



Brújula. Semilleros de Investigación

Volumen 13, Número 25, enero-junio, pp. 34-42

Bogotá D. C., Colombia

ISSN 2346-0628 (en línea)

<https://doi.org/10.21830/23460628.172>

DOSIER

Control+Alt+Delito: reflexiones jurídicas sobre la cibercriminalidad en Colombia

Angela Rosa Mejía Corrales 

Fundación Universitaria del Área Andina, Valledupar, Cesar

RESUMEN

Este artículo analiza, desde una mirada crítica y jurídica, los desafíos que enfrenta el país frente al auge de delitos informáticos. Si bien Colombia ha dado pasos importantes en la construcción de un marco normativo —como la *Cartilla metodológica de atención a delitos informáticos*, de la Fiscalía General de la Nación, la cual pretende ser una guía para abordar este tipo de crímenes estableciendo protocolos de acción para las autoridades y rutas de atención a usuarios y víctimas—, es necesario cuestionar su aplicabilidad práctica y si requiere una actualización profunda para ser verdaderamente efectiva.

PALABRAS CLAVE

datos personales; delitos informáticos; denuncia; derecho a la información; derecho a la privacidad; derecho del ciberespacio

CITACIÓN APA

Mejía Corrales, A. R. (2025). Control+Alt+Delito: reflexiones jurídicas sobre la cibercriminalidad en Colombia. *Revista Brújula de Investigación*, 13(25), 34-42.

<https://doi.org/10.21830/23460628.172>

Recibido: 15 de abril 2025 **Aceptado:** 20 de junio de 2025

Contacto: Angela Rosa Mejía Corrales ✉ amejia90@estudiantes.areandina.edu.co



Introducción

Vivimos en una era donde el acceso a la información, la hiperconectividad y la digitalización de servicios han transformado la forma en que nos comunicamos, trabajamos y vivimos. Sin embargo, este avance también ha traído consigo nuevas formas de criminalidad que desafían los límites del derecho tradicional. En este contexto, surge un fenómeno creciente y complejo: la cibercriminalidad, la cual plantea retos técnicos, normativos y éticos para los operadores jurídicos, las instituciones del Estado y la ciudadanía en general.

El objetivo de este artículo es analizar críticamente el marco jurídico colombiano frente a los delitos informáticos, especialmente a la luz de la *Cartilla metodológica de atención para los delitos informáticos*, de la Fiscalía General de la Nación (FGN), diseñada para guiar a operadores judiciales y técnicos en el abordaje de esta problemática. Se abordarán las categorías delictivas más frecuentes, los retos probatorios asociados a la evidencia digital y la cooperación internacional como mecanismo indispensable en la lucha contra el cibercrimen.

Desde una perspectiva teórico-jurídica y práctica, se expondrán los principales avances normativos, así como las limitaciones operativas y conceptuales que enfrenta el Estado frente a un fenómeno transnacional, dinámico y técnicamente sofisticado. La cibercriminalidad no solo desafía al derecho penal clásico en sus categorías tradicionales de tipicidad, antijuridicidad y culpabilidad, sino que exige una constante actualización de capacidades institucionales, normativas y periciales.

Este análisis se propone contribuir al debate académico sobre los alcances reales de la legislación vigente y su aplicabilidad, proponiendo además una mirada crítica sobre la eficiencia de las herramientas disponibles para el control social y penal en entornos digitales. Busca responder a la pregunta problema: ¿es efectiva la respuesta jurídica del Estado colombiano frente a la cibercriminalidad, particularmente a través de la Ley 1273 de 2009 y la *Cartilla metodológica de atención a delitos informáticos*, de la Fiscalía General de la Nación? La importancia de este trabajo radica en que permite comprender cómo se está protegiendo —o dejando de proteger— uno de los activos más valiosos de nuestra sociedad: la información.

Marco teórico

En el VI Congreso Internacional de Derecho Penal, organizado por la Universidad de los Andes en 2012, Fernando Miró, docente español, detalló el concepto de *cibercriminalidad*. Este término puede parecer un concepto legal, pero en realidad es criminológico, ya que hace referencia al contexto en el que se produce la infracción. Señaló que los seres humanos convivimos en dos espacios simultáneamente: un espacio físico o



material, donde se cometen delitos físicos —los cuales encontramos ya desarrollados en la Ley 599 de 2000, por la cual se dicta el Código Penal colombiano— y otro, denominado *ciberespacio*, donde se perpetran ciberdelitos o delitos informáticos mediante el uso de las tecnologías de la información y la comunicación (TIC).

Los cibercrímenes han sido objeto de estudio por juristas y ordenamientos jurídicos nacionales e internacionales. Para definir el término *cibercriminalidad*, el Convenio de Budapest sobre Ciberdelincuencia de 2001 establece que son aquellas infracciones “contra la confidencialidad, la integridad y la disponibilidad de la información, de los datos y de los sistemas informáticos”. En Colombia, por su parte, se expidió la Ley 1273 de 2009, donde se crea el bien jurídicamente tutelado de la información, los datos y los sistemas de información, y, tipificando conductas asociadas a la afectación de este bien, se crearon los siguientes tipos penales: Capítulo I, “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”. En este capítulo podemos encontrar conductas penales como: acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de *software* malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales. Capítulo II, “De los atentados informáticos y otras infracciones”; este capítulo tipifica el hurto por medios informáticos y semejantes, así como la transferencia no consentida de activos.

Los antes anotados tipos penales se encuentran determinados a partir del artículo 269A de la Ley 1273 de 2009, que añadió estas conductas al Código Penal colombiano (Ley 599 de 2000), donde se establece el tipo *acceso abusivo a un sistema informático*. En este tipo penal se sanciona a quien, sin autorización, accede a un sistema informático protegido o no. Es la base para tipificar la intrusión no consentida a redes o servidores, muy común en *hackeos*. Se sanciona con pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La Sentencia SP592-2022 del 2 de marzo de 2022, proferida por la Corte Suprema de Justicia, se refirió por primera vez sobre los elementos del ciberdelito en los siguientes términos:

- i) Sujeto activo no calificado, por no necesitar de una condición especial para quien realiza los verbos rectores; ii) Sujeto pasivo, persona natural o jurídica titular del sistema informático; iii) Lesionar varios bienes jurídicos tutelados, entre ellos, la información, los datos y la intimidad. En ese sentido, ha sido reconocido como un tipo penal pluriofensivo; iv) Solo admite el dolo en el actuar del ciberdelincuente; v) Es un delito de mera conducta, por cuanto, la sola intromisión en una red informática, en las condiciones establecidas en el tipo penal, afecta el bien jurídico tutelado; vi) Contempla dos verbos rectores, acceder o mantener; vii) Como ingrediente normativo, exige que



el sujeto activo de la acción acceda en el sistema informático sin autorización, o, aun cuando, teniendo el permiso del titular legítimo del derecho, se mantiene dentro del mismo, excediendo las facultades otorgadas.

Otro de los artículos de la misma ley es el 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación*, el cual penaliza la interferencia con el funcionamiento de un sistema informático o red de telecomunicación o la eliminación, alteración o supresión de datos, lo cual puede paralizar servicios esenciales. También está consagrado el artículo 269C: *Interceptación de datos informáticos*. Este delito castiga a quien intercepte sin autorización datos transmitidos entre sistemas, incluso si no los modifica. Se puede visibilizar en casos de espionaje digital. Artículo 269D: *Daño informático*. Tipifica la conducta de quien, sin autorización, dañe, deteriore, altere o suprima información contenida en un sistema informático. Este 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.

Además, del artículo 269E: *Uso de software malicioso*. Establece la pena para quien incurra en la creación, distribución o uso de programas diseñados para causar daño informático, como virus, troyanos o *ransomware* (*malware* que secuestra o retiene datos dentro de un sistema operativo a cambio de un rescate para remover esta restricción). O el artículo 269F: *Violación de datos personales*, donde se sanciona el acceso, uso o divulgación no autorizada de datos personales almacenados en sistemas informáticos, conectando con el derecho fundamental al *habeas data*, establecido en el artículo 15 de nuestra Constitución Política. Así como unos muy comunes actualmente, como el artículo 269G: *Suplantación de sitios web para capturar datos personales*. Con este se penaliza la creación o manipulación de páginas web falsas con el fin de capturar datos de los usuarios para usos ilícitos.

Y, por supuesto, los artículos 269I y 269J, donde se determinan respectivamente el *hurto por medios informáticos y semejantes* y la *transferencia no consentida de activos*. El primero establece como delito el apoderamiento de bienes (como dinero), es decir, adueñarse de estos bienes ajenos mediante manipulación informática, simulaciones digitales o fraudes electrónicos. Mientras que el segundo aborda el uso no autorizado de sistemas para mover activos (como fondos electrónicos), sin necesidad de vulnerar la seguridad del sistema, pero sí de aprovecharlo para un beneficio económico.

Todos estos delitos informáticos también se encuentran incluidos en la cartilla metodológica expedida por la Fiscalía General de la Nación, además de una descripción detallada de las rutas de atención, roles de los actores institucionales y canales disponibles para la recepción de denuncias, tanto en entornos presenciales como



virtuales. Su enfoque parte de una clara diferenciación entre usuario y víctima, y delimita funciones específicas para fiscales, policías judiciales y peritos forenses.

Métodos

Como aspecto metodológico de la investigación sobre la efectividad de la respuesta jurídica colombiana frente a la cibercriminalidad, es pertinente mencionar que se ha requerido de una revisión bibliográfica con un método de investigación hermenéutico, puesto que es necesaria la recopilación, análisis y síntesis de información proveniente de diversas fuentes documentales, orientado a la comprensión crítica de esos textos normativos, doctrinales y técnicos relevantes en el ámbito jurídico y forense digital.

Esta perspectiva hermenéutica ha facilitado el estudio del contenido legal de la Ley 1273 de 2009, su utilidad en la esfera penal, además de los componentes operativos y procedimientos presentes en la *Cartilla metodológica de atención para los delitos informáticos* emitida por la Fiscalía General de la Nación. Esta revisión no solo analiza las reglas y directrices, sino también su contexto, amplitud, restricciones y vínculo con los fenómenos actuales de delincuencia digital.

Este método nos ayudará tanto a explicar el fenómeno de la cibercriminalidad como a evaluar la capacidad del Estado para enfrentarlo, llevándonos hacia una explicación más detallada del porqué mediante diferentes técnicas que se caracterizan por su contextualización, como un análisis normativo y jurisprudencial de la Ley 1273 de 2009, una revisión crítica de la cartilla metodológica y algunas entrevistas semiestructuradas a fiscales de la ciudad de Valledupar, miembros de la división de delitos informáticos y policías judiciales, para que nos informen sobre la utilidad de esta cartilla, indicando si es eficiente o si ha tenido dificultades para su aplicación.

Resultados

En la anterior indagación, se analizó la Ley 1273 de 2009 y la *Cartilla metodológica de atención de delitos informáticos*, expedida por la Fiscalía General de la Nación, en la que se destacan tanto sus fortalezas como sus debilidades. Se pudieron identificar algunos desafíos legales en la persecución de delitos informáticos:

Vacíos normativos: impunidad y falta de sanción

Si bien la cartilla se sustenta en un marco legal robusto (incluyendo la Constitución, el Código Penal y el Convenio de Budapest), su aplicabilidad en la realidad colombiana es un punto de debate. A pesar de la existencia de leyes como la Ley 1273 de 2009,



que tipifica los delitos informáticos, el crecimiento exponencial de nuevas formas de criminalidad digital como el *ransomware* o el *cyberbullying*, los cuales no están bien determinados en la norma, genera que los delincuentes puedan eludir el castigo. Si las leyes no han sido actualizadas o no se han desarrollado normas específicas para ciertos tipos de delitos, quienes cometen estos actos pueden quedar impunes, ya que no hay un marco legal claro que los defina como ilegales. Estos vacíos normativos en los delitos informáticos también generan dificultades para los jueces y las autoridades, pues limita su deber legal de administrar justicia al no lograr una interpretación clara de la norma que defina si las conductas que encuentran en los diferentes casos se ajustan o no a un tipo penal.

Colaboración internacional en la lucha contra el cibercrimen

Se menciona la importancia de tratados internacionales como el Convenio de Budapest y los acuerdos con Europol y Ameripol. Sin embargo, en la práctica, la cooperación internacional de los delitos informáticos enfrenta obstáculos significativos. Según el *Módulo 7: Cooperación internacional contra los delitos cibernéticos* de la UNODC (Oficina de las Naciones Unidas contra la Droga y el Delito), la colaboración internacional se promueve mediante acuerdos bilaterales, regionales y multilaterales sobre delitos cibernéticos, siempre que haya una doble sanción (es decir, una estipulación en los acuerdos que requiera que el comportamiento denunciado sea visto como ilegal en los países colaboradores). Sin la doble penalización y sin normativas equilibradas, se generan refugios seguros para los crímenes cibernéticos donde no se puede juzgar a los responsables. La lucha contra el cibercrimen requiere la cooperación de diferentes países debido a varios factores, como la globalización de internet y que los delitos informáticos pueden involucrar actores y víctimas de diferentes países.

Rol de los actores y canales de denuncia/atención

El rol de los actores clave en la investigación de delitos informáticos (fiscales, policías judiciales y peritos forenses) está claramente definido en la cartilla. Sin embargo, una de las críticas recurrentes a la efectividad de la justicia en estos casos es la falta de formación especializada y de herramientas tecnológicas avanzadas. Sin un equipo capacitado y con acceso a *software* de análisis forense de última generación, la lucha contra el crimen informático se ve severamente limitada. A pesar de que el documento presenta distintos canales de denuncia (presencial, virtual, telefónica y escrita), la realidad es que a nivel local (Valledupar) muchas de las personas afectadas y usuarios no pueden acceder a ellos en el instante que los necesitan.



Discusión

Los resultados previstos en este estudio permiten una respuesta afirmativa, aunque con algunos matices, a la cuestión planteada: ¿es eficaz la reacción legal del Estado colombiano ante la cibercriminalidad mediante la Ley 1273 de 2009 y la cartilla metodológica? El estudio de este marco normativo muestra que su instauración representó un importante hito regulatorio en Colombia, al categorizar por primera vez comportamientos vinculados a crímenes informáticos. Sin embargo, la rápida transformación tecnológica ha dejado ciertas lagunas frente a nuevas modalidades de delincuencia como el *ransomware*, el *phishing* basado en inteligencia artificial o la explotación de vulnerabilidades en la nube.

Respecto de la cartilla metodológica de la FGN, se aprecia positivamente su contribución como herramienta de guía operativa para la gestión de cibercrímenes, al establecer de manera precisa los participantes, sus roles y las rutas de atención. No obstante, su eficacia se encuentra restringida por elementos estructurales: escasez de personal especializado, escasa formación en informática forense, ausencia de coordinación institucional y problemas en el acceso de los ciudadanos a los medios de denuncia. Estos componentes influyen de manera negativa en la ejecución práctica de las directrices de la cartilla.

Probablemente, un descubrimiento significativo será la tensión entre la presencia de un marco legal jurídicamente integral y su escasa aplicación práctica, fenómeno que ha sido ampliamente debatido en investigaciones anteriores del derecho penal en Colombia. Otra posible interpretación es que la cibercriminalidad no solo demanda una reacción legal, sino también un cambio cultural e institucional para que los actores legales, expertos y ciudadanos puedan abordarla de manera holística.

Dentro de las restricciones del estudio se encuentra la imposibilidad de acceder a detalles de investigaciones reservadas de la FGN, además de la limitación de conseguir un número limitado de declaraciones de especialistas si no se consiguen las entrevistas previstas. Sin embargo, la orientación documental del estudio garantiza un enfoque adecuado para las multas sugeridas.

Conclusión

La *Cartilla metodológica de atención de los delitos informáticos*, de la Fiscalía General de la Nación, no aborda de manera profunda los mecanismos de apoyo y reparación a las víctimas, más allá del proceso judicial, y su efectividad se ve afectada por la falta de actualización frente a nuevas modalidades de delito, la insuficiencia



de recursos tecnológicos y humanos, y las dificultades en la cooperación internacional. Sin embargo, no podemos desmeritar la gran iniciativa que representa este documento, pues es un instrumento importante para estandarizar los procesos de investigación. Para hacer frente a los desafíos del cibercrimen moderno, es indispensable que la FGN fortalezca la capacitación del personal, implemente herramientas de inteligencia artificial en la investigación y optimice los mecanismos de denuncia y atención a víctimas. Así como la ciudadanía debe mantenerse informada sobre las modalidades para cometer ciberdelitos y prevenir estas vulneraciones de derechos, la meta es estar y sentirnos seguros en el ciberespacio.

Declaración de divulgación

La autora declara que no existe ningún potencial conflicto de interés relacionado con el artículo. Los puntos de vista y los resultados de este artículo pertenecen a la autora y no reflejan necesariamente los de las instituciones participantes. No se emplearon herramientas de generación de contenido por inteligencia artificial (IA) para su elaboración.

Sobre la autora

Angela Rosa Mejía Corrales. Estudiante de la Facultad de Derecho, Fundación Universitaria del Área Andina, sede Valledupar. Integrante del grupo de investigación Verbaiuris, Semillero Derecho Procesal y Probatorio a cargo de la Dra. Margarita Martínez.

<https://orcid.org/0009-0007-3018-4364>

Contacto: amejia90@estudiantes.areandina.edu.co

Referencias

- Ámbito Jurídico. (2012, 10 de septiembre). Cibercriminalidad: la delincuencia en “el otro espacio”. *Ámbito Jurídico*. <https://www.ambitojuridico.com/noticias/penal/penal/cibercriminalidad-la-delincuencia-en-el-otro-espacio>
- Corte Suprema de Justicia. (2022). *Sentencia SP592-2022* (Radicación 50621). [enlace sospechoso eliminado]
- Fiscalía General de la Nación. (s. f.). *Cartilla metodológica de atención de los delitos informáticos*. <https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Methodologica-de-Atencion-de-Delitos-Informaticos.pdf>
- Fiscalía General de la Nación. (2024, 6 de noviembre). *¿Qué es el ciberdelito?* <https://www.fiscalia.gov.co/colombia/judiccionario/que-es-el-ciberdelito/>



Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Enero 5 de 2009. DO. N.º 47.223.

Madariaga Pérez, X. C. (s. f.). *La Corte Suprema de Justicia aclaró elementos normativos del acceso abusivo a un sistema informático*. Blog Opiniones del Instituto Colombiano de Derecho Penal. <https://icdp.org.co/la-corte-suprema-de-justicia-aclaro-elementos-normativos-del-acceso-abusivo-a-un-sistema-informatico/>

Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC]. (2019, junio). *Módulo 7: Cooperación internacional contra los delitos cibernéticos*. <https://www.unodc.org/e4j/es/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html>