructuras de apoyo. (Fiscalía general de la nación, 2021)

1.2.2. Investigación

Esta etapa constituye la primera fase procesal formal que tendrá como finalidad fortalecer el acervo probatorio que sirvió de fundamento para la formulación de la imputación, con el fin de estructurar una teoría del caso sólida que permita sustentar una acusación formal contra los presuntos autores o partícipes de la conducta punible investigada.

Para que proceda la presentación del escrito de acusación, deben concurrir elementos materiales probatorios, evidencia física o información legalmente obtenida que permitan inferir razonablemente tanto que una conducta encaje en un tipo penal como la responsabilidad del imputado. Es decir, se requiere un estándar probatorio suficiente para justificar el paso a la etapa del juicio.

Durante esta fase, el proceso puede tomar distintos rumbos procesales. En primer lugar, si se verifica la existencia de alguna de las causales de terminación de la actuación previstas en el artículo 333 de la Ley 906 de 2004, la investigación podrá concluir mediante preclusión. En segundo lugar, si concurren las causales contempladas en el artículo 324 de la misma normatividad, podrá procederse a la suspensión, interrupción o renuncia de la acción penal, según corresponda.

La etapa de investigación formal se inicia con la formulación de imputación y se extiende hasta la presentación del escrito de acusación, la solicitud de preclusión o la

aplicación de un principio de oportunidad. El término procesal para adoptar cualquiera de estas decisiones es de treinta días, contados a partir de la formulación de imputación. En caso de que el fiscal no adopte ninguna medida dentro de este término, pierde la competencia sobre el caso, y deberá ser designado un nuevo fiscal. Si este segundo fiscal tampoco actúa dentro del término establecido es decir los 30 días, se configurará una causal de preclusión por vencimiento de términos.

l.3 Juicio

l.3.l. Formulación de la acusación

En esta fase la Fiscalía presentó un escrito ante el juez de conocimiento donde identifica los hechos, la calificación jurídica y las pruebas que respaldan esta acusación para que las partes conozcan de manera clara el objeto del juicio y preparar su intervención. Este escrito debe tener precisión sobre la teoría del caso del ente acusador para poder delimitar el debate que se desarrollará posteriormente en juicio y garantizar que el acusado tenga pleno conocimiento del contenido de la imputación que enfrentará.

La audiencia de formulación de acusación tiene lugar luego de la radicación del escrito y cumple varias funciones procesales. Se verifica que se hayan cumplido los requisitos legales del acto de acusar, se reconoce formalmente al imputado como acusado y se activa la etapa del juicio oral. A partir de este momento, se consolidan las garantías que rigen esta fase del proceso, como el derecho a la contradicción, a la defensa técnica y a participar activamente en el debate público y oral. Esta transición marca un cambio sustancial en el rol procesal del imputado, quien ahora debe enfrentar una acusación estructurada, con base en elementos de convicción previamente conocidos.

Durante este momento el juez también valida que las pruebas propuestas se ajusten a lo que está legalmente permitido, lo cual garantiza que las pruebas cumplan con los principios

de legalidad y pertinencia, y que no se introduzcan elementos que puedan afectar el desarrollo equilibrado del juicio porque reduce el riesgo de controversias improcedentes en la etapa oral. Da lugar también a que las partes comiencen a preparar su estrategia de juicio en igualdad de condiciones.

La normatividad vigente establece un plazo de treinta (30) días para realizar esta audiencia, contados desde la presentación del escrito. Para asegurar la continuidad del proceso, evitar dilaciones y proteger los derechos tanto del acusado como de la sociedad. En caso de inactividad injustificada por parte del fiscal, se pierde competencia y el caso debe ser reasignado, de acuerdo con lo dispuesto en el Código de Procedimiento Penal.

Es importante señalar en esta etapa procesal que la competencia para conocer de este tipo de delitos es de los jueces penales municipales, conforme a lo que establece el artículo 37, numeral 6 del Código de Procedimiento Penal. Dicho numeral dispone que este será competente cuando se trate de los delitos contemplados en el Título VIII Bis del mencionado código. Este juez será el encargado de culminar las demás etapas procesales hasta la culminación del proceso penal ya sea con las sentencia o si hay lugar a incidente de reparación integral.

1.3.2 Audiencias preparatorias

La audiencia preparatoria permite depurar el juicio, ordenar el debate probatorio y asegurar que la etapa oral se adelante bajo condiciones de legalidad, equilibrio procesal y claridad argumentativa. Su realización está regulada por el artículo 357 y siguientes del Código de Procedimiento Penal y se lleva a cabo después de la formulación de la acusación.

La audiencia comienza con la verificación del descubrimiento probatorio, es ahí donde el juez constata que la Fiscalía ha puesto a disposición de la defensa todos los elementos materiales de prueba, evidencia física e información obtenida durante la investigación para

garantizar que la defensa pueda preparar su intervención en juicio de manera efectiva, protegiendo así el principio de contradicción.

Una vez cumplida esta etapa, cada una de las partes debe presentar su solicitud de pruebas. En esta fase procesal se indican cuáles serán los elementos probatorios que se pretenden hacer valer durante el juicio y se justifica su pertinencia, conducencia y utilidad. Además, se pueden proponer estipulaciones probatorias, que son acuerdos entre las partes sobre hechos no controvertidos, con el objetivo de evitar la práctica de pruebas innecesarias y centrar el juicio en los aspectos sustanciales del conflicto penal.

Después, el juez realiza el control de legalidad sobre las pruebas ofrecidas. Revisa su origen, su adecuación al objeto del proceso y su utilidad para esclarecer los hechos, y decide sobre su admisión, exclusión o práctica especial para delimitar cuáles serán los elementos probatorios que se practicarán durante el juicio oral y cuál será su forma de incorporación.

Durante esta audiencia también se resuelven cuestiones incidentales que puedan obstaculizar o entorpecer el avance del proceso, tales como nulidades, impedimentos, recusaciones o solicitudes especiales que hayan sido formuladas por las partes.

Finalmente, el juez deja en firme el listado de pruebas admitidas que serán practicadas en el juicio oral y adopta las medidas necesarias para garantizar su realización, tales como definir fechas, establecer prioridades en la práctica probatoria, resolver sobre protección a testigos o disponer del uso de medios tecnológicos.

1.3.3 Juicio oral

En el desarrollo de la audiencia de juicio oral se inicia con las declaraciones de las partes, lo que comúnmente se conoce como la presentación de la teoría del caso. Tanto la Fiscalía General de la Nación como la defensa tienen la oportunidad de presentar su versión

de los hechos, estructurada desde una perspectiva fáctica y narrativa. Esta etapa permite a cada parte establecer las bases argumentativas sobre las cuales sostendrán su postura tanto de culpabilidad como de absolución en el transcurrir del juicio.

Una vez concluidas las teorías del caso se da paso a la práctica de pruebas, iniciando con los interrogatorios directos, re-directos **y** contrainterrogatorios a los testigos. El orden en esta fase está determinado por el principio de carga de la prueba, por lo cual el ente acusador interviene primero, seguido por la defensa; es decir primero se interrogarán a los testigos solicitados por la fiscalía y posteriormente los que fueron solicitados por la defensa. Durante esta etapa, el juez de conocimiento también examinará las pruebas documentales, periciales y materiales que fueron recolectados en el transcurrir del proceso a las cuales les asignará el valor probatorio correspondiente conforme a los criterios legales y jurisprudenciales aplicables a cada prueba en concreto.

Finalmente, una vez culminada la práctica de todas las pruebas admitidas, la Fiscalía procede a presentar sus alegatos de conclusión, en los que realiza un análisis valorativo del material probatorio, con el fin de tipificar la conducta punible que previamente fue objeto de la formulación de la acusación buscando así demostrar la culpabilidad del acusado Posteriormente, la defensa expondrá sus alegatos finales, orientados a refutar los argumentos de la parte acusadora, desvirtuar la imputación y, en su caso, solicitar la absolución.

1.3.4 Fijación de pena y sentencia

Una vez concluida la práctica de pruebas, el juez procederá a emitir el sentido del fallo, el cual deberá ser pronunciado de manera oral y pública dentro de la audiencia, este deberá de referirse a cada una de las solicitudes hechas en los alegatos de conclusión. En garantía del debido proceso, debe estar sustentada en razones fácticas y jurídicas debidamente expuestas. Por lo tanto, todas las providencias de carácter interlocutorio según los

pronunciamientos de las altas cortes deben expresar con claridad los fundamentos que motivan la decisión adoptada por el juez.

Esta audiencia se encuentra estrechamente relacionada con la audiencia de individualización de la pena y sentencia. En caso de que el sentido del fallo sea condenatorio, tanto la Fiscalía General de la Nación como la defensa podrán intervenir para referirse a aspectos relevantes del condenado, como sus condiciones personales y familiares, sus antecedentes penales si estos tuviesen lugar y otros factores estos podrán influir de manera significativa en la dosificación de la pena esto dado cumplimiento al artículo 447 del Código de Procedimiento Penal. Por el contrario, si la decisión es absolutoria, el juez de conocimiento deberá ordenar de manera inmediata que se adopten todas las medidas necesarias para que el procesado sea puesto en libertad.

1.3.5 Incidente de reparación

El incidente de reparación integral constituye un acto procesal mediante el cual se busca materializar los derechos de las víctimas estos son: verdad, justicia y reparación dentro del proceso penal, una vez el juez de conocimiento profiere sentencia condenatoria, la víctima, el fiscal o el Ministerio Público podrán solicitar la apertura del incidente, con el fin de que se determine la forma en que serán resarcidos los perjuicios y daños derivados la conducta punible.

Cabe destacar que en esta acción procesal podrán intervenir terceros civilmente responsables, los cuales podrán ser llamados al proceso por la víctima o por el condenado, en la fase de apertura del incidente. La presencia de estos terceros tiene como finalidad

determinar su responsabilidad patrimonial para responder por los daños causados en atención a la comisión del delito.

Esta solicitud debe ser presentada dentro del término de treinta días hábiles siguientes a la ejecutoria del fallo, es decir, una vez se hayan agotado las etapas procesales correspondientes.

Emitido el fallo condenatorio, el juez de conocimiento es decir el que llevó a cabo todo el proceso penal desde la formulación de la acusación hasta la emisión del fallo deberá convocar a audiencia pública denominada apertura del incidente de reparación integral dentro de los ocho días siguientes a la emisión del fallo de responsabilidad penal, en la cual la víctima deberá formular de manera oral su pretensión indemnizatoria, señalando la modalidad de reparación solicitada manifestando si esta indemnización es meramente económica o no y las pruebas que pretende hacer valer en el proceso, Es sumamente importante expresar que si esta es meramente monetaria SÓLO la víctima podrá darle apertura al incidente no tendrá legitimación en la causa por activa ni el ministerio público ni la fiscalía.

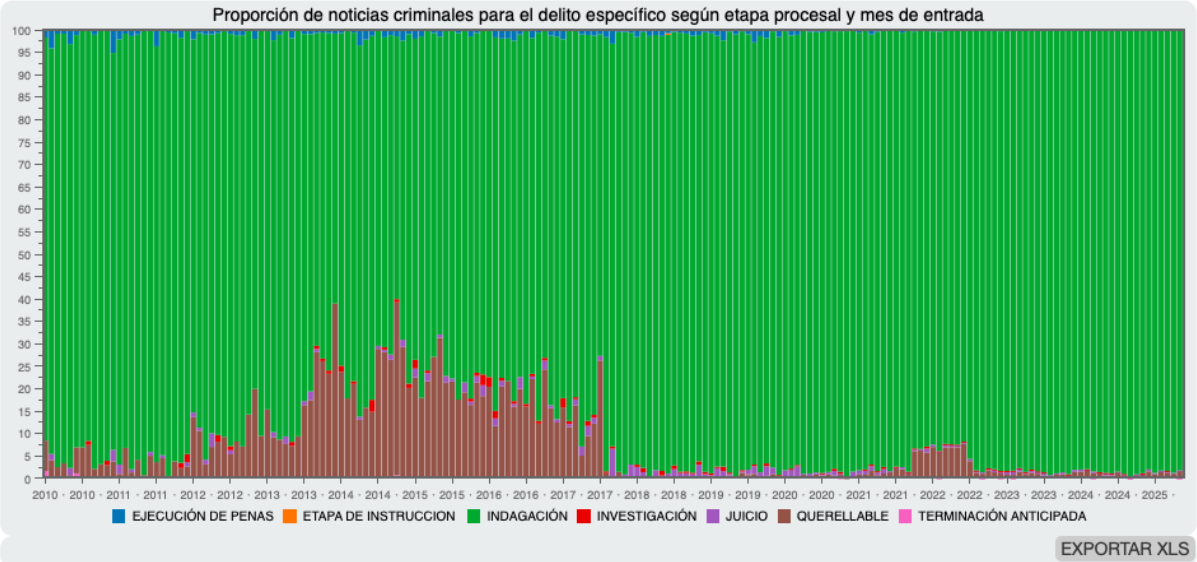
Una vez sea admitida la pretensión, el juez planteará a las partes la posibilidad de conciliación, la cual es requisito sine qua non para proceder a las siguientes etapas procesales. por lo cual se convocará a audiencia la cual deberá llevarse a cabo dentro de los ocho días siguientes a la apertura del incidente, es importante mencionar que la posibilidad de conciliación estará abierta durante todo el proceso Pero en caso de no alcanzarse un acuerdo conciliatorio, el juez convocará a una última audiencia en la que se llevara a cabo la práctica de pruebas y alegatos de conclusión, Esta audiencia concluirá con una decisión judicial que pondrá fin al incidente y cuya parte resolutiva se incorporará a la sentencia penal.

En este contexto, resulta relevante examinar el componente estadístico y procesal de los delitos informáticos dentro del sistema penal acusatorio colombiano, con el fin de

determinar la eficacia de los mecanismos institucionales frente a la persecución de esta tipología penal, esto implica interrogarse sobre sobre la proporción de denuncias que llegan a la Fiscalía General de la Nación que, habiendo sido recepcionadas como noticia criminal logra transitar todas las distintas etapas del proceso hasta culminar con una sentencia de fondo.

Figura 2.

Delito: Acceso Abusivo a un sistema informático, Artículo 269A código penal.



Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos. 2025

Previo analizar el comportamiento del proceso penal cuando el delito es el consagrado en el art. 269 A, es importante identificar su estructura normativa como a continuación se presenta:

> Artículo 269A: *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo de- recho a excluirlo, incurrirá en pena de prisión

de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, enero de 2009).

Figura 3.

Fuente: Imagen de elaboración propia.

En primer lugar, avizoramos que este delito es de mera conducta, ya que no exige el resultado material o daño en concreto sobre la información o sistema al que se accede. La simple acción de acceder sin autorización, sin importar si se altera, destruye, configura la conducta punible esto atendiendo a los bienes jurídicos que se protegen con este delito.

Asimismo, es un delito de ejecución instantánea pues este se consuma desde el momento en el que se accede sin autorización al sistema informático, esto no quiere decir que el delito no pueda ejecutarse de una manera continua prolongándose en el tiempo, solo que la conducta se perfecciona desde el mismo instante en el que se ve vulnerado el derecho del titular legítimo del sistema.

Desde la estructura del tipo penal, se observa que estamos frente a un tipo penal simple**,** ya que contiene un único verbo rector que es acceder. No hay múltiples conductas o acciones de ejecución que permitan configurar el tipo penal.

En cuanto a su estructura normativa presenta un tipo penal cerrado**,** en el sentido de que su redacción es precisa y concreta. No exige al juez acudir a cláusulas abiertas o normas en blanco para determinar si la conducta encaja o no en la descripción típica. La conducta está claramente delimitada, no tiene margen de ambigüedad.

En cuanto a la calidad del autor del delito, se trata de un tipo penal monosubjetivo, ya que su comisión puede realizarse de forma individual. No requiere de la participación de varias personas para su configuración. Igualmente, es importante señalar que este delito puede ser cometido por cualquier persona, lo que lo define como un tipo de sujeto activo simple. No exige una cualificación o condición especial en el sujeto,

Respecto al sujeto pasivo, éste será quien ostente el derecho legítimo de excluir el acceso al sistema informático: normalmente, el propietario, titular o usuario autorizado del mismo. Por tanto, puede tratarse de una persona natural o jurídica.

Finalmente, debe resaltarse que, con la modificación introducida por la Ley 1273 de 2009, se amplió el ámbito de aplicación del tipo penal, eliminando la exigencia previa de que el sistema estuviera protegido por una medida de seguridad. Algunas modalidades en las que se comete este delito son por medio de ingeniería social, software malicioso, phishing, smishing, SIM SWAP, explotación de vulnerabilidades.

En estudio de las etapas procesales por el delito de acceso abusivo a sistemas informáticos enmarcada en el artículo 269A Ley 599 de 2000. revela una concentración en la fase inicial de indagación a lo largo de todo el período examinado, particularmente a partir del

año 2015. Tal predominancia evidencia que un alto porcentaje de las denuncias permanecen estancadas en las primeras fases preliminares de investigación, sin que se produzca un avance significativo hacia etapas procesales siguientes que conlleven a la etapa final del proceso penal acusatorio.

Entre los años 2010 al 2014, si bien la indagación era la etapa más sobresaliente en donde las denuncias se estancaron, en estos años se observa el crecimiento de otras etapas como es la investigación, las audiencias preparatorias y en un menos porcentaje la apertura del juicio oral, este fenómeno sugirió que en un mayor porcentaje estas denuncias lograban superar las barreras iniciales que se encontraban en el transcurso del proceso.

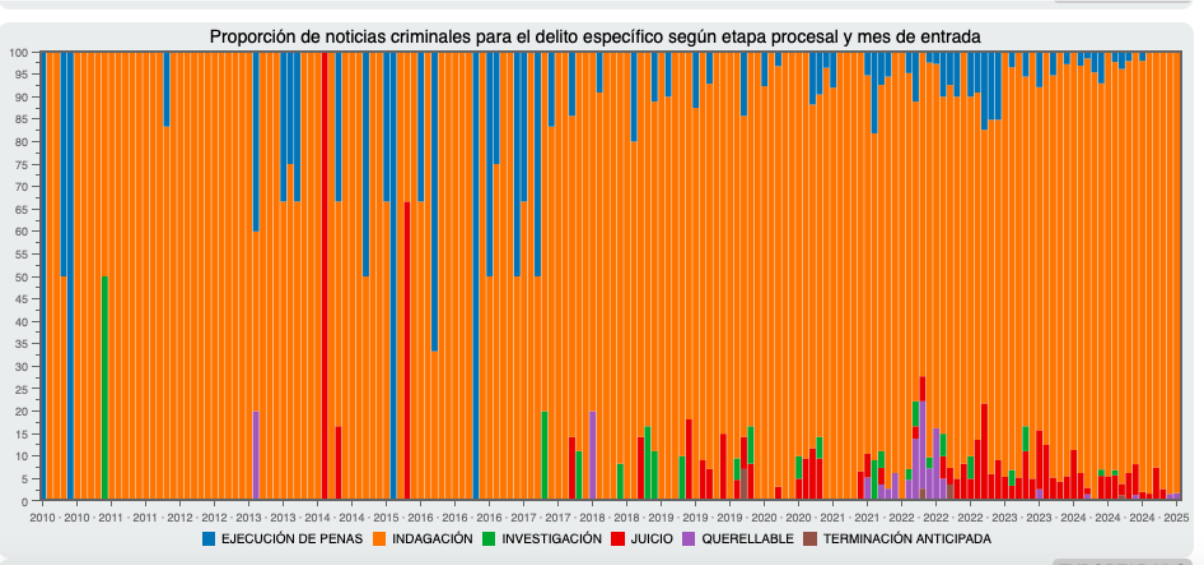
Entre 2014 y 2017 se registra un aumento significativo en la etapa de investigación, acompañado por la aparición de procedimientos que asumieron la calidad de querellables, lo cual podría indicar una intensificación en la judicialización y en la actividad investigativa especializada. La consideración de ciertos casos como querellables sugiere, asimismo, la existencia de delitos susceptibles de ser perseguidos mediante acción privada o bajo mecanismos alternativos de solución de controversias.

En el año 2018 se observa un retroceso al avance de las etapas procesales, manifestado en una concentración casi exclusiva en la etapa preliminar de indagación y una drástica disminución en la prosecución de los procesos hacia las fases de investigación, juicio oral y ejecución de penas. Esta tendencia pone en evidencia una ralentización o bloqueo en el tránsito procedimental, reflejando dificultades estructurales y procesales que afectan la eficacia del sistema de justicia penal.

Sigue persistente la marginalidad de las etapas de juicio oral y ejecución de sanciones penales, fases que representan la culminación del proceso penal mediante la imposición y cumplimiento efectivo de las penas.

Figura 4.

Delito: Obstaculización ilegítima de sistema informático o red de telecomunicación, artículo 269B código penal.

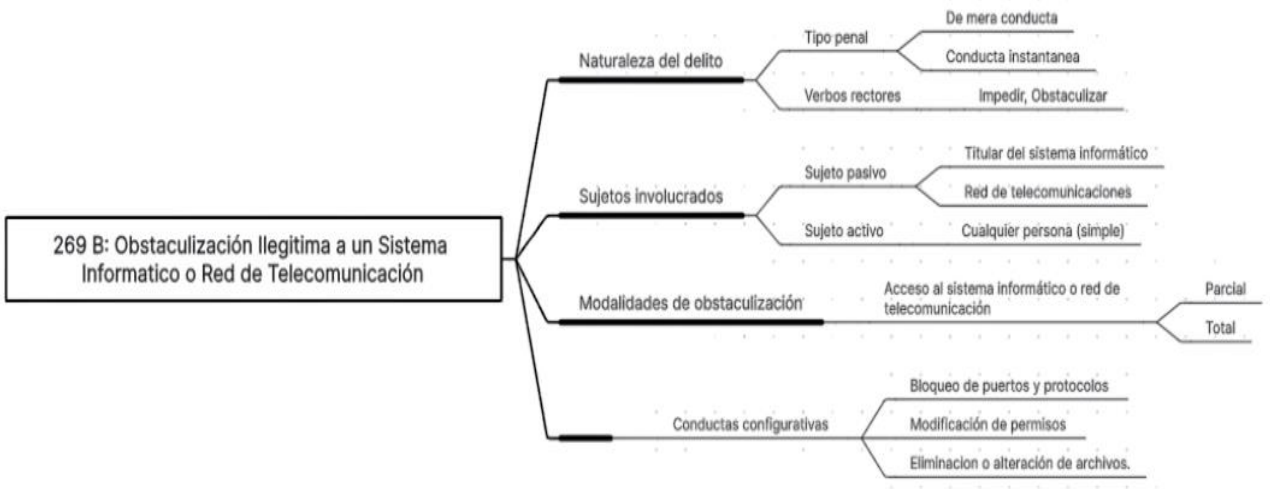


Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos, 2025.

Previo analizar el comportamiento del proceso penal cuando el delito es el consagrado en el art. 269 B, es importante identificar su estructura normativa como a continuación se presenta:

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

Figura 5.



Fuente: Imagen de elaboración propia.

En primer lugar este tipo penal está compuesto, al contemplar dos verbos rectores: impedir y obstaculizar; impedir hace referencia a imposibilitar completamente la ejecución de un sistema mientras que obstaculizar alude a entorpecer o dificultar su funcionamiento normal.

En cuanto a configuración en el tiempo se trata de un tipo penal de mera conducta, ya que no exige un resultado material para que se configure la conducta típica, la sola acción de impedir o obstaculizar es suficiente,

Asimismo, se trata de un tipo penal de ejecución instantánea, en la medida en que la conducta se consuma con la realización del acto obstaculizador o impeditivo. No requiere de una permanencia prolongada ni de una afectación sostenida en el tiempo; sin embargo esto no quiere decir que esta conducta no pueda sostenerse en el tiempo.

Desde su configuración normativa, el artículo 269B es un tipo penal cerrado, ya que establece de forma clara y específica las conductas prohibidas, sin necesidad de acudir a cláusulas generales o normas complementarias para entender su alcance.

El delito también se configura como monosubjetivo**,** ya que su comisión no requiere la participación de varias personas. Puede ser ejecutado por un único individuo, cuya conducta se dirige de forma unívoca a afectar el funcionamiento de los sistemas o redes descritas. A su vez, el sujeto activo es simple, no requiere una cualificación especial, como un rol técnico, administrativo o profesional. Basta con que la persona no esté facultada para realizar la acción que ejecuta.

El sujeto pasivo, por su parte, será el titular legítimo del sistema informático o de la red de telecomunicaciones afectada, esto es, el propietario o usuario autorizado que ve limitado su derecho a acceder o utilizar dichos sistemas.

En cuanto al objeto material, el delito puede recaer sobre tres soportes claramente definidos: el sistema informático, los datos contenidos en él y la red de telecomunicaciones. Esta amplitud permite una protección integral del entorno digital**.**

Desde una mirada informática, resulta relevante destacar que este delito puede materializarse mediante múltiples medios técnicos: bloqueos de puertos, saturación de red, modificación de permisos, ransomware de bloqueo o cifrados, Ataque DoS, Ataque DDoS, Botnet, Ataque DNS, Buffer Overflow.

Por otro lado, este tipo penal tiene una naturaleza pluriofensivo**,** al afectar simultáneamente más de un bien jurídico**.** En efecto, además de la seguridad e integridad de la información, se protege el derecho a la comunicación y el libre acceso a los servicios tecnológicos, fundamentales en una sociedad digitalizada.

Entre los años 2010 y 2012 se observa una preponderancia en la etapa de ejecución de penal, con picos esporádicos que se extienden hasta el 2016; A partir de 2013 al 2014, y con consolidación clara desde 2017 hasta 2018, se produce una transición estructural hacia el estancamiento en las fases preliminares, particularmente en la indagación preliminar, que se convierte en la fase dominante hasta 2024.

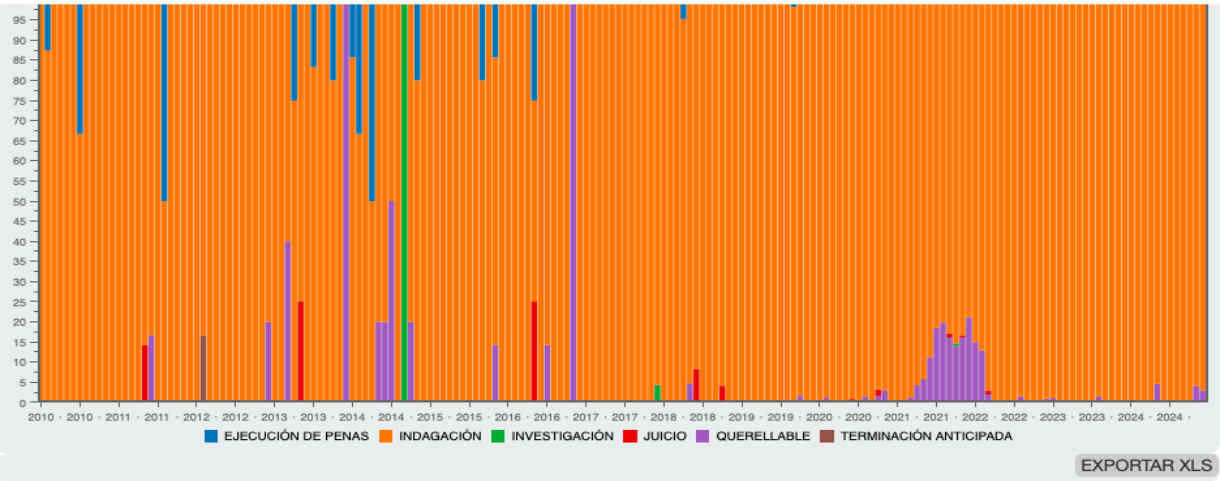
La investigación se torna de una manera intermitente entre los años 2017 al 2019 y en 2021, pero sin consolidarse como una fase sólida que perdura en el tiempo. Su desaparición en otros periodos denota la dificultad para sostener imputaciones formales de manera continua.

acción penal querellable y terminación anticipada del proceso emergen de manera mínima y esporádica, sin representar mecanismos eficaces de resolución.

Finalmente, del año 2018 al 2019 se registra una drástica caída en la ejecución de penas, que se torna prácticamente imperceptible, consolidando un patrón regresivo que persiste hasta 2024.

Figura 6.

Delito: Interceptación de datos informáticos, artículo 269 C código penal.

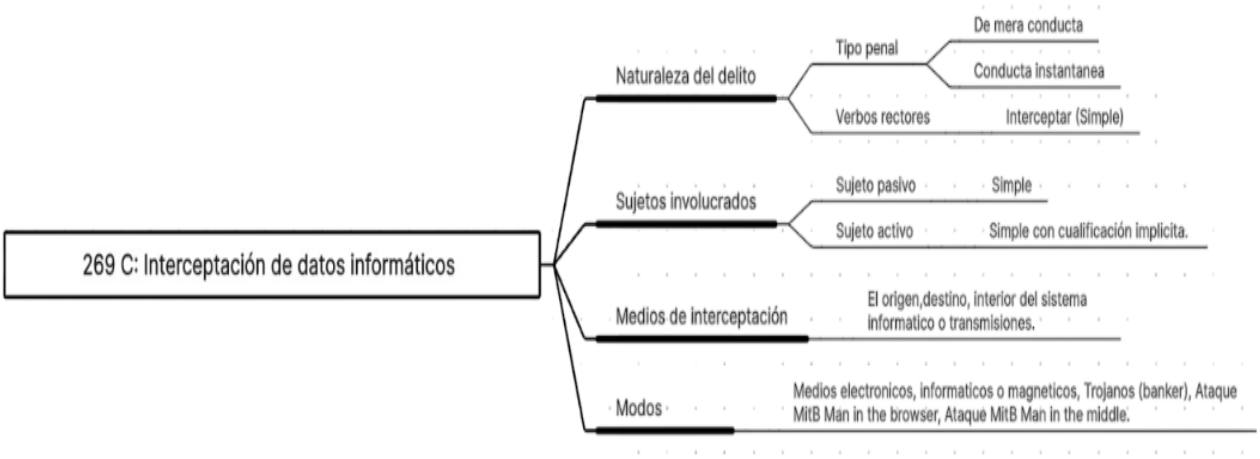


Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

Previo analizar el comportamiento del proceso penal cuando el delito es el consagrado en el art. 269 C, es importante identificar su estructura normativa como a continuación se presenta:

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

Figura 7.



Fuente: Imagen de elaboración propia.

La conducta típica descrita consiste en la interceptación no autorizada de datos informáticos, ya sea durante su tránsito (origen o destino), mientras permanecen en el sistema, o incluso en la captación de las emisiones electromagnéticas que los transportan. Esta conducta tiene una estructura de tipo penal instantáneo, en tanto se consuma con la mera interceptación, sin que se requiera la permanencia de la acción o sus efectos.

Así mismo se trata de un tipo penal simple, con un solo verbo rector "interceptar" no tienen distintas acciones que permitan configurar el tipo penal. Adicionalmente este tiene un elemento normativo especial que es la ausencia de orden judicial previa y es lo que constituye un elemento diferenciador de una actuación legítima y la convierte en reprochable.

Es de gran relevancia hablar del sujeto activo de la actuación aunque el tipo penal utiliza la fórmula genérica "El que", en su aplicación práctica se ha entendido que no se configura ante cualquier sujeto simple sin cualificación. En efecto, quién puede incurrir en esta conducta típica debe ser un funcionario autorizado para realizar interceptaciones, lo que implica una calificación especial implícita del sujeto activo.

Esta calificación se deduce del hecho de que, por regla general, las interceptaciones solo pueden realizarse en el marco de una investigación penal y con previa autorización judicial, Por tanto, el sujeto activo más comúnmente asociado con este delito es aquel que,

ostentando funciones de policía judicial o de apoyo investigativo, omite obtener la autorización judicial requerida o actúa al margen de ella.

Por su parte el sujeto pasivo si bien es simple el afectado siempre será el titular de los datos interceptados de manera ilegítima. Aquel cuya intimidad , privacidad y protección de la información resulta vulnerada por diferentes medios como medios electrónicos, informáticos, ópticos, magnéticos, Trojanos (Banker), Ataque MitB Man in the browse, Ataque MitM Man in the middle.

La característica más sobresaliente y estructuralmente persistente del periodo analizado es la hegemonía prácticamente absoluta de la etapa de indagación preliminar dentro de la dinámica procesal de los casos de interceptación ilícita de datos informáticos.

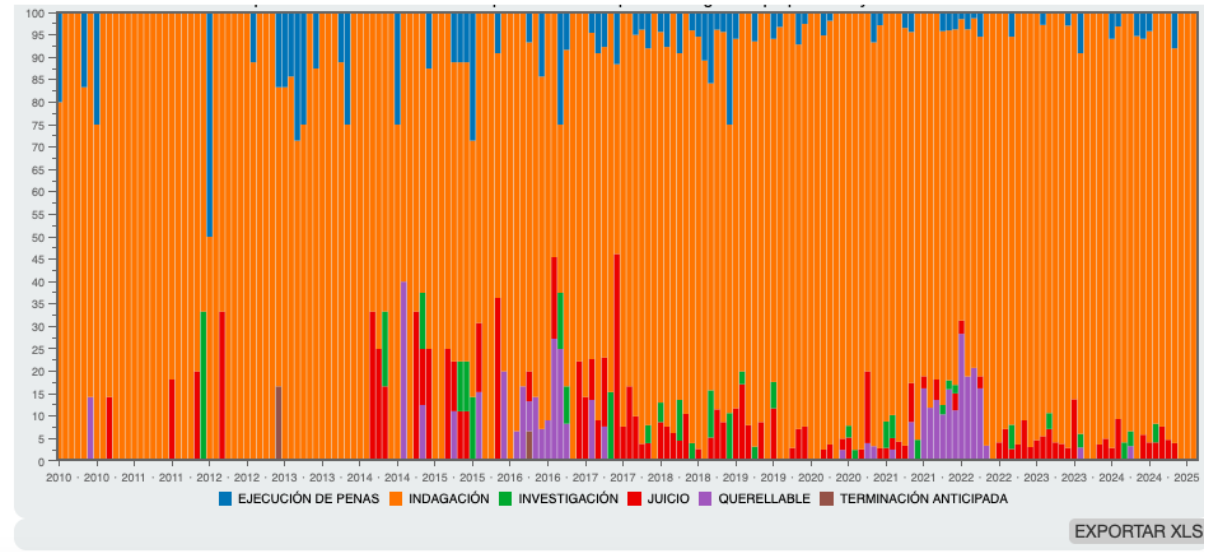
Entre los años 2013 y 2015 se identificaron mayor activación de la etapa de investigación logrando sobrepasar la etapa preliminar, sin embargo, no logra consolidarse en el tiempo siendo así que entre los años 2016 y 2017 esta etapa sufre una recaída casi desapareciendo por completo y estancándose nuevamente en la etapa de indagación.

Entre los años 2021 y 2022 se realizó un aumento significativo de denuncias con naturaleza querellable. Este pico, si bien cuantitativamente es relativamente bajo con relación a las noticias criminales, es jurídicamente significativo. Podría ser indicativo de recalificaciones tipológicas donde se privilegia la reparación integral o la solución alternativa al conflicto.

En el periodo del año 2024 hay una significativa regresión en la que la indagación es la única etapa visible mientras que las demás etapas se desvanecen casi por completo.

Figura 8.

Delito: Daño informático, Artículo 269D código penal.

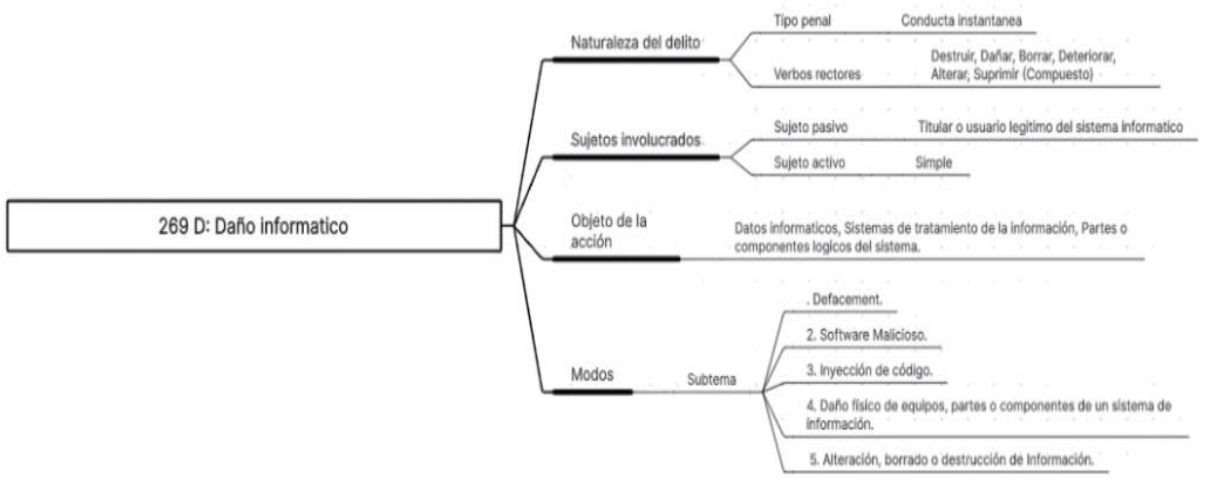


Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

Previo analizar el comportamiento del proceso penal cuando el delito es el consagrado en el art. 269 D, es importante identificar su estructura normativa como a continuación se presenta:

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

Figura 9.



Fuente: Imagen de elaboración propia.

Esta conducta se trata de un delito de acción instantánea, ya que su consumación ocurre en el momento mismo en que el sujeto activo realiza alguna de las conductas típicas sin que sea necesario un resultado posterior o un daño adicional para que se configure la conducta típica.

Por su parte el sujeto activo es un sujeto simple, no requiere ninguna cualificación o característica especial. Sin embargo, su elemento esencial es la ausencia de facultad para ejecutar las conductas descritas, es decir, debe actuar sin autorización.

El sujeto pasivo es el titular o titular del sistema informático o de los datos afectados. Pueden ser tanto personas naturales como jurídicas que poseen la titularidad, el derecho de uso o control legítimo sobre los sistemas de información

Este tipo penal está compuesto ya que su norma trae consigo diversidad de verbos rectores tales como: destruir implica causar una pérdida grave y casi irreversible de los datos o sistemas, o. Dañar supone alterar o impedir el funcionamiento adecuado de los sistemas o datos, afectando su uso legítimo. Por su parte, borrar **y** suprimir aluden a la eliminación o desaparición de la información, mientras que deteriorar implica un menoscabo o

empeoramiento del estado funcional del sistema o datos. Finalmente, alterar refiere a modificar el contenido, la forma o los metadatos, cambiando la esencia original de la información o sistema, Estos acciones se pueden dar por modos como: Defacement, Software malicioso, Inyección de códigos, Daños físico de equipos, partes o componentes de un sistema de información y Alteración, borrado o destrucción de información.

En cuanto al resultado, la norma no exige la materialización de un daño patrimonial específico o una afectación concreta adicional, ya que la consumación del delito ocurre con la realización de cualquiera de las conductas descritas

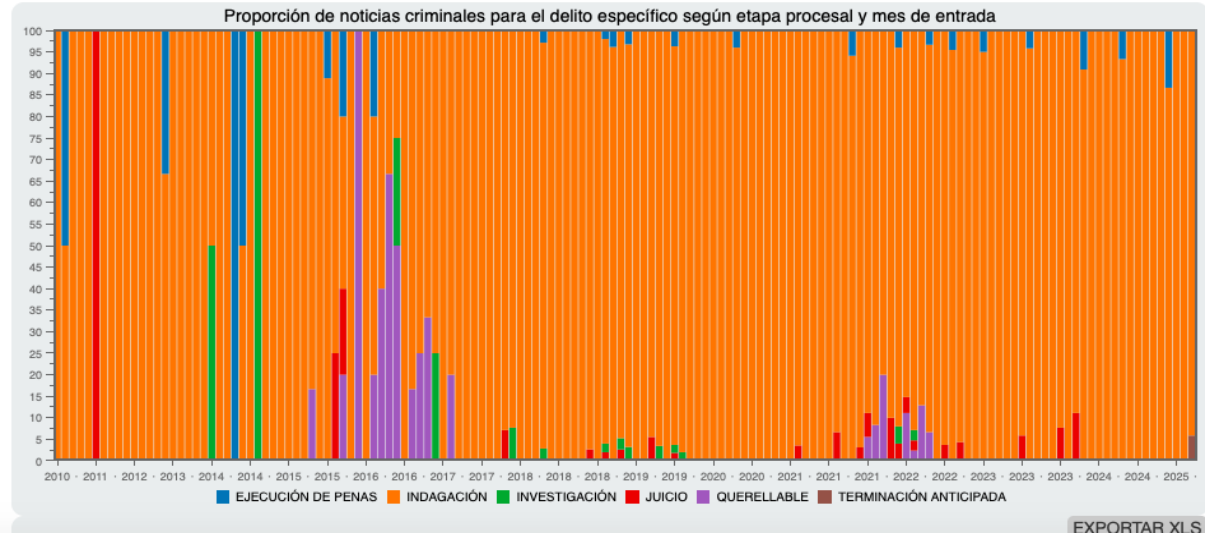
El análisis estadístico realizado en los comportamientos procesales en los casos de daño informático que se encuentra tipificado en la ley 599 del 200, hay una prevalencia en la etapa de indagación entendida esta como una fase preliminar. Esta etapa procesal ha acaparado de manera sistemática la mayoría de los registros procesales, configurando un patrón de anclaje que inhibe la progresión hacia etapas más avanzadas como la investigación, el juicio oral o la ejecución de la pena; Tal hegemonía de esta etapa que fue sostenida por aproximadamente 15 años, revela un hipo eficacia institucional en términos de resultados.

Entre los años 2010 y 2013, la indagación ya ostentaba una proporción significativa. La escasa aparición de otras fases procesales sugiere, por un lado, la existencia de dinámicas judiciales de baja litigiosidad y, por otro, un contexto normativo o institucional aún incipiente en el tratamiento penal del daño informático; A partir de 2014 se identifica una leve incrementación de etapas de investigación y juicio oral, con ciertos picos de actividad hacia los años 2016 y 2017. La eventual aparición de casos tramitados como delitos querellables, aunque marginal, sugiere la existencia de supuestos de afectación patrimonial o moral susceptibles de ser subsumidos en tipos penales de menor entidad; A finales de 2019 y con mayor notoriedad entre 2020 y 2025, esto evidencia un marcado retroceso en la trazabilidad

procesal. Las etapas avanzadas del procedimiento penal prácticamente desaparecen del registro estadístico, dejando como única variable que las denuncias se estancaron en la etapa de indagación o también llamadas etapa preliminar.

Figura 10.

Delito:,Uso de software malicioso, artículo 269 E código penal.

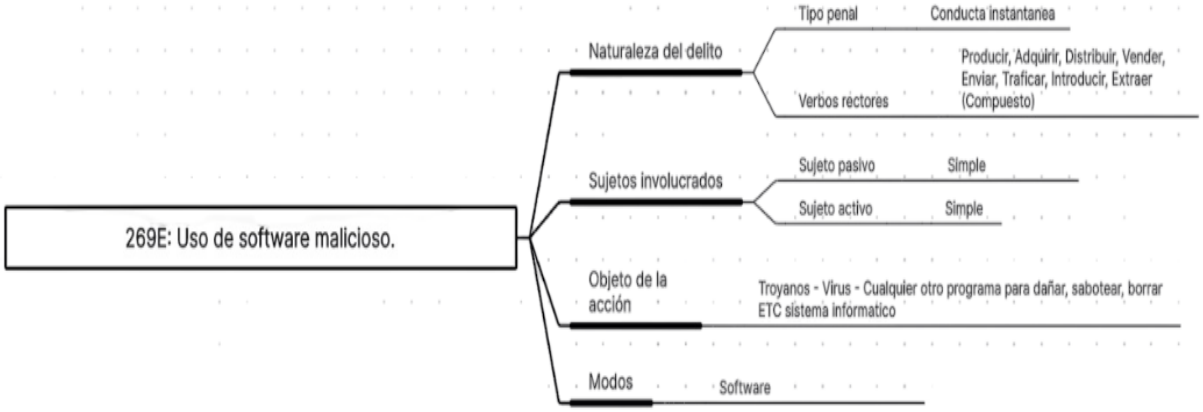


Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

Previo analizar el comportamiento del proceso penal cuando el delito es el consagrado en el art. 269 E, es importante identificar su estructura normativa como a continuación se presenta:

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

meses y en multa de 100 a 1.000 salarios mínimos legales men- suales vigentes (Congreso de Colombia, 2009).



Fuente: Imagen de elaboración propia.

Desde un punto de vista estructural, se trata de un tipo penal compuesto, ya que integra múltiples conductas en su redacción mediante el uso de varios verbos rectores: producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer . En términos subjetivos, se configura como un delito monosubjetivo no requiere la participación de varias personas para que este se configure.

El sujeto activo es un sujeto simple no requiere ninguna cualificación ni característica especial, pero que sí debe actuar sin facultad legal o contractual. Esta carencia de autorización constituye un elemento normativo esencial del tipo, ya que si el sujeto actúa con permiso legítimo no se configura una conducta típica.

El sujeto pasivo es la sociedad en general y a su vez la persona natural o jurídica que resulte potencialmente perjudicada por el uso y la diseminación de programas dañinos.

En cuanto al objeto material, se centra en el software malicioso o “malware”, que comprende programas diseñados específicamente para causar daño, alterar, borrar, extraer

información o interferir en los sistemas informáticos. Esta categoría incluye, entre otros, virus, gusanos, troyanos, ransomware, y cualquier otro programa con efectos intrínsecamente nocivos.

Respecto a la conducta típica, esta se configura con cualquiera de los ocho verbos rectores contemplados por la norma: producir, traficar, adquirir, distribuir, vender, enviar, introducir o extraer del territorio nacional. Todos ellos hacen referencia a etapas del ciclo de circulación de software malicioso, sin que sea necesario que el mismo sea ejecutado o instalado en un sistema informático determinado. Es decir, el legislador opta por sancionar el comercio y la distribución del malware en cualquiera de sus fases.

En los periodos comprendidos entre 2010 y 2013, tienen una preponderancia de la etapa de ejecución de penas, con una proporción estadística que, en varios meses, resulta atípicamente elevada para este tipo de criminalidad. Esta anomalía, dado el contexto general de los delitos informáticos. Sin embargo, a partir de los años 2014 y 2015, se advierte una decadencia de la ejecución de penas, en donde se consolida como etapa predominante la indagación “fase preliminar”. La cual se intensifica de forma crítica desde 2018 hasta 2025, periodo en el cual la indagación absorbe una proporción abrumadora de las noticias criminales.

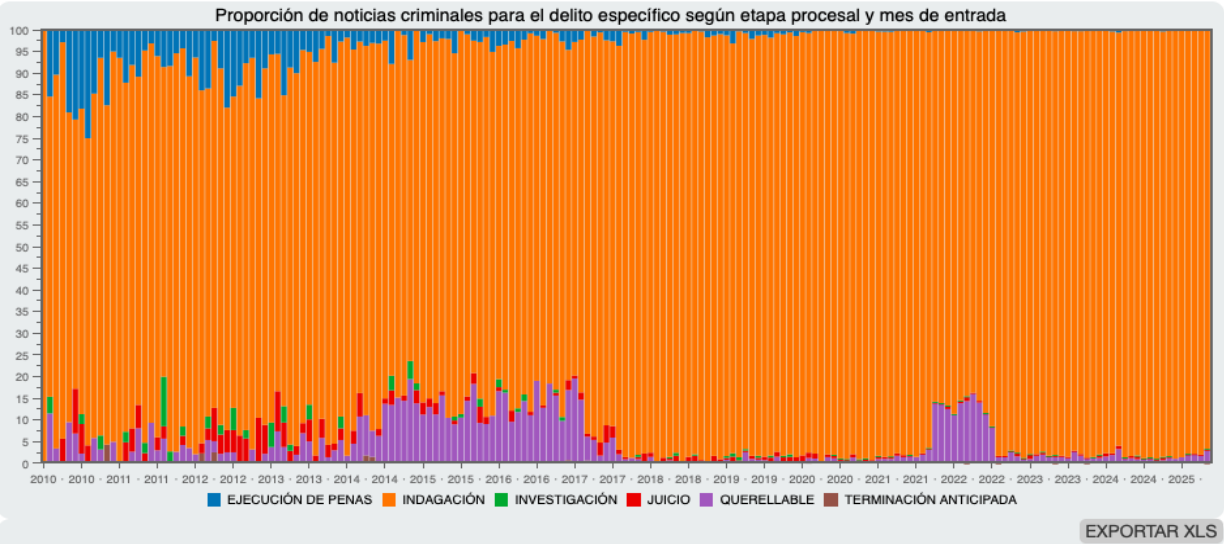
En cuanto a la etapa de investigación, fragmentaria en el paso de los años, con algunos picos de actividad entre 2014 y 2017, y un repunte entre los años 2021 y 2022, sin que ello implique una tendencia a una consolidación procesal de esta etapa.

Por su parte, las figuras procesales de acción penal querellable y terminación anticipada del proceso muestran una presencia marginal jurídicamente irrelevante en términos cuantitativos.

El patrón más preocupante se consolida hacia el final del periodo particularmente a partir de 2019 y proyectado hasta 2025**,** con la absorción casi total de la actividad procesal por parte de la etapa de indagación

Figura 11.

Delito: Violación de datos personales, artículo 269F código penal.

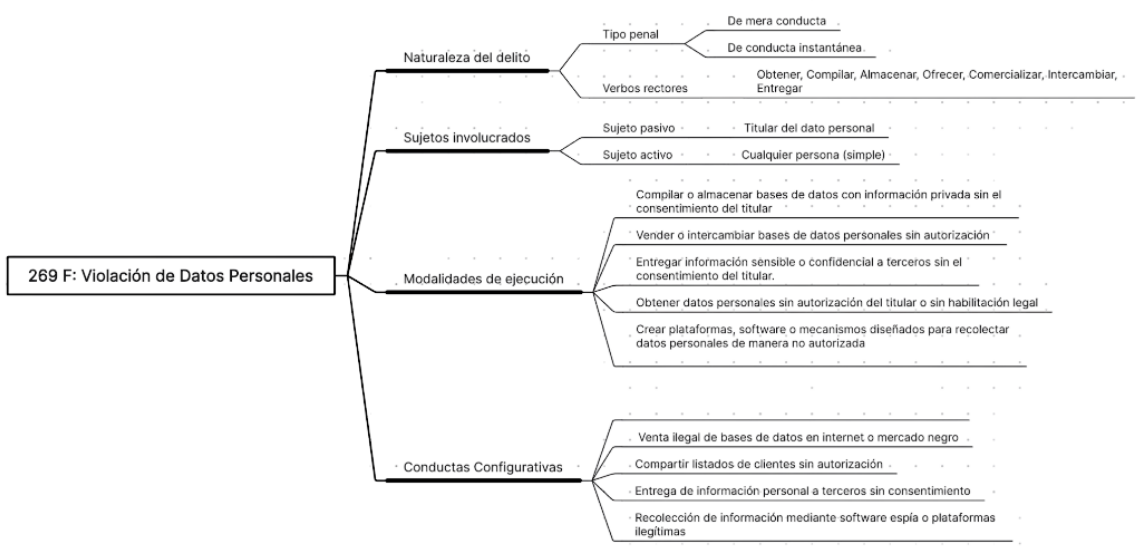


Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

Previo a analizar el comportamiento del proceso penal cuando el delito es el consagrado en el artículo 269F, es importante identificar su estructura normativa como a continuación se presenta:

> Artículo 269F: Violación de datos personales.El que, sin estar facultado para ello, y valiéndose de cualquier medio, obtenga, compile, almacene, ofrezca, comercialice, intercambie o entregue datos personales a terceros, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes. (Congreso de Colombia, enero de 2009).

Figura 12.



Fuente: Imagen de elaboración propia.

En este tipo penal basta con que se realicen actos como obtener, compilar, almacenar, ofrecer o entregar datos personales sin estar facultado. Por tanto, se configura como un delito de mera actividad, donde lo sancionable es el acceso o manipulación no autorizada de datos privados.

Desde la perspectiva constitucional, este delito se relaciona con el artículo 15 de la Carta Política, que protege el derecho a la intimidad y al habeas data. Más allá de una norma jurídica, representa una defensa frente al uso abusivo de la información personal, recordando que detrás de cada dato hay una persona cuya dignidad debe ser respetada.

Este tipo penal está construido con verbos múltiples, que reflejan diferentes fases del manejo indebido de la información personal. No es necesario que todos se presenten en conjunto porque la ocurrencia de uno solo de estos actos configura la conducta típica. El uso de verbos como “comercializar” o “ofrecer” evidencia la mercantilización de la privacidad en

el entorno digital, donde empresas, plataformas y actores criminales negocian con datos sensibles sin autorización ni transparencia.

El delito se consuma con la sola ejecución de cualquiera de los actos mencionados en el tipo penal. Aunque el efecto (como el uso comercial de los datos o el daño reputacional) puede perdurar en el tiempo, la conducta es de ejecución única. Esta característica busca sancionar el momento mismo en que se vulnera el control que el titular tiene sobre su información y esto permite proteger proactivamente el derecho a la autodeterminación informativa, pero también exige precisión probatoria, ya que la persecución penal requiere acreditar el momento en que se produjo la acción no autorizada.

El delito puede ser cometido por cualquier persona natural o jurídica que realice tratamiento de datos sin habilitación legal, incluyendo empresas que recopilan información sin autorización, funcionarios que acceden indebidamente a bases de datos estatales, personas que venden datos en el mercado negro digital o manipulan información privada con fines dañinos reflejando la débil cultura de protección de datos personales, tanto en el ámbito público como en el privado.

La víctima es la persona sobre la cual recae la información manipulada. Es importante destacar que este sujeto puede no estar al tanto de la violación a su intimidad, lo que dificulta la denuncia y el acceso a la justicia. En muchos casos, las personas descubren que su información ha sido usada de forma ilegítima solo después de enfrentar consecuencias (suplantación, fraude, discriminación digital, etc.).

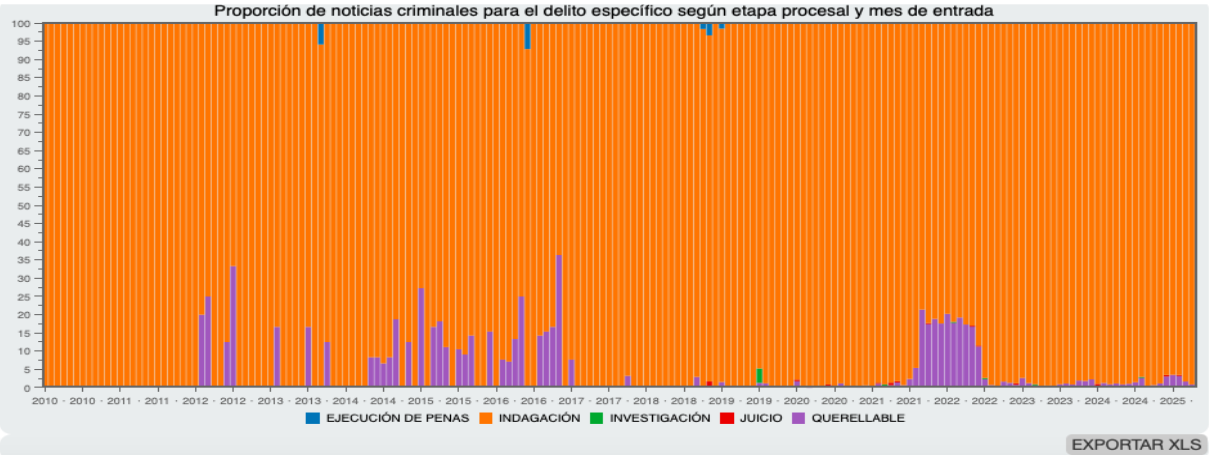
Entre los años 2010 y 2025**,** persistente en la trayectoria procesal la preponderancia absoluta de la etapa de indagación etapa preliminar**.** Este delito presenta un aspecto singular respecto a la fase de acción penal querellable, cuya presencia, aunque minoritaria en términos cuantitativos resulta significativamente más constante.

Se advierten fluctuaciones significativas en la activación de la fase querellable durante el periodo 2010 a 2016, en el cual se registran picos procesales relevantes**.** Posteriormente, se observa un repunte sostenido a partir de 2020**,** alcanzando su mayor expresión cuantitativa y visibilidad procesal entre los años 2021 y 2023.

No obstante, la dimensión más crítica desde una perspectiva garantista y de política criminal es la práctica inexistencia de las etapas formales de investigación, juicio oral y ejecución de penas durante la totalidad del periodo observado. A pesar de ciertos repuntes intermitentes en la categoría querellable, a partir de 2018 al 2019 y de forma sostenida hasta 2025, se consolida un modelo de regresión procesal, en el cual la etapa de indagación no solo persiste como la fase inicial, sino que se institucionaliza como fase terminal de facto**,** configurando un patrón de ineficacia estructural en el sistema de administración de justicia penal.

Figura 13.

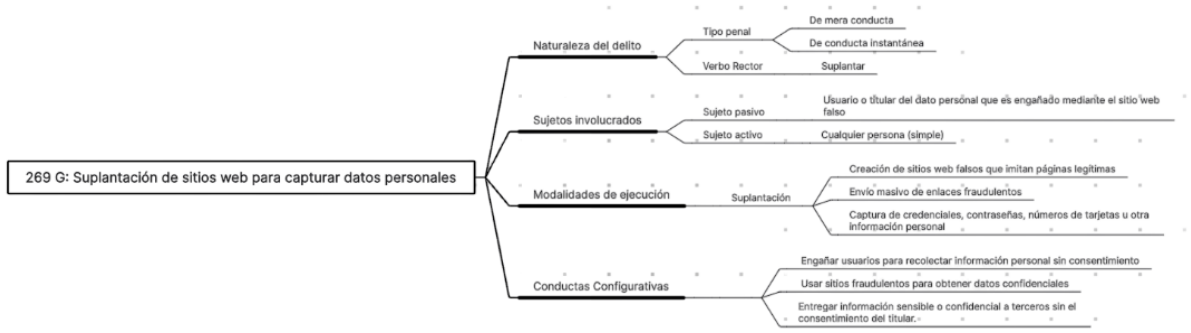
Delito:, Suplantación de sitios web para capturar datos personales, artículo 269G código penal.



Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

Artículo 269G: Suplantación de sitios web para capturar datos personales: El que, con la intención de obtener datos personales, cree, copie, clone o falsifique una página web o sitio de internet, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes. (Congreso de Colombia, Ley 1273 de 2009).

Figura 14.



Fuente: Imagen de elaboración propia.

Este delito es de mera actividad, se consuma sin necesidad de que se logre efectivamente la captura de los datos personales. Basta con crear, copiar, clonar o falsificar una página web con intención de obtener esa información. Desde el punto de vista constitucional, se vincula al derecho a la privacidad, al habeas data (art. 15 CP), y a la seguridad informática como extensión de los derechos fundamentales en entornos digitales.

El tipo penal incorpora varias formas de suplantación digital. Se puede simular o imitar un sitio web que tenga apariencia legítima para engañar al usuario y obtener su información abarcando estrategias tecnológicas como el phishing, spoofing, pharming o ataques man-in-the-middle, que han ganado popularidad en Colombia basándose en el abuso

de la confianza digital, lo que evidencia la necesidad de educación en ciudadanía digital y mayores niveles de alfabetización tecnológica entre la población.

Se consuma en el momento en que el autor crea o utiliza el sitio web fraudulento con la finalidad de obtener datos personales, sin que sea necesario lograr la obtención de esa información. Lo que es una característica útil en contextos donde los daños se producen rápidamente, como fraudes bancarios o filtraciones pero muchas veces se elimina la página antes de que la conducta pueda ser perseguida.

Cualquier persona puede ser sujeto activo, sin que se requiera una cualificación especial. No obstante, en la práctica se trata de personas con conocimientos técnicos en diseño web, programación, ciberseguridad o manipulación de plataformas electrónicas.

La víctima es cualquier persona cuya confianza es manipulada para obtener su información personal a través del engaño digital. Este delito también afecta desproporcionadamente a poblaciones con menor formación digital, como adultos mayores, jóvenes sin educación digital crítica, o comunidades rurales.

Entre los años 2010 y 2025, existe una predominancia absoluta de la etapa de indagación como etapa preliminar, que est**á** destinada a la *noticia criminis* y la recolección de elementos materiales probatorios. Esta etapa absorbe por completo la mayor proporción de las denuncias, sin traducirse en avances significativos hacia fases procesales posteriores.

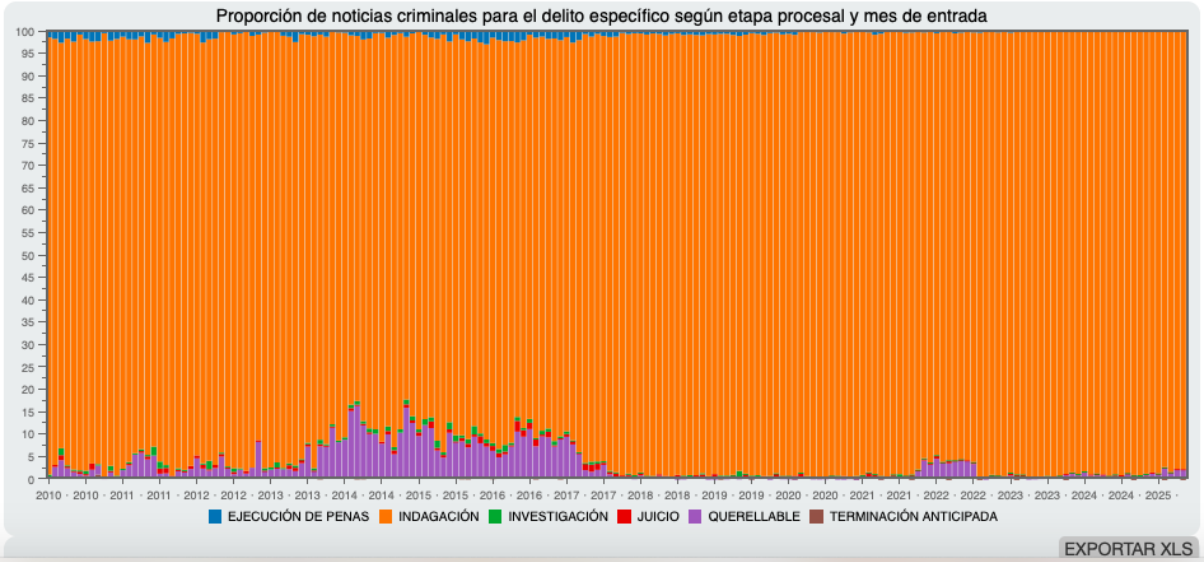
Entre 2011 y 2013 se presenta un pico relevante en los registros de actuaciones “querellables”, y aunque su presencia sigue siendo marginal en comparación con la indagación, se observa un nuevo repunte entre 2021 y 2022.

No obstante, la dimensión más crítica del periodo 2010–2025 es la inexistencia **d**e las etapas de investigación, juicio oral y ejecución de penas. Esta ausencia configura un patrón de ineficacia procesal estructural.

A partir de 2018–2019 y hasta 2025, se intensifica un fenómeno de **c**ongestión procesal en forma de "embudo", donde la etapa de indagación acapara casi por completo el flujo procesal, y las fases subsiguientes se reducen a niveles casi imperceptibles.

Figura 15.

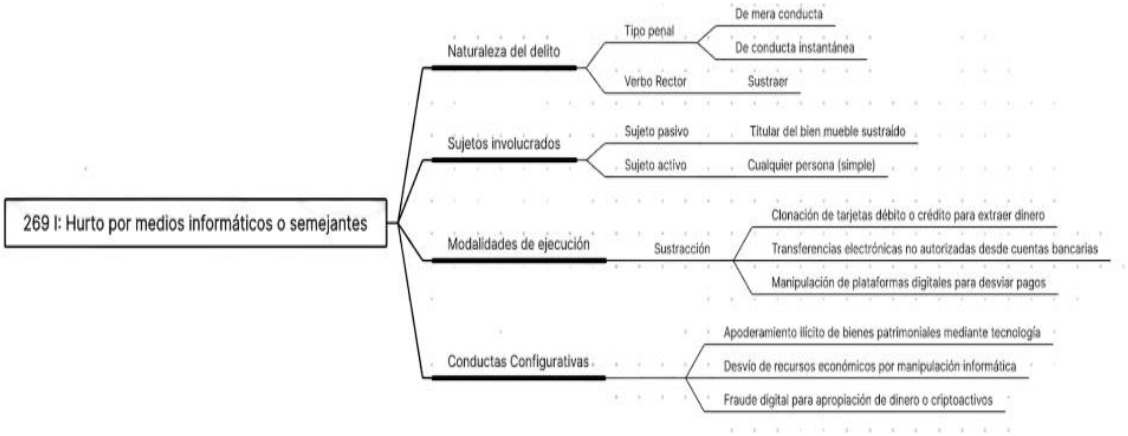
Delito: Hurto por medios informáticos o semejantes, Artículo 269 I código penal.



Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

> **Artículo 269I: Hurto por medios informáticos o semejantes:** El que, mediante la manipulación informática o la utilización de semejantes artificios, sustraiga para sí o para otro bienes ajenos muebles, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veintiocho (128) meses y multa de 6,66 a 1500 salarios mínimos legales mensuales vigentes.(Congreso de Colombia, Ley 1273 de 2009)

Figura 16.



Fuente: Imagen de elaboración propia.

Este delito protege el bien jurídico del patrimonio económico, y su naturaleza es simple, pues se consuma con la sustracción de bienes muebles ajenos a través de medios informáticos o técnicos, sin requerir un resultado agravado ni posterior.

Es la manifestación digital del hurto clásico. La ley penal reconoce que el desarrollo tecnológico ha transformado las formas de apropiarse de lo ajeno, permitiendo que la apropiación pueda realizarse sin presencia física ni violencia directa.Según la Constitución Política de Colombia (1991, art. 58), la propiedad es un derecho inviolable que no puede ser vulnerado sino por motivos de utilidad pública o interés social… adaptado ahora a contextos virtuales y activos digitales.

El verbo “sustraer” conserva el mismo contenido dogmático del hurto tradicional que es apropiarse sin consentimiento del titular, de un bien mueble ajeno, pero mediante herramientas informáticas, manipulaciones digitales o artificios tecnológicos.

En el ámbito digital puede incluir accesos indebidos a plataformas financieras, manipulación de aplicaciones de pagos, robo de criptomonedas, entre otros. No requiere contacto físico ni violencia, por lo que se vuelve un delito de alta invisibilidad y sofisticación, y por tanto difícil de investigar con herramientas tradicionales.

La conducta se consuma en el momento de la apropiación por medios informáticos. No requiere que el bien sea posteriormente usado, ni que la víctima se percate del hurto en ese instante y así el rastro digital del delito es efímero y requiere reacción rápida y conocimientos especializados para su judicialización efectiva.

El delito puede ser cometido por cualquier persona, aunque en la práctica los autores suelen tener acceso privilegiado o conocimiento técnico. Casos comunes incluyen empleados que manipulan software financiero, hackers que acceden a cuentas bancarias, o grupos delictivos que crean plataformas falsas para desviar pagos. También en ocasiones, el sujeto activo puede estar fuera del país, lo que plantea retos de cooperación penal internacional.

La víctima es quien tiene el derecho de disposición sobre el bien sustraído, que puede ser dinero, activos digitales, saldos virtuales, criptomonedas, u otros elementos patrimoniales accesibles por vía digital. Incluyendo tanto personas naturales como jurídicas (empresas, bancos, comercios).

La evolución procesal del delito de hurto perpetrado mediante medios informáticos evidencia un patrón conductual que resulta especialmente significativo desde la óptica del análisis estructural del sistema de administración de justicia penal en su dimensión funcional. El elemento definitorio de dicha trayectoria es la marcada y sostenida preponderancia de la fase de indagación preliminar, la cual se configura como el eje procesal hegemónico que subsume, en términos cuantitativos y cualitativos, la casi totalidad de los casos registrados en el intervalo temporal comprendido entre los años 2010 y 2025.

La etapa de investigación, que es la apertura formal del proceso penal, exhibe una presencia intermitente a lo largo de los años, si bien esta etapa tiene unos picos significativos entre los años 2013 y 2017 fue una etapa que no logró consolidarse tendiendose en el tiempo.

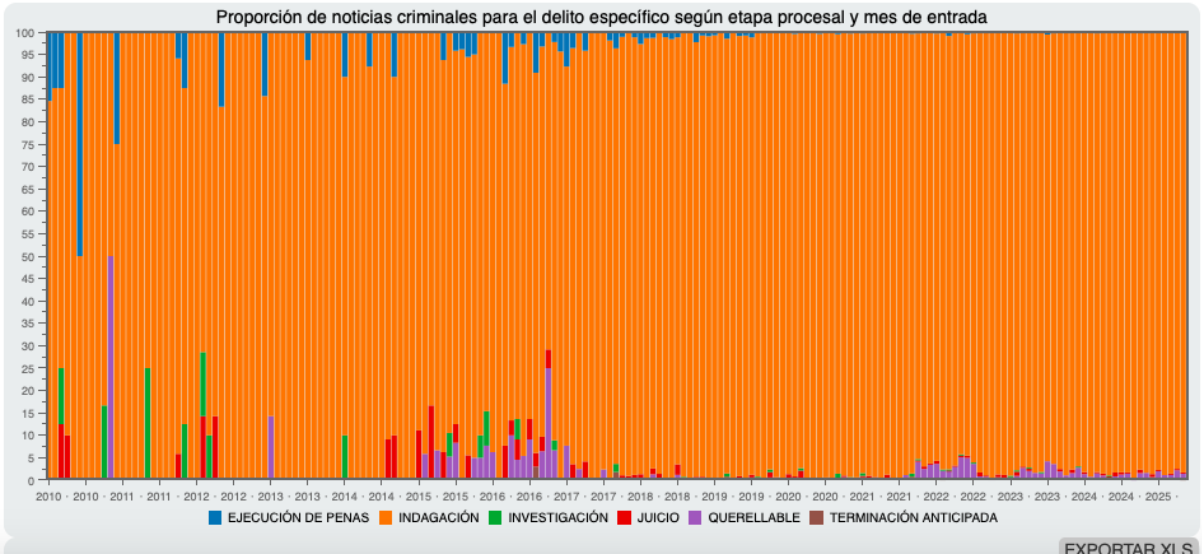
Entre los años 2013 y 2017 aparecieron casos calificados como "querellables". Aunque el hurto informático agravado no constituye típicamente una conducta susceptible de acción penal privada dada su gravedad y su impacto patrimonial, esta categoría procesal podría ser indicativa de una recalificación de la conducta hacia figuras de menor entidad, tales como el hurto simple. Aplicando principios de oportunidad por parte de la Fiscalía General de la Nación, que habrían permitido la terminación anticipada del proceso a través de mecanismos como la conciliación, la reparación integral.

La dimensión más crítica del análisis la constituye la inexistencia de las etapas de juicio oral y ejecución de penas, las cuales representan, respectivamente, la verificación de los hechos en un contradictorio formal y la materialización efectiva de la justicia penal a través de la imposición y cumplimiento de la sanción. Su virtual desaparición del registro empírico a lo largo de los quince años estudiados configura un déficit funcional de alta gravedad jurídica, que socava los principios de efectividad, proporcionalidad y obligatoriedad de la acción penal, pilares fundamentales del modelo acusatorio consagrado en la Ley 906 de 2004.

A partir del año 2018 se advierte una tendencia regresiva acelerada, caracterizada por una concentración casi absoluta de los procesos en la etapa de indagación y una reducción aún más marcada de todas las demás fases procesales.

Figura 17.

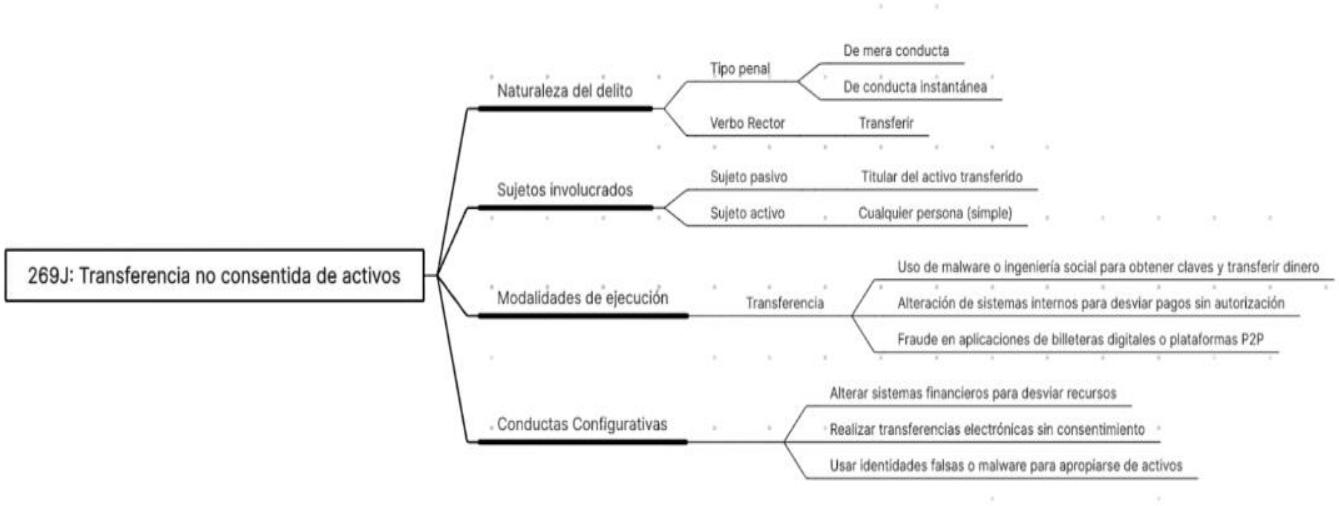
Delito:, Transferencia no consentida de activos, artículo 269J código penal.



Fuente: Fiscalía General de la Nación, Estadísticas, Datos abiertos.

> **Artículo 269J: Transferencia no consentida de activos:** El que, valiéndose de maniobra informática, realice transferencia no consentida de cualquier activo con el propósito de obtener un beneficio para sí o para un tercero, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y multa de 100 a 1500 salarios mínimos legales mensuales vigentes. (Congreso de Colombia, Ley 1273 de 2009).

Figura 18.



Fuente: Imagen de elaboración propia.

Este tipo penal es de mera actividad, la conducta se consuma con el solo hecho de realizar una transferencia no autorizada de cualquier tipo de activo mediante el uso de maniobras informáticas, sin que sea necesario que el beneficiario reciba o use el activo. Esta estructura normativa busca dar una respuesta penal anticipada y se conecta directamente con la garantía constitucional de la propiedad privada (art. 58 C.P.) y la libertad económica (art. 333 C.P.), especialmente en el contexto digital.

El verbo “transferir” se refiere a la acción de mover un activo económico de un titular a otro, valiéndose de medios informáticos y sin el consentimiento del primero. Puede implicar el acceso a plataformas de pagos, sistemas financieros, billeteras digitales o cualquier canal que permita la disposición de activos Es una operación simulada como legítima que revela una transformación profunda de los delitos patrimoniales en la era digital, porque el delito sólo requiere ingeniería informática y manipulación de sistemas.

Más allá de su configuración como delito de mera actividad, el tipo penal previsto en el artículo 269I del Código Penal cumple una función disuasiva frente a las nuevas formas de apropiación patrimonial digital. Al sancionar la sola ejecución de una transferencia no

autorizada mediante medios informáticos, la norma reafirma la inviolabilidad de los bienes digitales y la necesidad de preservar la confianza en las operaciones electrónicas, anticiparse al daño, proteger el ecosistema económico digital y fortalecer la seguridad jurídica en contextos donde la vulnerabilidad técnica puede facilitar conductas lesivas.

Este delito puede ser cometido por cualquier persona, aunque su ejecución suele requerir conocimientos técnicos avanzados o acceso privilegiado a sistemas informáticos. Entre las modalidades más frecuentes se encuentran la manipulación de plataformas de pagos digitales para realizar transferencias, la suplantación de identidad para acceder a cuentas bancarias, el uso de malware o keyloggers para robar credenciales, la alteración de sistemas internos para redirigir fondos y la transferencia no autorizada desde billeteras virtuales o criptomonedas. La víctima, es quien ve transferido su dinero, saldo o valor sin consentimiento, y puede ser una persona natural, una empresa, una organización o incluso una entidad pública.

En el periodo del 2010 hasta el 2025, la dinámica procesal se evidencia una persistente hegemonía de la etapa de indagación, la cual concentra, de forma casi ininterrumpida, la mayor proporción de las actuaciones penales registradas. revela una disfuncionalidad estructural en el ejercicio de la acción penal.

Aunque se identifican picos en la etapa de investigación formal entre 2010 y 2017, especialmente entre 2015 y 2017, tales picos o anomalías no logran consolidarse al transcurrir en tiempo.

La dimensión más crítica del fenómeno analizado radica en la práctica inexistencia de las etapas procesales de juicio oral y, de manera aún más acentuada, de la ejecución de la sanción penal, durante la totalidad del periodo comprendido desde la entrada en vigor del sistema procesal penal acusatorio (Ley 906 de 2004) hasta la actualidad. Esta omisión

sistemática no sólo configura una afectación sustantiva al principio de progresividad procedimental, sino que compromete de forma severa la operatividad y efectividad del *ius puniendi* estatal, en tanto impide la obtención de decisiones judiciales con fuerza de cosa juzgada ya sean condenatorias o absolutorias.

CAPÍTULO II

Herramientas Técnicas y Jurídicas para la Recolección y Análisis de Evidencia Digital en el Proceso Penal Colombiano

2.1 Introducción

Los delitos informáticos requieren un tratamiento técnico y jurídico en el manejo de la evidencia desde las primeras actuaciones para garantizar su validez dentro del proceso penal. La prueba en estos casos casi siempre está compuesta por datos almacenados en medios digitales y su recolección, preservación y análisis necesitan intervenciones especializadas. Esto, porque un mínimo error en estos procedimientos puede afectar su integridad o impedir que sea valorada en juicio. Esta evidencia necesita protocolos cuidadosos y buena coordinación porque es un elemento central en las investigaciones penales sobre conductas cometidas a través de tecnologías de la información.

En Colombia, la Ley 906 de 2004 establece los principios aplicables al manejo probatorio, como la legalidad, la cadena de custodia, la contradicción y la autenticidad. La Ley 1273 de 2009 tipifica conductas que afectan la integridad, disponibilidad y confidencialidad de los datos y sistemas informáticos. Lo cual se complementa con desarrollos jurisprudenciales y estándares internacionales, como los que están establecidos en

la Convención de Budapest, que orientan la labor de los operadores judiciales en contextos digitales y transnacionales.

Este capítulo tiene como propósito presentar una visión clara del estado actual del proceso penal frente al tratamiento de la evidencia digital en delitos informáticos, desde lo que dice la norma hasta lo que enfrentan quienes la ponen en práctica. La revisión normativa permite entender qué herramientas han sido previstas por el legislador para dar respuesta a este tipo de criminalidad, y cómo se espera que se recolecte, conserve y valore este tipo de prueba. Sin embargo, el componente práctico es igual de importante. Las entrevistas realizadas a funcionarios que intervienen en estas investigaciones permiten contrastar la norma con la realidad institucional, evidenciando el nivel de preparación técnica, las limitaciones operativas y los vacíos que todavía afectan el desarrollo de los casos para identificar tanto las capacidades del sistema como los aspectos que requieren ajustes, con el fin de avanzar hacia investigaciones más sólidas, mejor estructuradas y con mayores garantías procesales.

2.2 Delitos más susceptibles y más complejos de investigar

La investigación de delitos informáticos en Colombia presenta notables diferencias en cuanto a su nivel de complejidad, dependiendo no solo del tipo penal involucrado, sino también del contexto en el que se ejecuta la conducta, el momento de su detección, la configuración técnica del sistema afectado y el nivel de sofisticación del agresor.

Las capacidades técnicas en Colombia se organizan a través del Centro Cibernético Policial, que concentra peritajes, alertas y laboratorios especializados. Sin embargo, la presencia regional es desigual y limita la cadena nacional de análisis forense. Un análisis académico reciente confirma que, aunque en los últimos años se han logrado progresos en la informática forense colombiana con nuevas herramientas y laboratorios que fortalecen la

capacidad de investigación digital persisten brechas técnicas y desigualdades en su despliegue territorial que afectan la trazabilidad de la prueba (Bustamante Riaño, 2021).

Los expertos entrevistados coinciden en que existen ciertos delitos cuya estructura técnica favorece la labor investigativa, mientras que otros imponen retos significativos tanto en el plano técnico como probatorio. Entre los más susceptibles de investigación se encuentra el acceso abusivo a un sistema informático (art. 269A C.P.) y el uso de software malicioso (art. 269E C.P.), en la medida en que estas conductas suelen generar rastros claros y verificables. La propia dinámica de estos delitos deja evidencia en forma de registros de conexión, direcciones IP, datos de autenticación o modificaciones identificables en los sistemas comprometidos, especialmente si los incidentes ocurren en entornos organizados con infraestructura técnica establecida. Según los entrevistados, esta tipología de conductas tiene en común que la acción típica es de ejecución cerrada o instantánea, lo que permite acotar el marco temporal de análisis y concentrar los esfuerzos forenses en un conjunto de evidencias relativamente delimitado.

En contraste, los delitos más complejos de investigar son aquellos en los que la evidencia es volátil, susceptible de ser borrada rápidamente, o bien cuando se emplean técnicas antiforenses avanzadas. Ejemplos de ello son la interceptación ilícita de datos informáticos (art. 269B C.P.) y la violación de datos personales (art. 269F C.P.), donde la prueba requiere demostrar la captación no consentida y el eventual uso indebido de la información, elementos que, en la práctica, suelen carecer de registros persistentes y pueden estar alojados en memorias RAM que se borran al finalizar la sesión o apagar el equipo. A ello se suman los ataques con malware sofisticado o ransomware, que secuestra y cifran la información, también eliminan metadatos, sobrescriben archivos en el espacio no asignado y ejecutan borrados seguros, reduciendo al mínimo las posibilidades de recuperación. Es por

eso que en tales casos, aunque sea posible detectar el código malicioso, vincularlo con su origen o con una dirección de ataque específica resulta sumamente difícil.

Otro factor que agrava la dificultad investigativa es la ausencia de administración técnica en el entorno afectado. Tanto Bastidas como Vargas señalan que las redes domésticas o los sistemas improvisados carecen de mecanismos de registro y monitoreo, lo que impide contar con logs históricos o configuraciones de seguridad que permitan reconstruir los hechos. Incluso en los casos en que la infraestructura sí existe, si no hay una detección oportuna y la recolección de evidencia no se inicia de inmediato, el carácter efímero de los datos digitales puede conducir a su pérdida irreversible.

Otro factor que agrava la dificultad investigativa es la ausencia de administración técnica en el entorno afectado. Tanto Bastidas como Vargas señalan que las redes domésticas o los sistemas improvisados carecen de mecanismos de registro y monitoreo, lo que impide contar con logs históricos o configuraciones de seguridad que permitan reconstruir los hechos. Incluso en los casos en que la infraestructura sí existe, si no hay una detección oportuna y la recolección de evidencia no se inicia de inmediato, el carácter efímero de los datos digitales puede conducir a su pérdida irreversible. También , muchas veces, cuando un perito llega al lugar de los hechos, el sistema ya ha sido apagado, reiniciado o manipulado por usuarios que sin mala intención, borran sin saberlo rastros esenciales para el caso. Otras veces, las autoridades dependen de dispositivos o programas especializados que no están disponibles en el momento y lugar donde se requiere, lo que obliga a solicitar apoyo a terceros como proveedores de servicios de internet o empresas que administran plataformas digitales.

El problema se agrava cuando el atacante usa herramientas diseñadas para ocultar su huella. Tecnologías como redes privadas virtuales (VPN), proxys encadenados o el navegador

Tor que permiten modificar la ubicación aparente del usuario y dificultan seguir la pista hasta llegar a la persona real detrás del ataque.

Este contraste entre lo que es técnicamente posible y lo que las condiciones reales permiten marca una gran diferencia en los resultados. Un delito que parece sencillo de investigar puede complicarse por una respuesta tardía, una mala configuración de los sistemas o la astucia de un agresor que sabe cómo borrar sus huellas. Por el contrario, un caso que se proyectaba como difícil puede resolverse con rapidez si se detecta a tiempo, hay registros claros y existe coordinación entre quienes investigan, procesan y juzgan. Por eso, la complejidad investigativa en el ámbito de los delitos informáticos no es una etiqueta fija que dependa únicamente del tipo penal: es un escenario cambiante, moldeado por la tecnología, la velocidad de reacción y la capacidad de trabajar en equipo.

2.3 Trazabilidad de la evidencia digital

La trazabilidad de la evidencia digital es uno de los pilares que sostiene cualquier investigación penal en el terreno de los delitos informáticos. En pocas palabras, es la capacidad de seguir el rastro de la información desde el momento exacto en que se detecta hasta el día en que se presenta frente a un juez, asegurando que en todo ese recorrido permanezca intacta y que cada acción sobre ella quede registrada y pueda explicarse sin vacíos.

Cuando la intrusión sucede en entornos bien estructurados como las redes de una empresa o de una entidad pública con un equipo técnico competente el camino para los investigadores es mucho más claro. En estos escenarios, cada movimiento deja huella de forma automática: servidores que almacenan detallados logs de acceso, cortafuegos que guardan historiales de actividad, sistemas que detectan intrusiones, copias de seguridad programadas y protocolos de seguridad que se cumplen rigurosamente. Con este respaldo, los

peritos pueden reconstruir casi de forma cronológica y precisa cómo se llevó a cabo el ataque. Como relató Héctor Vargas, en algunos casos incluso se logra capturar información “en vivo” mientras la agresión digital está ocurriendo, conservando datos de sesión, fragmentos de memoria y tráfico de red que, de otra manera, se perderían en cuestión de segundos.

Sin embargo, el escenario cambia radicalmente cuando la intrusión se da en redes domésticas o en sistemas sin administración técnica. Bastidas resaltaba que, en este tipo de entornos, muchas veces no existen registros históricos confiables y la información sobre conexiones o accesos puede sobrescribirse o eliminarse automáticamente. Un simple reinicio de equipo o el apagado del dispositivo puede borrar evidencia crucial. Aquí, la trazabilidad se convierte en una carrera contrarreloj: cada minuto cuenta, y cualquier demora puede significar la pérdida irreversible de datos que serían clave para la investigación.

A estas dificultades se suman las estrategias deliberadas que emplean los atacantes para ocultar su rastro. El uso de redes privadas virtuales (VPN), proxys encadenados, el navegador Tor o direcciones IP dinámicas fragmenta el camino que debería seguir la investigación, obligando a los fiscales y peritos a solicitar información a múltiples proveedores de servicios, muchas veces ubicados en diferentes países. Jonathan Masso advertía que esta fragmentación no solo retrasa el proceso, sino que, en la práctica, puede llevar a que, cuando se recibe la respuesta, la información solicitada ya haya sido borrada por políticas internas de retención de datos, que en algunos casos no superan los treinta días.

Este panorama revela que la trazabilidad no depende únicamente de la pericia técnica de los investigadores, sino también de la cooperación oportuna de actores externos, desde empresas proveedoras de servicios hasta organismos internacionales. La rapidez con la que se cursa una solicitud, la claridad del lenguaje utilizado y la existencia de protocolos

estandarizados para estas interacciones son factores determinantes. Sin ellos, incluso con herramientas forenses de última generación, el trabajo puede verse afectado.

En el plano jurídico, la trazabilidad está íntimamente vinculada con la cadena de custodia, que en Colombia encuentra sustento normativo en la Ley 906 de 2004 y en los lineamientos técnicos de la Fiscalía General de la Nación. Es la garantía de que la prueba que se presenta en juicio es la misma que se obtuvo en la investigación, sin alteraciones ni manipulaciones indebidas. La literatura técnica resalta que la cadena de custodia informático-forense debe incorporar procedimientos controlados desde la localización de evidencia hasta su valoración judicial, garantizando supervisión en cada etapa para evitar adulteraciones o pérdidas, tal como lo exponen Arellano & Castañeda (2012). Un fallo en este punto puede llevar a que el juez declare la inadmisibilidad de la evidencia, anulando meses de trabajo. Como bien señalaban los entrevistados, la integridad probatoria no solo se pierde por errores evidentes, como la alteración directa de un archivo, sino también por omisiones documentales mínimas, como no dejar constancia de la herramienta utilizada para extraer un dato o del funcionario que tuvo acceso a él en determinado momento.

Las guías internacionales sobre evidencia electrónica insisten en protocolos de preservación y cadena de custodia estricta: el UNODC recomienda procedimientos específicos para asegurar integridad, autenticidad y trazabilidad de los datos digitales desde su recolección hasta su presentación en juicio (UNODC, s.f.). Estas recomendaciones ayudan a definir estándares técnicos que complementen las exigencias procesales internas. (UNODC, Handling of digital evidence).

La trazabilidad también tiene un componente preventivo: comienza mucho antes de que se cometa el delito. La existencia de configuraciones de seguridad adecuadas, políticas de registro y monitoreo, y personal capacitado para responder a incidentes son la base para que,

llegado el momento, los investigadores cuenten con datos confiables. En ese sentido, la capacitación de administradores de sistemas, el diseño de planes de contingencia y la concienciación de usuarios comunes sobre la importancia de no alterar dispositivos tras un incidente son tan relevantes como las herramientas forenses más avanzadas.

La trazabilidad de la evidencia digital es el puente que conecta la tecnología con la justicia. Sin ella, la prueba se convierte en un dato aislado, susceptible de ser cuestionado y, en última instancia, descartado. Garantizarla requiere una suma de esfuerzos coordinados: infraestructura tecnológica sólida, peritos especializados, fiscales y jueces formados en la comprensión de evidencia digital, y canales de cooperación que respondan a la velocidad que exige el mundo digital. Tal como coincidieron Bastidas, Vargas y Masso, en el universo de los delitos informáticos la trazabilidad no es un lujo, sino la línea vital que puede marcar la diferencia entre una condena y un caso más archivado en la estadística de la impunidad.

2.4 Herramientas técnicas y jurídicas complementarias para el análisis de evidencia digital

Una vez asegurada la evidencia digital y garantizada su trazabilidad, el siguiente objetivo para los investigadores es transformarla en prueba sólida, inteligible y jurídicamente defendible. Lo cual ,exige un trabajo conjunto entre especialistas técnicos y operadores judiciales, pues la evidencia digital, por sí sola, rara vez “habla” de forma clara; necesita ser interpretada dentro de un contexto legal preciso.

En la práctica, el análisis forense digital requiere herramientas capaces de procesar y examinar información sin alterar su contenido original. Entre las más utilizadas a nivel institucional y por laboratorios forenses se encuentran programas como EnCase, FTK, Magnet AXIOM y Autopsy, así como utilidades específicas para

análisis de memoria como Volatility. Estas aplicaciones permiten reconstruir la actividad de un sistema, recuperar archivos eliminados, examinar metadatos y detectar patrones de intrusión. Según lo explicó Jonathan Londoño, no se trata únicamente de encontrar un archivo comprometedor, sino de entender cuándo, cómo y bajo qué circunstancias fue creado o modificado, y si su contenido coincide con los hechos investigados.

En el plano jurídico, todo hallazgo técnico debe someterse a los filtros que impone el proceso penal para que pueda ser valorado por un juez. Aquí entran en juego herramientas como la cadena de custodia, los protocolos de manejo y la validación de las herramientas forenses utilizadas. Héctor Vargas advirtió que la jurisprudencia colombiana ha sido clara en que cualquier ruptura en la continuidad de la custodia, o el uso de métodos no confiables, puede llevar a la exclusión de pruebas, incluso si estas contienen información incriminatoria evidente.

Casos recientes han evidenciado que la ausencia de comprobantes técnicos como el código hash o la dependencia de versiones impresas sin verificación digital puede llevar a la exclusión de evidencia, debilitando los procesos penales. Esta problemática ha sido destacada en estudios que alertan sobre la urgencia de adaptar protocolos a la naturaleza volátil de la información digital (Sanabria, 2025).

El análisis se vuelve más complejo cuando la información relevante está alojada en plataformas privadas, especialmente si estas son extranjeras. Redes sociales, servicios de mensajería y proveedores de almacenamiento en la nube poseen registros esenciales para la investigación, pero acceder a ellos exige conocer los procedimientos

de solicitud y también actuar con rapidez para evitar la pérdida de datos por políticas automáticas de eliminación. En este punto, Bastidas enfatizó que la cooperación con el sector privado es tanto una herramienta como un desafío: cuando funciona, acelera la investigación; cuando falla, puede cerrarla antes de tiempo.

Además, el uso de herramientas técnicas debe ir acompañado de habilidades para interpretar sus resultados en clave jurídica. Un reporte forense extenso y detallado pierde valor si no se explica de forma comprensible para el juez, o si no se conecta directamente con los elementos del tipo penal que se busca demostrar. Ricardo de la Pava subrayó que la comunicación entre peritos, fiscales y jueces es tan importante como el software empleado, ya que sin un lenguaje claro, los hallazgos técnicos pueden pasar inadvertidos o ser malinterpretados.

El debate jurídico colombiano también ha destacado que la protección constitucional de la prueba digital exige reforzar la cadena de custodia como garantía de integridad y debido proceso. Según Ámbito Jurídico (2018), la alteración mínima de un archivo electrónico puede invalidar toda la prueba, lo que obliga a implementar protocolos especializados que trasciendan la regulación general.

2.5 Marco Normativo y estándares internacionales aplicables a la Evidencia Digital en Colombia

En el proceso penal colombiano, la evidencia digital se apoya en una combinación de normatividad colombianas, cooperaciones internacionales y

estándares técnicos a esto nos referimos sobre los protocolos que se deben seguir de acuerdo a cada prueba a recolectar que los encargados siempre serán personas especializadas en el tema en Colombia estaríamos hablando del policía judicial, por lo cual no podemos encajar esta evidencia en un solo marco normativo ya que esta se encuentra regulada en multiplicidad de normas pero que todos van encaminados a un propósito común: que la información recolectada en el transcurso de una investigación pueda llegar a juicio con plena validez y autenticidad ya que la prueba se le pueda dar valor probatorio debe de mantener la esencia de la misma, sin modificaciones, alteraciones, sin que en el camino se vulneren derechos fundamentales del victimario ya que si esto sucede estamos en el riesgo que posteriormente estas información recolectada sea ilegal o ilícita y a sí mismo ser excluida de ser valorada. A diferencia de la evidencia física, que suele conservarse con autenticidad con el paso del tiempo, la digital es frágil y volátil; basta un solo minuto inclusos segundos para que se altere, se duplique o desaparezca sin dejar rastro. La naturaleza de la prueba en delitos informáticos es efímera, es muy rápida por lo que obliga a que su manejo sea por protocolos estrictos pero a su vez sean implementados muy rápidamente y adicionalmente exista una coordinación inmediata entre todos los operadores que intervienen en la investigación, debe existir una estrecha comunicación entre los peritos forenses, informáticos y el fiscal, el perito manteniendo sus protocolos que garantiza la prueba y el fiscal realizando todos los controles de legalidad pertinentes para que este pueda llegar a juicio y se le de valor probatorio.

En el marco interno, la Ley 906 de 2004 reconoce expresamente la validez de la prueba digital, pero condiciona su admisibilidad a que se respeten ciertos principios básicos: la legalidad, que exige que la obtención de los datos esté prevista en la ley y, cuando corresponda, cuente con autorización judicial esto también conocido como controles posteriores y anteriores a la actuación que realizará el especialista; la autenticidad, que demanda demostrar que los registros son genuinos y corresponden fielmente a la fuente original; la integridad, que asegura que la información no se ha modificado desde el momento de su recolección; y la continuidad, garantizada a través de la cadena de custodia, que obliga a dejar constancia de cada traslado, análisis o manipulación. Esta última es, en palabras de muchos investigadores, la columna vertebral del sistema probatorio: sin una cadena de custodia impecable, incluso la mejor prueba técnica pierde su valor. Héctor Vargas lo advertía con claridad al señalar que un descuido mínimo en este proceso puede anular por completo un material que, en lo técnico, sería intachable. Su reflexión deja ver que no basta con tener normas escritas; se requiere disciplina, entrenamiento constante y una verdadera cultura institucional de cuidado extremo en el manejo de la información digital.

La Ley 1273 de 2009, por su parte, incorporó al Código Penal un catálogo de delitos informáticos que va desde el acceso abusivo a sistemas hasta la violación de datos personales. Esta regulación cumple una doble función: tipificar las conductas reprochables y orientar la labor investigativa al delimitar los elementos que deben acreditarse en juicio. Sin embargo, como señalaba Samir Bastidas, el problema no radica tanto en el contenido de la ley que está alineado con las categorías

internacionales sino en la capacidad operativa de las autoridades para aplicarla porque muchas unidades carecen de los recursos técnicos adecuados y se dificulta abordar conductas sofisticadas en las que la evidencia desaparece rápidamente o se oculta mediante técnicas antiforenses.

En el ámbito internacional, la adhesión de Colombia al Convenio de Budapest en 2018 significó un paso decisivo al establecer medidas como la conservación inmediata de registros y el acceso a datos transfronterizos de tráfico o suscriptores. Estos mecanismos fortalecen la capacidad investigativa frente a delitos que trascienden fronteras. No obstante, la práctica muestra sus límites porque lo que se denomina cooperación "rápida" puede resultar insuficiente en un contexto donde la información desaparece en cuestión de horas o incluso minutos. Como subraya Bastidas, el desfase entre los tiempos de la cooperación judicial y la volatilidad de la evidencia digital sigue siendo uno de los grandes desafíos.

El marco se complementa con estándares técnicos de alcance global, entre los que se destaca la ISO/IEC 27037, que ofrece directrices sobre identificación, recolección y preservación de evidencia digital. Aunque no es de obligatorio cumplimiento, ha influido en los manuales internos de la Fiscalía y la Policía Judicial. A ello se suman las guías de INTERPOL y de la Oficina de Naciones Unidas contra la Droga y el Delito, que buscan unificar procedimientos para el análisis forense y la cooperación entre países. Masso destaca que estas herramientas permiten que los investigadores compartan un lenguaje técnico y jurídico común, pero advierte que en Colombia su aplicación real se ve limitada por la falta de entrenamiento y recursos en muchas regiones. En la práctica, los estándares suelen aplicarse con rigor en grandes

ciudades, mientras que en zonas apartadas la realidad obliga a recurrir a soluciones improvisadas que ponen en riesgo la validez de la prueba.

Todo este andamiaje normativo y técnico, se enfrenta a una realidad incontestable de que la efectividad depende únicamente de lo que dicen las leyes o los tratados y de la capacidad de reacción de las instituciones. El tiempo es un factor crítico, porque cualquier demora puede borrar de manera irreversible la huella digital del delito. Igualmente crucial es la coordinación entre fiscales, jueces, peritos y proveedores de servicios tecnológicos, cuya articulación marca la diferencia entre una investigación exitosa y una que se pierde en vacíos procedimentales. A esto se suma la necesidad de laboratorios forenses bien equipados, licencias de software actualizado y una capacitación permanente que permita a los operadores adaptarse al ritmo acelerado de la tecnología.

2.6 Reflexiones finales sobre las herramientas técnicas y jurídicas en la investigación de evidencia digital

El recorrido por las herramientas jurídicas y técnicas disponibles en el proceso penal colombiano para enfrentar los delitos informáticos permite advertir que este campo se mueve en una constante tensión entre lo ideal y lo posible. Sobre el papel, el país cuenta con un marco normativo coherente y relativamente actualizado: la Ley 906 de 2004 consagra los principios procesales que sostienen la validez de la prueba digital, la Ley 1273 de 2009 tipifica de manera específica las conductas que lesionan bienes jurídicos informáticos, y la adhesión al Convenio de Budapest en 2018 conectó a Colombia con un entramado internacional diseñado para dar respuestas rápidas y

coordinadas a fenómenos criminales transnacionales. A ello se suman estándares técnicos como la ISO/IEC 27037 o las guías de INTERPOL y la Oficina de Naciones Unidas contra la Droga y el Delito, que proporcionan lineamientos claros sobre cómo identificar, recolectar y preservar evidencia digital.

No obstante, el verdadero campo de batalla se encuentra en la práctica diaria de fiscales, jueces y peritos. Como lo señalaron los entrevistados, la existencia de la norma y de los estándares no garantiza por sí sola que la evidencia digital llegue intacta al juicio. La volatilidad de la información digital exige respuestas inmediatas, equipos forenses especializados y una disciplina rigurosa en la cadena de custodia. Héctor Vargas fue enfático en que un mínimo descuido en la documentación de la custodia puede dejar sin valor un elemento técnicamente impecable, lo cual revela que el éxito investigativo depende tanto de la pericia jurídica como del cuidado minucioso en los procedimientos técnicos.

Samir Bastidas, por su parte, advirtió que la Ley 1273 de 2009 es coherente con las categorías internacionales de ciberdelito, pero que su aplicación real tropieza con limitaciones materiales: no todas las unidades investigativas cuentan con laboratorios equipados, software forense actualizado o personal entrenado para enfrentar conductas donde la evidencia se borra rápidamente o se esconde bajo técnicas antiforenses. Esto genera una brecha evidente entre la sofisticación de los agresores y las capacidades institucionales de respuesta.

Masso aportó otra perspectiva al destacar que los estándares internacionales cumplen una función de unificación, al permitir que investigadores de distintos países

compartan un lenguaje técnico y jurídico común. Sin embargo, también subrayó que en Colombia su implementación es desigual: mientras en las grandes ciudades existen grupos especializados que aplican con rigurosidad estas guías, en regiones apartadas la carencia de recursos obliga a improvisar soluciones que ponen en entredicho la validez de la prueba. Este contraste entre centro y periferia refleja una deuda pendiente en materia de descentralización de capacidades y acceso equitativo a la justicia.

La cooperación internacional se presenta como un elemento indispensable pero al mismo tiempo problemático. El Convenio de Budapest promete mecanismos de preservación rápida y acceso transfronterizo a datos, pero la experiencia demuestra que lo "rápido" en términos de derecho internacional muchas veces resulta lento frente a la inmediatez con la que desaparece la evidencia digital. Esta tensión temporal se convierte en uno de los mayores retos del proceso penal en delitos informáticos: mientras los datos pueden evaporarse en minutos, las solicitudes de cooperación pueden tardar días o semanas en concretarse.

Más allá de la norma, el factor tiempo, la infraestructura disponible y la coordinación interinstitucional marcan la diferencia entre una investigación exitosa y una fallida. Los delitos informáticos que dejan huellas más claras como el acceso abusivo a un sistema o el uso de malware resultan más accesibles a la investigación, mientras que aquellos con evidencia efímera como la interceptación ilícita de datos o la violación de datos personales suelen quedar sin resolver. Este panorama evidencia que la política criminal debe avanzar hacia estrategias diferenciadas que fortalezcan las capacidades institucionales y reduzcan la brecha entre el potencial probatorio de la evidencia digital y su real utilización en juicio.

En conclusión, el proceso penal colombiano ha dado pasos importantes para integrar la evidencia digital en su engranaje normativo y técnico, pero todavía enfrenta un reto estructural: transformar la letra de la ley y los estándares internacionales en prácticas efectivas, uniformes y sostenibles en el tiempo. Esto supone invertir en laboratorios forenses, garantizar entrenamiento permanente a fiscales, jueces y peritos, y fortalecer los canales de cooperación tanto a nivel interno como internacional. Solo así será posible cerrar la distancia entre lo que hoy existe como posibilidad en el papel y lo que en la realidad institucional se traduce en investigaciones truncadas. La evidencia digital, por su fragilidad y relevancia, no admite improvisaciones: exige rigor, coordinación y compromiso estatal para que las investigaciones no se pierdan en vacíos procedimentales y logren su propósito último, que es garantizar justicia en un entorno cada vez más digitalizado.

CAPITULO lll

Desafíos Técnicos y Jurídicos en la Investigación y Juicio de Delitos Informáticos: Perspectivas de los Actores del Proceso Penal

3.1 Introducción

Los delitos informáticos han empezado a ocupar un lugar importante dentro del derecho penal, porque involucran dinámicas muy distintas a las que tradicionalmente se han

manejado siempre en el sistema judicial. En estos casos, hay que entender el hecho en términos jurídicos, saber quién lo cometió, cómo se obtuvo la información digital y qué valor tiene esa prueba dentro del proceso y es necesario que el derecho se combine con herramientas de investigación, conocimientos técnicos y una mirada crítica sobre cómo funcionan realmente las instituciones encargadas de adelantar estos casos, teniendo en cuenta las limitaciones y condiciones en las que trabajan jueces, fiscales, defensores e investigadores.

En el contexto colombiano, se han establecido herramientas normativas para enfrentar estas conductas. La Ley 1273 de 2009 introdujo tipos penales que regulan situaciones como el acceso indebido a sistemas, el daño informático, la interceptación de datos y el uso de software malicioso. A su vez, la Ley 906 de 2004 plantea un procedimiento penal que contempla mecanismos para investigar y juzgar estos delitos. Sin embargo, los registros muestran que gran parte de los casos se queda en etapa de indagación y pocos logran avanzar hacia fases como la imputación, la acusación o el juicio oral generando un interrogante sobre qué ocurre en la práctica.

Aunque fiscales, jueces, defensores e investigadores tienen roles distintos, todos enfrentan problemas similares cuando se trata de investigar delitos que exigen conocimientos técnicos, el uso de tecnologías actualizadas, protocolos claros y una coordinación efectiva entre las distintas entidades. Así que es necesario ver qué pasa en la práctica. En su trabajo diario, estos operadores deben tomar decisiones en medio de una alta carga laboral, con escasa formación especializada, recursos limitados y sin una línea jurisprudencial consolidada sobre la valoración de la prueba digital.

Con el propósito de entender más a fondo por qué esto ocurre, este capítulo recoge las voces de cuatro operadores jurídicos que han estado cara a cara con estas problemáticas: el

juez penal del circuito Andrés Felipe Arango Giraldo, el abogado litigante Jonathan Londoño, el ex magistrado Ricardo de la Pava y el juez Jhon Rojas.

A través de un análisis temático que articula sus reflexiones, se identifican factores que según los entrevistados , explican el estancamiento de estos procesos como vacíos normativos que dejan sin respuesta ciertas conductas, enormes dificultades para recolectar y valorar pruebas digitales, falta de formación especializada, escasa prioridad institucional, desarticulación entre las entidades involucradas y una cultura jurídica que aún no logra dimensionar la gravedad y el impacto de estos delitos.

Se basa en un enfoque cualitativo sustentado en entrevistas a operadores judiciales que han tenido experiencia directa en el tratamiento de delitos informáticos donde buscaremos ofrecer una visión más cercana a las dinámicas reales del sistema, visibilizar las limitaciones que enfrentan quienes tienen a cargo estas investigaciones.

3.2 Evaluación de la efectividad de las entidades judiciales en la etapa de investigación y juicio de los delitos informático

Contexto y limitaciones del sistema judicial ante los delitos informáticos

La expansión de las tecnologías digitales ha cambiado de gran manera nuestra forma de vivir. Hoy, gran parte de nuestra rutina transcurre frente a una pantalla: A quienes amamos los saludamos diariamente con un mensaje de texto, compartimos momentos importantes a través de una videollamada, trabajamos desde la comodidad del hogar, tomamos clases en línea desde cualquier lugar del mundo y gestionamos desde lo más simple hasta lo más complejo en solo minutos que antes nos tomaban horas. Esto ha creado un contexto y un entorno lleno de oportunidades y beneficios logrando que la tecnología sea una compañera cotidiana, casi invisible pero indispensable que también ha conseguido que los delitos

informáticos se abran paso volviéndose cada vez más comunes. Los cuales tienen un impacto directo en las víctimas vulnerando su intimidad, información financiera y hasta su identidad mediante medios digitales, sino que también impacta y pone a prueba la capacidad de las instituciones encargadas de garantizar justicia. Las cuales, veían este problema como lejano y técnico. Pero se ha vuelto una realidad cotidiana que afecta a personas del común, empresas de todas las magnitudes y también a instituciones públicas., Y aunque la Ley 1273 de 2009 establece un marco legal para enfrentar este tipo de delitos, la capacidad del sistema judicial para abordar eficazmente estos casos es objeto de debate y revisión constante.

El estudio *Eficacia del Estado Colombiano para la Judicialización de los Delitos Informáticos* destaca que la Ley 1273 de 2009 representó un avance importante en materia penal, pero que el marco normativo a la fecha no resulta lo necesariamente suficiente para enfrentar conductas delictivas recientes. Al respecto, el exmagistrado Ricardo de la Pava advierte que "el marco normativo no está preparado para fenómenos como el ransomware o el uso malicioso de inteligencia artificial", lo cual obliga a fiscales y jueces a aplicar de manera forzada tipos penales tradicionales a conductas nuevas, generando así inseguridad jurídica. Los delitos cibernéticos son como un monstruo que cambia de forma cada día adaptándose y aprovechándose de cada nueva vulnerabilidad que surge en la red. Lo que hoy parece una barrera de seguridad mañana puede ser un punto débil, y así, casi sin darnos cuenta, la ciberdelincuencia se reinventa siempre y parece estar un paso por delante haciendo que nuestro sistema judicial se encuentre en una carrera contra el tiempo, con herramientas tradicionales que muchas veces ya no bastan para hacerle frente y que haya una brecha técnica que limita para la hora de actuar. Esto exige que fiscales, jueces y policías judiciales cuenten con formación específica en análisis de pruebas digitales, técnicas de rastreo en la red y manejo de evidencia electrónica. Lo cual debido a que muchos casos se diluyen en tecnicismos, las pruebas pierden valor por mal manejo o no se logra establecer la

responsabilidad penal de quienes cometen estos actos, así mismo como lo sostiene El juez penal del circuito Andrés Felipe Arango Giraldo que señala "la prueba digital es tan volátil que si no se asegura de inmediato, se pierde; y lamentablemente, muchas veces, cuando llega a audiencia, ya no tiene valor probatorio". En la misma línea, el abogado litigante Jonathan Londoño enfatiza que "el tiempo es enemigo del proceso en estos delitos: cada día que pasa sin actuar reduce las posibilidades de éxito".

Otro aspecto importante que no debemos ignorar es la falta de herramientas tecnológicas para llevar a cabo la investigación digital. Para obtener y analizar pruebas electrónicas no basta con voluntad y conocimiento, se necesita de equipos y software especializados, pero muchas entidades judiciales en el país aún carecen de estos recursos básicos. Estas carencias no solo son limitantes técnicas, sino que es una puerta que se le cierra a quienes buscan justicia. Solo nos basta con imaginar la frustración que sentiríamos al saber que nuestra información personal fue robada o que tu vida digital fue vulnerada, y ver cómo los investigadores no cuentan con las herramientas necesarias, no pueden hacer más que enfrentarse a un muro invisible que oculta a los responsables. Sin estas herramientas, rastrear actividades ilícitas en la web se vuelve más complejo, se dificulta la identificación de los responsables y se pone en riesgo la solidez de las pruebas en juicio.

Además, la lentitud en los procesos judiciales dificulta que las investigaciones sean realmente efectivas. En el mundo físico esperar es duro; pero la tecnología avanza tan rápido que la información importante puede desaparecer o volverse inaccesible en poco tiempo, en este caso el tiempo es aún más cruel. Sin embargo, muchos casos se alargan tanto que, cuando finalmente se recopilan las pruebas, pueden haber perdido su valor debilitando las investigaciones y haciendo que también se lleve a que los casos queden archivados, dejando a las víctimas sin respuestas y a los responsables en libertad.

El informe de Asobancaria sobre la eficiencia de la Ley 1273 de 2009 pone en evidencia una discrepancia notable entre el número de denuncias y la cantidad de condenas que finalmente se logran. Aunque la ley ha permitido tipificar y perseguir delitos como el acceso abusivo a sistemas informáticos y la interceptación de datos, en la práctica, muchos casos no logran avanzar más allá de la etapa de investigación.

Una problemática principal es la gran dificultad para identificar a los responsables, más que todo cuando operan desde el extranjero. Los ciberdelincuentes se encuentran protegidos en un anonimato casi total con frecuencia suelen utilizar VPN, direcciones IP dinámicas y sistemas de cifrado avanzado, logrando que sea más complejo rastrear su ubicación. Adicionalmente, la cooperación entre países lo hace más desesperante porque todavía enfrenta varias barreras y complica el intercambio de información y la coordinación de investigaciones internacionales.

Detrás de todo este panorama estructural, hay un aspecto que a menudo queda invisibilizado: el impacto humano. Cuando hablamos de delitos informáticos no nos referimos sólo a cifras y datos abstractos. Cada ataque informático, cada acceso indebido a un sistema o cada robo de datos personales no es simplemente una cifra en una estadística. Son personas que pierden su tranquilidad, su dinero o su confianza en el entorno digital. Empresas que ven comprometidos sus años de esfuerzo y su futuro. Instituciones públicas que deben reconstruir su credibilidad. El costo de estos delitos, aunque difícil de cuantificar en su totalidad, tiene una dimensión profundamente social y emocional que el sistema judicial aún tiene el desafío de reparar completamente estas heridas que aún no alcanza plenamente.

Además de estos obstáculos, un desafío creciente es la aparición de nuevas formas de ciberdelincuencia, como el Ransomware y los delitos cometidos mediante herramientas de inteligencia artificial, fenómenos que actualmente no tienen un desarrollo normativo

específico en Colombia. Estos vacíos normativos dificultan la judicialización porque obligan a adaptar tipos penales tradicionales a nuevas conductas digitales, generando incertidumbre en fiscales y jueces. Así mismo, el incremento de denuncias sin respuesta oportuna refleja la saturación que vive el sistema judicial, un fenómeno que afecta a la justicia penal en general, pero que en el ámbito de los delitos informáticos se amplifica debido a la naturaleza técnica y volátil de las pruebas digitales.

3.3 Esfuerzos institucionales frente al crecimiento de los delitos informático

Por otro lado, en respuesta a la gravedad del fenómeno de los delitos informáticos en Colombia, las instituciones del Estado como la Fiscalía General de la Nación, consciente de la necesidad de un enfoque especializado, mediante la resolución 117 de 2023 por medio de la cual se reglamenta y conforma la Dirección Especializada Contra los Delitos Informáticos que está integrada por fiscales e investigadores que cuentan con formación específica y actualizada. La Policía Nacional, a su vez, fortalece continuamente su Centro Cibernético Policial, desarrollando plataformas como el CAI Virtual que permite a los ciudadanos reportar delitos informáticos desde cualquier lugar y ha impulsado capacitaciones en ciberseguridad entendiendo que la prevención es tan importante como la sanción. También es relevante destacar que Colombia se adhirió en 2018 al Convenio de Budapest, el principal tratado internacional que fomenta y regula la cooperación frente a la ciberdelincuencia con herramientas legales para colaborar con otros países en la recolección de pruebas, el intercambio de información y la extradición de responsables, algo vital cuando los ciberdelincuentes actúan desde fuera del territorio nacional. Sin embargo, su alcance aún es limitado frente al tamaño del problema.

Las cifras recientes nos permiten entender la magnitud de la situación y, más importante aún, ponen rostro a las personas que sufren las consecuencias de estos delitos.

Según la Fiscalía, entre octubre de 2022 y diciembre de 2023, se lograron solo 69 capturas, 45 imputaciones, 15 escritos de acusación y 6 condenas. Todo esto frente a un mar de casi 79.000 denuncias relacionadas con delitos informáticos. Estos números, aunque impactantes, reflejan solo una parte de la realidad, pues cada uno de estos casos representa una vida afectada, un daño que no siempre recibe la atención ni la respuesta que merece.

La Policía Nacional reportó que en 2023 se registraron 54.121 denuncias por ataques cibernéticos, una cifra alarmante pero que también revela que, en apenas dos años, estos delitos crecieron un 79% respecto a 2021. Este aumento nos permite evidenciar lo vulnerables que somos como sociedad en relación con este fenómeno tan difícil de contener.

Además, si bien en algunos sectores se han logrado avances importantes, estos aún resultan insuficientes frente a la magnitud del problema. Un ejemplo de esto es que en el sector financiero colombiano Asobancaria reportó que a pesar de enfrentarse a aproximadamente 43 ciberataques por segundo el 99,99% de las transacciones digitales no presenta reclamaciones por fraude mostrando notablemente que el sector privado hace un gran esfuerzo en la mitigación de riesgos, pero también que la protección no es de la misma manera en todos los sectores, y que muchos ciudadanos, pequeñas empresas y entidades públicas siguen expuestos y desprotegidos ante el cibercrimen porque mientras los bancos y grandes compañías blindan sus sistemas, las personas del común de nuestro país no cuentan con la información o los medios para protegerse

Frente a este panorama, es evidente que, aunque las acciones institucionales como la creación de unidades especializadas y la adhesión a tratados internacionales han representado avances importantes, la brecha entre el crecimiento de los delitos informáticos y la capacidad de respuesta de nuestro sistema sigue siendo muy profunda. Las víctimas no solo enfrentan pérdidas económicas de las cuales muchas veces tristemente no se logran recuperar, sino

también una sensación creciente de que sus historias quedan invisibilizadas siente vulnerabilidad, desconfianza en el entorno digital y, en muchos casos, en la misma posibilidad de acceder a la justicia.

Vale la pena destacar que, en 2023, Colombia presentó la Estrategia Nacional de Ciberseguridad 2023-2027, una señal clara de que el país está empezando a tomar en serio los riesgos del mundo digital y el deber de proteger a sus ciudadanos frente a ellos. Lo cual, representa un esfuerzo por acercar la justicia y la seguridad a quienes más lo necesitan, especialmente a quienes se sienten vulnerables frente a las amenazas en línea y es importante para construir un entorno digital más seguro, más justo y humano.

3.4 Análisis crítico de la efectividad en la investigación y judicialización de los delitos informáticos

El proceso judicial en Colombia continúa arrastrando fallas estructurales que dificultan que se obtenga una respuesta oportuna y eficaz. La falta de tiempos de reacción adecuados y una alta congestión procesal, hace que muchos casos se enfrenten a demoras que terminan debilitando las pruebas que en muchos casos llevan al archivo del proceso sin resultados concretos que impiden que se esclarezcan los hechos e igualmente afecta la percepción de legitimidad del sistema judicial en su conjunto generando una imagen de impunidad que trasciende al caso particular. Por eso, cada proceso que se extiende indefinidamente o se diluye en la inacción institucional representa una oportunidad perdida para fortalecer la respuesta frente al cibercrimen ya que se refleja una necesidad urgente de modernizar y adaptar los mecanismos judiciales, de modo que puedan responder con agilidad y efectividad a las dinámicas cambiantes del delito en línea.

Lejos de encontrar alivio en la justicia, muchas víctimas cargan con doble dolor del trauma provocado por el ataque y luego, la angustia de ver cómo su caso se pierde en un mar

de demoras y falta de respuestas. Los retrasos, cada notificación que no llega, audiencias que se aplazan, reabren las heridas y prolonga el sufrimiento. La revictimización, no es solo una forma de revivir el daño causado, sino sentirse abandonadas, e ignoradas por quienes debían protegerlas en su momento más vulnerable. Si las personas perciben que la justicia es inaccesible o ineficaz, es mucho menos probable que se acerquen a las autoridades a denunciar los delitos porque la percepción de que los delincuentes no serán castigados y que el proceso judicial será largo y poco transparente desmotiva enormemente a las víctimas a dar el paso de presentar una denuncia y contribuye a que la magnitud de la ciberdelincuencia no se refleje correctamente en las estadísticas oficiales. Y de la misma manera que si quienes cometen el delito sienten que las probabilidades de ser capturados y procesados son bajas, se sienten motivados a seguir cometiendo delitos. Es decir que la impunidad perpetúa la criminalidad en el ámbito digital porque se sienten seguros a la hora de operar y esta falta de consecuencias claras no solo incrementa la tasa de criminalidad, sino que debilita la confianza en el sistema judicial y en su capacidad para proteger a los ciudadanos.

3.4.1 Etapa de investigación

Durante esta fase, los entrevistados coincidieron en que en muchos casos se estancan por la falta de investigación identificación del agresor y porque las herramientas digitales utilizadas por los fiscales son insuficientes. El Dr. Rojas afirmó “Copiamos el sistema anglosajón sin importar las reglas de evidencia digital” lo que deja un vacío en la incorporación de pruebas. El Dr. Arango por su parte señaló que en esta parte preliminar muchos fiscales no saben cómo iniciar una investigación digital efectiva “No entienden ni siquiera que es un hash”. El Dr. De la Pava complementa “La aplicación práctica está desarticulada” y que si no existe una coordinación efectiva entre fiscalía, policía judicial y jueces. Coincidiendo así todos que la etapa de investigación se debilita por la falta de

capacitación de personal de estado, falta de protocolos claros y recursos humanos especializados.

3.4.2 Etapa formulación de la acusación y audiencias preparatorias.

En este punto, los entrevistados señalaron que las barreras técnicas y jurídicas en torno a la prueba digital, El Dr. Arango fue enfático: “el pantallazo de WhatsApp no es evidencia digital” advirtió que muchos jueces no tienen formaciones técnicas para valorar las pruebas lo que genera una inseguridad jurídica, desde esta perspectiva existe una tensión importante: no puede acceder a peritos técnicos con la misma facilidad que la fiscalía generando desigualdades procesales.

Asimismo, se resaltaron dificultades de carácter institucional. El Dr. De la pava “Los fiscales trabajan con cargas excesivas y poca prioridad para los delitos informáticos, lo que limita su capacidad de preparar imputaciones sólidas” A esto se le suma, como lo explico el Dr. Londoño, la falta de recursos económicos y técnicos para sostener investigaciones de larga duración, lo cual termina debilitando la acusación. En conclusión los jueces reclaman una mayor claridad en la estructuración de la teoría de caso mientras que los defensores señalan que la acusación suele llegar sin bases técnicas sólidas.

3.4.3 Juicio oral

Todos los entrevistados coincidieron en que esta fase es la menos activa para los delitos informáticos. El Dr. Londoño afirmo que “La impunidad de estos delitos supera el 98%”. Según el Dr. De la Pava, muchos fiscales no logran construir una teoría de caso solida porque “la evidencia digital no está bien preservada ni presentada” Los jueces, como explico el Dr. Rojas, deben decidir con pruebas insuficientes y sin equipos técnicos de apoyos, lo que puede generar fallos contradictorios. En esta fase hay tensiones muy fuertes y claras: La

fiscalía reclama la falta de apoyo institucional, la defensa cuestiona la debilidad de las pruebas y los jueces asumen la carga de decidir con vacíos probatorios.

3.5 Cooperación Internacional y casos relevantes

La naturaleza transnacional de muchos delitos informáticos exige que Colombia como país no enfrente solo la ciberdelincuencia. La conciencia de la cooperación internacional se ha venido reforzando mediante acciones concretas. Por ello, el Convenio de Budapest, que está vigente en el país desde 2008, se ha vuelto clave para facilitar la cooperación internacional. Es gracias a este tratado que Colombia puede intercambiar información y coordinar esfuerzos con otros Estados. Sin embargo, los procesos que requieren de colaboración internacional suelen tropezar con las diferencias de procedimientos legales, las demoras en las respuestas y en algunas ocasiones, la falta de recursos y de confianza entre las instituciones de distintos países.

Investigaciones colombianas como la de Valero, Ortiz Duarte & Lasso Mora (2019) muestran que la cooperación internacional se percibe como una estrategia necesaria pero con obstáculos reales, incluyendo diferencias legales y tecnológicas entre países, que retrasan la asistencia mutua.

En el año 2024 una red internacional de Phishing afectó a más de 480.000 personas en Colombia, Chile, Ecuador, Perú, España y Argentina. La operación, estuvo liderada por Europol y Ameripol, y dejó al descubierto que a los delincuentes digitales les basta con un computador y una conexión para entrar sin permiso en la vida de otros, aprovechándose de la confianza y la falta de información de la gente. Personas que, de un momento a otro, vieron cómo les vaciaban sus cuentas, les robaban sus datos o usaban su identidad. Perdieron dinero y tranquilidad. Vivieron con el miedo de no saber hasta dónde habían llegado sus datos y con

la sensación de haber perdido el control sobre su propia vida digital. Las autoridades lograron capturar a 17 personas y decomisar equipos utilizados para los fraudes. Sin embargo, aún hay líderes de esta organización esperando extradición, y eso revela que la justicia en muchos casos avanza de forma lenta, mientras las víctimas siguen esperando respuestas y garantías de que no volverán a vivir algo similar porque lo que se pierde no siempre se puede recuperar con solo un clic.

La cooperación internacional representa, ante todo, una oportunidad para el fortalecimiento conjunto de capacidades y el respaldo recíproco en la lucha contra la ciberdelincuencia. Cada país, con lo que tiene y sabe puede aportar desarrollo tecnológico o la formación especializada de sus equipos y para que esto sea verdaderamente eficaz es indispensable la idea de que la justicia global solo es posible si se construye de manera colaborativa teniendo en cuenta que no es fácil construir relaciones sólidas entre países que viven realidades muy distintas y priorizan de forma diferente. Las barreras culturales, las diferencias en los tiempos judiciales, los trámites legales e incluso en la manera de comunicarse, pueden frenar procesos que no dan espera porque lastimosamente en el mundo digital una prueba puede desaparecer en cuestión de horas y esto puede marcar la diferencia entre hacer justicia o no. Es por eso por lo que se debe considerar que, si los delitos digitales no se detienen ante fronteras, la justicia tampoco debería hacerlo. Porque solo cuando esas acciones se hacen realidad, es posible proteger a las personas que cada día confían en la tecnología para trabajar, aprender o simplemente conectarse con los demás. Así, se puede lograr tener un entorno digital seguro, donde la justicia sea una presencia constante y cercana para quienes la necesitan.

El Dr. Rojas destaca que “La cooperación con EE.UU es funcional, pero que muchas veces no se logra materializar por la rigidez de las normas externas.” El doctor Arango añadió

que, aunque Colombia hace parte de la Convención de Budapest, “No hay protocolo interno que guíe su implementación” Finalmente, el Dr. Londoño consideró que “Colombia ha perdido credibilidad en temas de ciberseguridad”, lo cual limita la posibilidad de colaboración con otros países en solicitud de información.

3.6 Limitaciones al acceso a la tutela judicial efectiva en los delitos informáticos en Colombia

El reconocimiento formal del derecho a la tutela judicial efectiva está garantizado tanto por la Constitución colombiana como por diversos instrumentos internacionales. En los delitos informáticos, esta garantía cobra una importancia particular debido a la forma de llevar ese derecho a la práctica porque enfrenta una serie de dificultades que se hacen visibles desde el primer momento en que una persona intenta acudir al sistema de justicia. Muchas personas no saben si lo que les ocurrió puede considerarse un delito ni cómo deben proceder para denunciarlo.

Al intentar denunciar, las personas también tienen problemas relacionados con el lenguaje técnico, a formularios mal adaptados o la falta de acompañamiento. Esto no depende únicamente del nivel educativo o de los recursos tecnológicos de la víctima. Al contrario, refleja una debilidad estructural en la forma en que se han construido los canales institucionales. Es claro y evidente que cuando no hay claridad sobre los procedimientos, los tiempos o las posibilidades reales de obtener una resolución, se genera frustración y se pierde impulso para continuar el proceso. Por lo tanto, cada fase del proceso debe facilitar el ejercicio de los derechos, desde el momento en que se interpone una denuncia hasta la resolución final del caso. Siendo esenciales para que el sistema de justicia pueda cumplir su función con legitimidad, la claridad procedimental, la atención respetuosa y la coherencia institucional.

La justicia digital forma parte de la experiencia social actual y debe consolidarse como una dimensión activa del sistema judicial colombiano y si se integra este enfoque en las prácticas institucionales se puede mejorar en gran medida la respuesta ante las nuevas formas de delito, y además también reafirma el valor del derecho como herramienta viva para la protección de las personas en todas las esferas en las que se desenvuelven.

3.7 Obstáculos legales y procesales

Frente a los delitos informáticos, Colombia ha venido fortaleciéndose en los últimos años especialmente desde la expedición de la Ley 1273 de 2009. Esta norma introdujo figuras penales dirigidas a sancionar conductas como el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones y la violación de datos personales.

Una limitación tiene que ver con la ausencia de tipos penales que aborden nuevas formas de criminalidad digital, como la manipulación de identidad mediante técnicas avanzadas como deep fakes, el uso indebido de datos biométricos o el control remoto de dispositivos sin autorización. Estas son conductas que no encajan en las definiciones penales existentes y dificultan totalmente su judicialización, pero también puede afectar la protección de principios como el debido proceso, al generar margen para interpretaciones contradictorias o para la desestimación temprana de casos.

También se identifican vacíos en la construcción de criterios jurisprudenciales que orienten la interpretación de los delitos informáticos porque las altas cortes aún no han desarrollado una doctrina lo suficientemente sólida y consolidada sobre la materia y esto causa que distintos operadores judiciales apliquen los mismos tipos penales con enfoques disímiles teniendo respuestas desiguales y poco predecibles ante casos con características similares.

Los delitos informáticos pueden involucrar elementos que tocan esferas civiles, penales, administrativas e incluso internacionales, lo que exige un trabajo articulado que no siempre está respaldado por una normativa clara. En algunos casos, las autoridades investigadoras enfrentan obstáculos para determinar qué entidad debe actuar, cómo canalizar las solicitudes de cooperación y qué normas aplicar de manera integrada.

En el plano penal, se activa la función punitiva del Estado para investigar, judicializar y sancionar conductas como el acceso no autorizado, el sabotaje informático o la interceptación ilegal de datos. Pero en muchos casos, la sola persecución penal no resuelve de forma suficiente el conjunto de consecuencias derivadas del delito.

Desde la perspectiva del derecho civil, estos hechos pueden generar daños patrimoniales o extrapatrimoniales que requieren ser indemnizados. Las víctimas pueden reclamar, por ejemplo, por perjuicios derivados del uso indebido de su imagen, del fraude financiero en línea, o del deterioro de su reputación por publicaciones falsas o manipuladas. Lo cual, permite activar mecanismos de reparación que, si bien no sustituyen la acción penal, la complementan y dan una respuesta más amplia a la afectación sufrida. Por todo lo anterior, se hace evidente que hay una necesidad de consolidar un enfoque normativo que pueda contribuir a articular de forma efectiva las distintas dimensiones de los delitos informáticos bajo criterios claros de competencia y cooperación para fortalecer la capacidad del Estado y así también, ampliar las posibilidades de garantizar una protección real y completa de los derechos afectados.

3.8 Barreras técnicas y probatorias

Además de los retos normativos y procesales, garantizar la tutela judicial efectiva frente a los delitos informáticos en Colombia sigue siendo un gran desafío más que todo por las barreras técnicas y probatorias que enfrentan las personas que buscan justicia. Son

obstáculos que, aunque muchas veces resultan invisibles para el ciudadano del común, terminan afectando profundamente la posibilidad de que las investigaciones avancen, se recojan pruebas válidas y se tomen decisiones judiciales justas y que estén bien fundamentadas.

Un problema mayor es la propia naturaleza de la evidencia digital porque muchas veces no se puede ver ni tocar, puede desaparecer en segundos, modificarse sin dejar rastro o estar almacenada en servidores de distintos países al mismo tiempo. A diferencia de una prueba física, como un arma o un documento impreso, un archivo digital puede ser borrado con un clic. Si no se interviene a tiempo, es posible que cuando la víctima logre formalizar la denuncia, la evidencia ya se haya esfumado.

La cooperación internacional, regulada por instrumentos como la Convención de Budapest y por reglas de asistencia judicial mutua, resulta esencial para acceder a registros que permanecen en servidores fuera del país; las demoras en estos mecanismos afectan la conservación de evidencias. (Council of Europe, 2001; Díaz-Pérez, 2022).

En este panorama, uno de los puntos más delicados es la falta de un protocolo unificado y de obligatorio cumplimiento que regule cómo debe manejarse la evidencia digital a lo largo del proceso penal. Aunque existen guías como la Cartilla Metodológica de Atención de Delitos Informáticos elaborada por la Fiscalía General de la Nación, su uso no es uniforme ni garantizado. Todo depende de cada funcionario, lo que termina generando enormes diferencias entre regiones y entre casos.

Esta ausencia de estandarización puede traducirse en consecuencias graves para las víctimas y para la justicia misma. Desde la invalidez de una prueba clave hasta la vulneración

de derechos procesales fundamentales, los riesgos son altos cuando no hay claridad ni coherencia en el manejo de este tipo de evidencia. En últimas, la falta de reglas claras debilita la confianza en el sistema y puede impedir que muchos casos lleguen a una resolución justa.

Además, preservar datos sensibles a tiempo es un reto que se vuelve aún más complejo cuando no existe claridad sobre cómo hacerlo sin poner en riesgo su validez. No basta con guardar un archivo o hacer una captura de pantalla. El cómo se recolecta, con qué herramientas, en qué formato se conserva y cómo se garantiza que no ha sido alterado, son pasos clave que deben cumplirse con extremo cuidado.

Cada detalle importa, porque en un proceso judicial, cualquier irregularidad puede ser usada para cuestionar la autenticidad de la prueba, excluirla o incluso invalidar todo un caso. Cuando no se siguen los protocolos adecuados o simplemente no existen, la evidencia puede terminar siendo inútil, y con ella se debilita toda la investigación. Así, lo que pudo ser una prueba contundente se convierte en una oportunidad perdida para alcanzar justicia.

A todo esto, se suma la necesidad de interactuar con plataformas tecnológicas que operan fuera del país. En la mayoría de los casos, la información clave para una investigación como registros de inicio de sesión, direcciones IP, mensajes privados o historiales de navegación está alojada en servidores de grandes compañías tecnológicas con sede en el extranjero.

El problema es que estas empresas no siempre colaboran de manera oportuna. Ya sea por trabas legales, políticas internas o simples demoras administrativas, las solicitudes de cooperación pueden tardar semanas o meses, cuando no son ignoradas por completo. Ese tiempo perdido es crucial. Mientras la información no llega, los indicios se enfrían, los rastros digitales se borran y las posibilidades de identificar y sancionar a los responsables se reducen considerablemente.

Estas dificultades técnicas y probatorias no son simples fallas operativas, sino que dejan al descubierto una tensión de fondo entre un proceso penal pensado para evidencias físicas y las nuevas demandas del mundo digital. Mantener ese desfase como si fuera un problema menor ya no es viable. La justicia penal debe asumir que la prueba digital no es una rareza, sino parte cotidiana de su labor. Hacer esa transición no se trata solo de agilizar trámites y es indispensable para proteger la confianza de una sociedad cada vez más conectada y la legitimidad misma del sistema judicial.

Los entrevistados resaltan la ausencia de protocolos especializados para la recolección custodia y presentación de la evidencia digital generando inseguridad jurídica y sin fin de nulidades en los procesos. El Dr Rojas indicó que la "La justicia no cuenta con peritos suficientes ni laboratorios adecuados para certificar la autenticidad de la información." Mientras que el Dr. Arango enfatizó que "La capacitación de la prueba digital es mínima, y eso convierte a cualquier audiencia en un escenario de improvisación." esta limitación es una explicación del por que los casos no prosperan más allá de las etapas procesales.

3.9 Falta de confianza y cultura de denuncia

Una de las mayores razones que limitan para que las víctimas de delitos informáticos ejerzan plenamente su derecho a la justicia es que hay una baja cultura de denuncia que persiste y está enraizada en la desconfianza estructural hacia el sistema judicial y las instituciones encargadas de investigar sobre estos hechos. Así las conductas delictivas en el entorno digital han aumentado de forma considerable en los últimos años, es muy preocupante que la gran mayoría de los casos nunca llega a conocimiento de las autoridades. Es decir que hay una brecha enorme entre lo que ocurre en la realidad digital y lo que efectivamente se tramita en las rutas judiciales.

Las razones para no denunciar este tipo de delitos son variadas. Algunas personas no saben a dónde acudir ni por dónde empezar. En el caso de otras, con cierta desilusión, se resignan pensando que “no vale la pena”, que el proceso será demasiado largo, complicado o inútil. También están quienes prefieren guardar silencio por miedo a exponerse aún más al agresor o por temor a revivir una experiencia dolorosa al enfrentarse al sistema judicial. Siendo un conjunto de barreras emocionales, sociales e institucionales las que terminan generando un silencio generalizado frente a la criminalidad digital, especialmente en casos como el robo de identidad, la extorsión virtual, la difusión no consentida de contenidos íntimos o el acoso en redes.

Muchas personas que han sido víctimas de delitos informáticos están llenas de desconocimiento, ni siquiera identifican lo que les ocurrió como algo que pueda denunciarse o sancionarse penalmente. Todavía persiste la idea equivocada de que estos hechos “no son tan graves”, que simplemente hacen parte de los riesgos de estar conectados o que por el hecho de tratarse de algo virtual no tienen consecuencias reales.

Esta forma de ver el problema nace y se refuerza por la falta de información clara, accesible y oportuna. Cuando el desconocimiento se combina con la desconfianza, no solo se refuerza la impunidad: también se debilita poco a poco la legitimidad del sistema de justicia, justo en un momento en que la sociedad necesita respuestas reales frente a los desafíos del mundo digital.

La sensación de lejanía o inaccesibilidad que muchas personas sienten frente al sistema judicial es un tema importante. Para buena parte de la población, especialmente para personas que viven en zonas rurales donde el acceso a la tecnología es limitado o prácticamente no existe, el tema de acudir a una entidad del Estado representa un trámite con limitantes geográficos, económicos, técnicos e incluso simbólicos.

En muchos casos el simple hecho de llegar hasta una oficina de atención es complicado porque implica desplazamientos largos y costosos. A esto se suma que no todas las personas cuentan con acceso a internet, dispositivos adecuados o habilidades digitales para utilizar plataformas en línea, lo cual los deja por fuera de los canales de denuncia más modernos porque el sistema no fue pensado para ellos, que su forma de hablar, su realidad cotidiana o sus urgencias no tienen cabida en un entorno lejano y poco empático causando que esa desconexión refuerce el silencio porque cuando el camino hacia la justicia se percibe como distante e incomprensible, muchas personas prefieren no recorrerlo.

La situación es más difícil cuando las víctimas pertenecen a grupos históricamente marginados como Mujeres, personas LGBTIQ+ y jóvenes que están especialmente expuestos a violencia digital como la difusión no consentida de imágenes íntimas, el acoso sistemático, la amenaza constante, la manipulación emocional y la suplantación de identidad con fines de extorsión.

Muchas de estas personas prefieren no denunciar porque temen no ser tomadas en serio, ser culpabilizarse por lo que pasó o enfrentar actitudes Revictimización por parte de quienes deberían brindarles apoyo y el silencio es una forma de autoprotección frente a un sistema que, en lugar de generar confianza, muchas veces perpetúa estigmas, prejuicios y respuestas insensibles.

La falta de confianza ciudadana y la falta de cultura denuncias, los entrevistados coinciden que el gran alto índice de impunidad desmotiva a las víctimas de estas conductas a presentar denuncias a las autoridades competentes El doctor Rojas señaló que “La gente siente que no pasa nada, que no vale la pena denunciar” a su vez el Dr Londoño agrega “que el sistema está destinado a fracasar desde el inicio si no se activan los mecanismos eficaces desde la etapa de denuncia.” Esta percepción que tiene la sociedad de la alta impunidad y la

ineficiencia institucional contribuye a la cultura de silencio que hay frente a esta clase de conductas. El Dr. de la Pava reafirma estas ideas manifestando lo siguiente: “Mientras se prioricen delitos comunes y no se fortalezcan los canales digitales de denuncia el ciudadano seguirá sin confiar en la justicia penal frente a lo informático.”

CAPITULO lV.

CONCLUSIONES

4.1 Conclusiones aplicables al capítulo 1

El desarrollo de este capítulo nos permite comprender que el proceso penal colombiano, a pesar de contar con un diseño normativo estructurado en principios de oralidad, inmediación y contradicción, se muestra insuficiente frente a la complejidad que plantean los delitos informáticos. El recorrido por cada fase procesal, desde la indagación hasta la sentencia, mostró que la mayoría de las denuncias se concentran y permanecen en la etapa preliminar y vemos una que situación configura un patrón de estancamiento que refleja una justicia que inicia la ruta procesal, pero que rara vez alcanza un desenlace definitivo con decisiones de fondo.

Las estadísticas y los análisis normativos evidenciaron que esta inercia procesal no obedece a una serie de limitaciones estructurales como la dificultad de recolectar, preservar y presentar pruebas digitales con la solidez que exige un juicio; la carencia de personal capacitado en investigación forense informática; la escasez de recursos tecnológicos dentro de la Fiscalía y los cuerpos de policía judicial; y la congestión judicial que obliga a dar prioridad a delitos considerados de mayor impacto social.

El análisis también permitió observar las consecuencias humanas que se desprenden de esta ineficacia procesal. Cada caso que no avanza hacia una imputación o un juicio oral representa a una víctima que no encuentra respaldo institucional. Son ciudadanos que, además de perder dinero, ver expuesta su intimidad o dañada su reputación, cargan con una herida que deja la ausencia de justicia. Detrás de cada denuncia archivada hay personas que sienten cómo su confianza se desmorona, que experimentan la angustia de haber sido vulneradas y la impotencia de no encontrar respaldo institucional que los obliga a convivir con la incertidumbre de un proceso que nunca llega a su fin.

Cada denuncia que se queda en el camino representa a una persona que buscó protección y terminó enfrentándose a un muro procesal que la dejó sin respuestas. La ausencia de una sentencia no significa sólo que el caso no se resolvió: significa que la víctima sigue conviviendo con la herida abierta del delito y con la sensación de que el Estado le dio la espalda.

El capítulo también muestra que la dificultad está en lo que dice la ley y también en cómo funciona el aparato judicial al enfrentarse a un fenómeno tan dinámico como el cibercrimen. Esta constatación nos invita a ver que el problema es estructural, que requiere cambios profundos que no puede seguir aplazándose y reconocerlo es un primer paso necesario para imaginar un sistema que no deje a las víctimas atrapadas en indagaciones sin fin, sino que les ofrezca decisiones concretas que reparen, sancionen y devuelvan la confianza en la justicia.

Al visibilizar los quiebres del proceso penal, este capítulo permite reconocer que el cibercrimen constituye una amenaza directa para la vigencia de los derechos fundamentales y para la confianza en las instituciones. Este fenómeno exige ser abordado con plena seriedad, pues cada caso inconcluso refleja una vulneración que permanece abierta en la vida de una

víctima. El panorama descrito reclama una justicia capaz de responder en la era digital con mecanismos eficaces, especializados y sensibles, que transformen las denuncias en decisiones judiciales concretas y brinden a las personas afectadas resultados claros, reparadores y dignos de confianza.

4.2 Conclusiones aplicables al capítulo 2

La gestión de la evidencia digital en los procesos penales de cibercrimen se desarrolla a través de una secuencia de actuaciones que exige cuidado y precisión. Desde que surge la noticia criminal hasta que el material probatorio es valorado en juicio, se despliega un entramado institucional donde confluyen policías judiciales encargados de asegurar los primeros rastros, fiscales que definen la estrategia investigativa, peritos que transforman los datos en hallazgos técnicos comprensibles, jueces que analizan su pertinencia y validez, y en ciertos casos, autoridades extranjeras que aportan información clave de carácter transnacional. Cada uno de estos momentos contribuye a la solidez de la investigación y determina si la prueba conservará la fuerza necesaria para sustentar una decisión judicial.

El análisis mostró que la fragilidad de la evidencia digital convierte su manejo en una tarea que exige precisión y rapidez. Un archivo borrado, una cadena de custodia incompleta o un análisis realizado sin las herramientas adecuadas puede comprometer un caso entero. Estos riesgos se agravan por la insuficiencia de equipos actualizados, la falta de laboratorios forenses en varias regiones y la carencia de programas permanentes de formación para operadores judiciales que enfrentan un fenómeno cambiante y altamente técnico.

El capítulo también permitió ver las desigualdades que marcan el acceso a la justicia digital en el territorio. En las principales ciudades existen laboratorios y equipos especializados, mientras en municipios apartados las investigaciones dependen de recursos

mínimos que reducen la validez de los resultados y la disparidad territorial genera un acceso desigual a la justicia y coloca a muchas víctimas en una situación de vulnerabilidad procesal.

La evidencia digital, además, impone un reto particular al sistema penal por su carácter volátil. El paso del tiempo afecta la conservación de la información y cada demora en la investigación puede significar la desaparición de un rastro o la alteración de un archivo esencial. Esta condición obliga a pensar en procedimientos judiciales más ágiles y compatibles con la naturaleza de la prueba tecnológica.

En conclusión, el capítulo 2 demuestra que la fortaleza de una investigación penal en delitos informáticos depende de la forma en que se protege, preserva y presenta la prueba digital. El marco legal ofrece lineamientos claros, pero la efectividad se ve comprometida por falencias técnicas, logísticas y de coordinación. Para avanzar hacia una justicia digital más efectiva, es necesario invertir en infraestructura tecnológica, formar operadores especializados y consolidar mecanismos de cooperación que permitan actuar con mayor agilidad.

Cada dato preservado con rigor representa una posibilidad de justicia para la víctima. Cada evidencia tratada de manera adecuada fortalece la confianza en las instituciones y abre el camino hacia decisiones judiciales que reparen el daño sufrido. La prueba digital es, en este contexto, es lo que constituye la vía para que la experiencia de la víctima se convierta en verdad judicial y para que el Estado reafirme su compromiso con la protección de los derechos en la era digital.

4.3 Conclusiones aplicables al capítulo 3

El capítulo 3 permitió evidenciar que las dificultades saturados de procesos, funcionarios que trabajan con recursos limitados, equipos que resultan insuficientes y la ausencia de una coordinación fluida entre las instituciones

La dispersión de competencias entre entidades se identificó como un factor que debilita la eficacia de las investigaciones. Las piezas del proceso no siempre logran articularse y los trámites se dilatan en solicitudes repetidas o en oficios sin respuesta y el camino procesal se convierte en una secuencia de gestiones que rara vez se conectan de manera efectiva, lo que impide consolidar expedientes con la solidez suficiente para ser debatidos en juicio.

Otro hallazgo importante fue la distancia entre las exigencias técnicas de los delitos informáticos y el nivel de preparación de muchos operadores judiciales. La carencia de formación constante en temas especializados limita la capacidad de actuar con seguridad y eficacia frente a estas conductas y también genera dependencia de pocos expertos, que prolonga la duración de las investigaciones y debilita su solidez.

El capítulo también permitió advertir que la saturación de los despachos produce una dinámica en la que los funcionarios se ven obligados a distribuir su tiempo entre múltiples procesos generando que las investigaciones de cibercrimen avancen de manera más lenta y con menor atención, siendo la consecuencia un debilitamiento de la legitimidad institucional y una percepción ciudadana de ineficacia que refuerza el desaliento frente al sistema judicial.

En conjunto este capítulo muestra que las dificultades para judicializar los delitos informáticos nacen de factores estructurales que pesan sobre la organización y el trabajo diario del sistema penal. Se evidencia ausencia de coordinación entre entidades, la escasez de recursos humanos y tecnológicos y la sobrecarga que enfrentan jueces y fiscales se convierten en un entramado que frena los procesos y termina cerrando el camino hacia la justicia digital. Estas limitaciones no se quedan en diagnósticos institucionales: se reflejan en personas concretas, en víctimas que ven cómo su denuncia se diluye y en funcionarios que intentan responder con herramientas que no siempre alcanzan.

La justicia digital depende de un aparato judicial con condiciones adecuadas para actuar. La existencia de normas y de marcos legales pierde eficacia cuando las instituciones no cuentan con la preparación ni con los recursos para aplicarlos y tener un modelo capaz de responder al cibercrimen exige instituciones articuladas, personal con formación especializada y un compromiso real de garantizar a las víctimas procesos que concluyan con decisiones reparadoras.

4.4 Conclusiones generales aplicables a todos los capítulos

La presente investigación deja en constancia que la judicialización de los delitos informáticos en Colombia exige más que una mera transcripción normativa que hoy la encontramos en la ley 1273 del 2009, demanda la articulación efectiva entre las garantías procesales, técnicas forenses y organización institucional.

Se evidencia una concentración persistente de las denuncias en la etapa de indagación, fenómeno que compromete la progresividad del derecho penal y la efectiva materialización del ius puniendi del estado, esta realidad más que revelar debilidades investigativas, si no también pone en riesgos principios rectores como la debida valoración probatoria y el derecho de las víctimas de obtener una respuesta judicial de fondo.

La naturaleza frágil y efímera de la evidencia digital exige el cumplimiento obligatorio de reglas procesales como lo son la legalidad de la actuación, la cadena de custodia, conservación y autenticidad de la misma y la implementación de técnicas permanentes como laboratorios forenses especializados, protocolos homologados y peritos calificados, desde un punto de vista dogmático y probatorio la investigación demuestra que la existencia de las normas aplicables como la Ley 906 de 2004, Ley 1273 de 2009 y convenios internacionales no bastan si no hay prácticas uniformes que garanticen la admisibilidad y el valor probatorio

de la evidencia que es la columna vertebral para que la denuncia pueda superar esa etapa de indagación.

Las entrevistas y análisis cualitativo de los datos abiertos de la fiscalía muestran que los fiscales, jueces y defensores enfrentan tensiones convergentes, insuficiente especialización, cargas procesales elevadas, una alta desarticulación institucional. Lo que esto genera desconfianza en las víctimas generando una cultura de no denuncia que agrava la impunidad es un problema sistémico que queda demostrado en la práctica de la judicialización de esos delitos.

En términos jurídicos, la eficacia del derecho penal frente a este nuevo reto que es la criminalidad informática exige un doble requisito i. la adecuación procedimental y probatoria, es decir reglas claras para la recolección y preservación de la evidencia digital y ll. una consolidación institucional que tenga capacidades técnicas que permita traducir la norma en decisiones judiciales efectivas.

REFERENCIAS

(n.d.). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Retrieved September 17, 2025, from https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Cayeron los troyanos. (2021, Noviembre 04). infobae. https://www.infobae.com/america/colombia/2021/11/04/cayeron-los-troyanos-senalados-de-robos-ciberneticos-por-mas-de-12-mil-millones-de-pesos/

CETS 185 - Convention on Cybercrime. (n.d.). https: //rm. coe. int. Retrieved September 17, 2024, from https://rm.coe.int/1680081561

Corte Constitucional de Colombia. (n.d.). *Sentencia C-595/05*.

Corte Constitucional de Colombia. (2005, junio 09). *Sentencia C-591/05*. SISTEMA PENAL ACUSATORIO COLOMBIANO. Retrieved octubre 05, 2024, from https://www.corteconstitucional.gov.co/relatoria/2005/c-591-05.htm

Fiscalía General de la Nación. (n.d.). Fiscalía General de la Nación. https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/

Ingeniería, investigación y desarrollo. (2021, Agosto 31). revistas uptc. https://revistas.uptc.edu.co/index.php/ingenieria_sogamoso/issue/view/732

Jesús Audelo González, Héctor Pérez Meana y Pedro Guevara López. (n.d.). *Gusanos informáticos*. Gusanos informáticos. Retrieved 10 12, 2024, from https://amc.edu.mx/revistaciencia/images/revista/66_3/PDF/Gusanos.pdf

Luis Enrique Arellano Carlos Mario Castañeda. (2012, Julio 08). *La Cadena de Custodia Informático-forense*. Tecnológico de Antioquia. https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/45

Sanabria, R. (2025, Marzo 07). *Prueba digital en el proceso penal: exclusión, cadena de custodia y la validez de la versión impresa sin código hash*. Ronald Sanabria. 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/

Valero, Jeffry Jacsir Ortiz Duarte, Wilson Orlando Lasso Mora, Nelson Andrés. (2019). *La cooperación internacional como estrategia para combatir los delitos informáticos*. Repositorio Digital Universidad Simón Bolívar. https://bonga.unisimon.edu.co/items/0692c758-f0e0-4b3d-8362-5c06bca6a88a

Variables asociadas a los delitos informáticos en Latinoamérica. (2024, Enero - Junio). Academia & Derecho. https://revistas.unilibre.edu.co/index.php/academia/article/view/11822/11598

ANEXOS

1. A continuación, se presentan las transcripciones completas de las entrevistas realizadas, junto con los respectivos consentimientos informados firmados por cada uno de los participantes en la investigación:

1.1 Juez Primero Penal del Circuito de Bello – John Alexander Rojas Duque.

1.2 Abogado Litigante – Jonathan Londoño Muñoz.

1.3 Ex Magistrado – Ricardo de la Pava Marulanda.

1.4 Juez Segundo Penal del Circuito de Envigado – Andrés Felipe Arango Giraldo.

1.5 Docente del ITM – Héctor Fernando Vargas.

1.6 Perito en Informática Forense – Samir Adolfo Batidas Núñez.

1.7 Investigador Digital / Perito Forense – Johnatan Mazo Ramírez.

2. Derecho de petición.

2.1 Ministerio de defensa.

2.2 Respaldo del derecho de petición por parte del director del centro de investigación Dr. David Villa y decano de la facultad de derecho Dr, Ramón Elejalde.

3. Respuestas a derechos de petición trasladados a las siguientes entidades por razón de competencia"

3.1 Fiscalía General de la Nación.

3.2 Dirección de investigación criminal e interpol -DIJIN-