Protección Jurídica de los Sistemas Informáticos en Colombia: Retos y Necesidades de Actualización de la Ley 1273 de 2009.

PABLO SUAREZ VALENCIA

Director

NICOLÁS ORTEGA TAMAYO

(Magister en Derecho)

Trabajo de grado presentado como requisito parcial para optar al título de abogado.

Pregrado en Derecho

Escuela de Derecho y Ciencias Políticas

Universidad Pontificia Bolivariana

Medellín

2025

Declaración de Originalidad

Fecha: 29/04/2025

Nombre del estudiante: Pablo Suarez Valencia

Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad.

Declaro, asimismo, que he respetado los derechos de autor y he hecho uso correcto de las normas de citación de fuentes, con base en lo dispuesto en las normas de publicación previstas en los reglamentos de la Universidad.

_____

Firma del estudiante

Dedicatoria

“El amor no mira con los ojos, sino con el alma.”

— William Shakespeare

Dedico este trabajo a mi madre, cuya presencia amorosa me sostuvo en cada jornada universitaria, día tras día, sin descanso ni condiciones. Su fuerza, su ternura y su fe en mí fueron el refugio más constante.

A mi padre, por estar siempre atento, dispuesto a escuchar y responder cada duda, por enseñarme a confiar en mi criterio sin olvidar la humildad del aprendizaje.

A mi hermana, compañera de vida, por ser alegría, apoyo y amor sincero en los momentos en que más lo necesité. Su cercanía me dio calma cuando las fuerzas escaseaban.

Y a mis gatos, Harry, Zeus y Kitty, por compartir conmigo el silencio de las madrugadas, el murmullo de las ideas, y brindarme con cada ronroneo una paz que solo ellos saben dar.

A todos ustedes, que son mi hogar, gracias por ser amor en todas sus formas.

Protección Jurídica de los Sistemas Informáticos en Colombia: Retos y Necesidades de Actualización de la Ley 1273 de 2009.

The Legal Framework for Computer System Protection in Colombia: Challenges and the Imperative to Update Law 1273 of 2009.

RESUMEN

La Ley 1273 de 2009 marcó un avance en la regulación de delitos informáticos en Colombia, como el intrusismo y el sabotaje informático; sin embargo, la evolución tecnológica ha generado vacíos normativos que dificultan la persecución de nuevas amenazas como el ciberacoso y la suplantación de identidad en redes sociales. Ante esta problemática, surge la necesidad de evaluar en qué medida la creación y modificación de tipos penales pueden fortalecer la legislación vigente, lo que se aborda en este trabajo a través de tres objetivos: contextualizar las normas, jurisprudencia y doctrina sobre delitos informáticos en Colombia; examinar la tipificación del sabotaje y el intrusismo informático; y analizar la necesidad de reformar el marco legal. Los resultados muestran que la normativa actual es insuficiente para enfrentar la cibercriminalidad emergente, por lo que se requiere una actualización que incluya nuevos tipos penales y una armonización con estándares internacionales para mejorar la persecución penal y la protección de los derechos digitales.

ABSTRACT

Law 1273 of 2009 marked a significant advancement in regulating cybercrimes in Colombia, such as intrusion and computer sabotage; however, technological evolution has created regulatory gaps that hinder the prosecution of new threats like cyberbullying and identity theft on social media. Given this issue, it is essential to assess to what extent the creation and modification of criminal

offenses can strengthen the existing legislation. This study addresses the topic through three objectives: contextualizing the laws, jurisprudence, and doctrine on cybercrimes in Colombia; examining the classification of sabotage and computer intrusion; and analyzing the need to reform the legal framework. The findings indicate that the current regulations are insufficient to tackle emerging cybercrime, making it necessary to update the legal framework by incorporating new criminal offenses and aligning with international standards to enhance prosecution effectiveness and protect digital rights.

PALABRAS CLAVE

Cibercriminalidad, sabotaje informático, ciberseguridad, protección de datos, malware, sistema informático.

Keywords

Cybercrime, computer sabotage, cybersecurity, data protection, malware, computer system.

INTRODUCCIÓN

La presente investigación se desarrolla en el contexto de la acelerada evolución tecnológica y la creciente sofisticación de los delitos informáticos en Colombia, fenómenos que han puesto de manifiesto las limitaciones de la Ley 1273 de 2009. Aunque esta normativa representó un avance significativo al tipificar conductas como el intrusismo y el sabotaje informático, la transformación constante del entorno digital ha generado vacíos normativos que dificultan la persecución efectiva de modalidades delictivas emergentes, tales como el ciberacoso, la suplantación de identidad en redes sociales y otros delitos que se adaptan rápidamente a los nuevos medios de comunicación. Esta problemática es de alta relevancia, ya que la seguridad digital se ha convertido en un elemento esencial para el funcionamiento de la sociedad moderna, afectando tanto a individuos como

a organizaciones y al propio Estado, lo cual exige una respuesta jurídica ágil y actualizada.

Ante esta coyuntura, el trabajo plantea la interrogante: ¿En qué medida la creación y modificación de nuevos tipos penales pueden constituir una solución efectiva a las deficiencias de la Ley 1273 de 2009? La investigación se orienta a dar respuesta a esta pregunta mediante el desarrollo de tres pilares fundamentales que constituyen, a su vez, los objetivos específicos del estudio. El primer pilar se centra en la contextualización de las normas, la jurisprudencia y la doctrina relacionada con los delitos informáticos en Colombia. Este análisis permite comprender la evolución del marco normativo y las dificultades interpretativas que han surgido a lo largo del tiempo, destacando cómo los cambios tecnológicos han impactado en la aplicación de la ley y en la interpretación de sus preceptos. Se revisan las principales críticas doctrinales y se examinan las sentencias relevantes que han contribuido a definir el alcance y la efectividad de los tipos penales existentes.

El segundo pilar se enfoca en la tipificación del intrusismo y el sabotaje informático, abordando en detalle los elementos constitutivos de estas conductas delictivas. En este apartado se analiza la estructura normativa vigente, identificando las deficiencias que limitan la eficacia de la persecución penal. Se presta especial atención a la dificultad para recopilar evidencia digital y a la naturaleza pluriofensiva de estos delitos, lo que complica la labor de los operadores jurídicos. Este análisis revela que la ambigüedad en la redacción de ciertos tipos penales y la falta de actualización respecto a las nuevas modalidades delictivas generan incertidumbre y desafíos prácticos en el campo de la justicia penal.

El tercer pilar se orienta a la propuesta de reforma, en la cual se examina la necesidad de crear o modificar tipos penales específicos que respondan de manera adecuada a la creciente incidencia de la ciberdelincuencia. Este apartado no solo aborda la revisión crítica de la normativa actual, sino que también propone un marco de referencia para la actualización legislativa, articulando una tercera teoría que integre tanto la evolución normativa como las exigencias prácticas derivadas del

análisis de casos y de la doctrina. La propuesta se fundamenta en la necesidad de armonizar la legislación nacional con los estándares internacionales, de modo que se fortalezca la efectividad de la persecución penal y se garantice una mayor protección de los derechos fundamentales en el entorno digital.

La metodología adoptada para esta investigación es de corte cualitativo y se fundamenta en el paradigma positivista, lo que implica la confrontación del estado actual de la normativa con los vacíos existentes. Se emplea el método analítico, que combina el estudio normativo, la revisión de jurisprudencia y el análisis de casos representativos, permitiendo así obtener una visión holística y crítica de la situación actual. Esta aproximación metodológica facilita la identificación de los elementos problemáticos en la tipificación de los delitos informáticos y sustenta la formulación de propuestas de reforma que sean consistentes con las nuevas realidades del ciberespacio.

La relevancia y pertinencia de este estudio radica en la urgente necesidad de adaptar el marco jurídico colombiano a las demandas de un entorno digital en constante cambio. La globalización, la digitalización de la información y la interconexión de sistemas incrementan la vulnerabilidad frente a ataques informáticos, lo que hace indispensable contar con una legislación que no solo penalice las conductas delictivas, sino que también actúe de manera preventiva y proteja eficazmente los derechos de las víctimas. La revisión de la doctrina y la jurisprudencia evidencia que, a pesar de los esfuerzos realizados, persisten interpretaciones divergentes y vacíos legales que impiden una aplicación uniforme y eficaz de la ley.

En síntesis, este trabajo se erige como una herramienta útil tanto para operadores jurídicos como para legisladores, al integrar de manera rigurosa y sistemática los tres pilares –contextualización, tipificación y propuesta de reforma– que orientan la búsqueda de una justicia penal más acorde con las nuevas realidades tecnológicas y los desafíos del cibercrimen. La ampliación y profundización de estos aspectos permiten no solo evidenciar las limitaciones del

marco legal existente, sino también proponer soluciones concretas que fortalezcan la respuesta estatal frente a los delitos informáticos, contribuyendo así a la construcción de un entorno digital más seguro y justo.

CAPÍTULO I: MARCO NORMATIVO Y JURISPRUDENCIAL DE LOS DELITOS INFORMÁTICOS EN COLOMBIA: AVANCES Y DESAFÍOS

El desarrollo acelerado de las nuevas tecnologías ha generado nuevos desafíos para el derecho penal, en especial en lo referente a la regulación de los delitos informáticos. En Colombia, la Ley 1273 de 2009 representó un avance significativo al tipificar conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos y el daño informático. No obstante, la evolución del mundo virtual ha puesto en evidencia las limitaciones de esta norma y la necesidad de actualizar el marco regulatorio e incluso modificar los tipos penales que allí se contienen.

El propósito de este capítulo es establecer el panorama normativo y judicial que rige la criminalidad informática en Colombia, identificando sus avances y vacíos, con el fin de sentar las bases para la discusión sobre las reformas necesarias en este campo.

NORMATIVA SOBRE DELITOS INFORMÁTICOS

En el ordenamiento jurídico colombiano, la Ley 1273 de 2009 (Congreso de la República, 2009) es la regulación principal que aborda el tema de los delitos informáticos. Además, existen otras disposiciones normativas relacionadas con la informática que complementan este marco. Por ejemplo, la Ley 527 de 1999 (Congreso de la República, 1999) regula el acceso y el uso de mensajes de datos, el comercio electrónico y las firmas digitales; la Ley 962 de 2005 (Congreso de la República, 2005) está orientada a la racionalización de trámites administrativos mediante el uso de las Tecnologías de la Información y Comunicaciones (TIC); y la Ley 1150 de 2007 (Congreso de la República, 2007) introdujo medidas para la eficiencia y transparencia en la contratación pública mediante medios electrónicos.

Asimismo, la Ley 2213 de 2022 (Congreso de la República, 2022), implementada en respuesta a la contingencia del COVID-19, permitió la realización de audiencias y diligencias de forma virtual, modernizando el acceso a la justicia.

Por último, el Acuerdo PCSJA24-12185 del Consejo Superior de la Judicatura (2024) estableció lineamientos específicos para audiencias virtuales o híbridas. Estas disposiciones reflejan la evolución del marco normativo colombiano en materia de tecnología y justicia, abarcando aspectos penales, procesales y administrativos relacionados con la informática y el ciberespacio.

JURISPRUDENCIA SOBRE DELITOS INFORMÁTICOS

En la misma línea, la Corte Suprema de Justicia ha estudiado varios casos en sede de casación, comenzando a definir un norte con respecto a algunos de los artículos que conforman el Título VII Bis. Incluso, es notorio que la Corte ha aplicado enfoques diferenciales de carácter técnico y lógico, lo que ha permitido que el ordenamiento jurídico avance, aunque de manera gradual, hacia una regulación más precisa en materia de delitos informáticos. A continuación, se analizarán algunas de las decisiones más relevantes en este campo.

En la sentencia SP1245-2015, la Corte Suprema de Justicia realiza un análisis profundo del delito de hurto por medios informáticos, estableciendo que este tipo penal se configura como una modalidad subordinada al hurto simple y no como una figura penal autónoma. En este sentido, la Sala de Casación Penal sostiene que el artículo 269I del Código Penal –que tipifica el hurto mediante la superación de medidas de seguridad informáticas– debe interpretarse como un complemento al tipo básico de hurto consagrado en el artículo 239, agregando un elemento agravante que refuerza la protección del patrimonio económico. Así, la Corte enfatiza "la citada disminuyente sólo es aplicable a los delitos que atentan contra el patrimonio económico, y no aquél que propende por la protección de la información y los datos" (CSJ AP 13 sep. 2011, rad. 37.145).

La sentencia profundiza en la integración de dos elementos esenciales para la configuración del delito: por un lado, la acción de superar las medidas de seguridad implementadas en los sistemas informáticos, y por otro, el apoderamiento ilícito de la cosa mueble ajena, lo que produce un perjuicio patrimonial. En este análisis, se subraya que el legislador, al incluir este precepto en el Título VII Bis –destinado a la protección de la información y los datos–, tenía como objetivo primordial resguardar el patrimonio económico.

Asimismo, la Corte critica la interpretación restrictiva que separa la protección de la información de la protección patrimonial, argumentando que es indispensable una lectura sistemática del ordenamiento penal. En consecuencia, si se demuestra que el acusado ha reparado efectivamente el daño ocasionado al patrimonio debe aplicarse el descuento punitivo previsto en el artículo 269 del Código Penal, en correspondencia con el objetivo preventivo y correctivo del derecho penal. La Corte concluye que "la decisión justa y prevalente frente al derecho sustancial es en este caso reconocer la aplicación de la disminuyente por el resarcimiento" (CSJ AP, 14 ago. 2012, rad. 39.160), lo que permite armonizar los elementos del ciberespacio con los fundamentos tradicionales de la tipicidad.

En la sentencia SP14302-2016, la Corte Suprema de Justicia, mediante la ponencia del Magistrado Luis Guillermo Salazar Otero, analiza de forma exhaustiva el delito de hurto por medios informáticos y su integración en el marco penal colombiano. La sentencia se centra en determinar si la conducta reprochada, consistente en la manipulación indebida de medios tecnológicos para sustraer fondos a través de cajeros electrónicos, encaja como una modalidad subordinada del hurto simple, previsto en los artículos 239 y 240 del Código Penal, o si merece ser considerada de forma autónoma.

La Corte interpreta que el delito de hurto por medios informáticos, tipificado en el artículo 269I, funciona como una extensión del hurto tradicional, al incorporar el elemento adicional de superar las medidas de seguridad electrónicas. En este sentido, se destaca que el legislador, al adicionar este tipo penal con la Ley 1273 de

2009, no pretendió crear una nueva figura delictiva, sino enriquecer el mecanismo de desplazamiento ilícito del bien mueble, enfatizando que "la conducta reprobada es el apoderamiento ilícito de una cosa mueble ajena" al cual se le suma la modalidad de vulnerar las seguridades informáticas (CSJ SP14302-2016, rad. 41517).

La sentencia explica que, para la configuración del delito, es indispensable analizar tanto el medio –es decir, la manipulación del sistema informático o la suplantación de la identidad digital– como el fin, que es el apoderamiento del valor económico, constituyendo así un delito pluriofensivo en el que se protegen simultáneamente el patrimonio económico y la seguridad en el tráfico de la información; esto es bastante similar a la sentencia evaluada anteriormente. Además, la Corte subraya la importancia de aplicar los beneficios de reducción de pena, argumentando que, en aras de los principios de necesidad, proporcionalidad y razonabilidad, el hecho de restituir el monto sustraído y la ausencia de antecedentes deben ser considerados para la disminución de la sanción (CSJ SP14302-2016, rad. 41517).

En sentencia SP2699-2022 se pronuncia de forma detallada sobre la configuración del delito de daño informático en el caso de Greis Katerin Gutiérrez Solano. En la sentencia, la Sala analiza que la conducta imputada –trasladar 64 archivos desde una carpeta compartida (NAS) a la "papelera de reciclaje" – encaja en la modalidad de daño informático, al afectar la integridad y la disponibilidad del sistema de tratamiento de la información.

La Corte enfatiza que, aunque el acto en cuestión no implica la eliminación definitiva de los datos –Conducta que sería compatible con la modalidad "suprimir"— , la reubicación de la información en la papelera de reciclaje vulnera los mecanismos de seguridad diseñados para garantizar la operatividad del sistema, constituyendo así un daño a la protección de la información. En su análisis, se señala que "la acción de manipular el equipo servidor, de trasladar archivos a un espacio destinado a la eliminación, afecta la funcionalidad del sistema y pone en

riesgo la integridad de los datos", lo que, en conjunto, configura el delito tipificado en el artículo 269D del Código Penal (CSJ SP2699-2022, rad. 59733).

Asimismo, la decisión aborda la importancia de valorar la prueba pericial y los testimonios, con el fin de determinar que la conducta de la acusada no se limitó a un simple error operativo, sino que se realizó de manera dolosa, con conocimiento de que dicho proceder alteraría la normal operación del sistema informático. La Corte, por tanto, interpreta que la modalidad "borrar" adoptada en el caso no se entiende únicamente en términos de la desaparición física de los datos, sino en función del perjuicio que causa la alteración de la estructura informativa y la interrupción en la disponibilidad de la información.

En definitiva, la sentencia subraya que la conducta punible debe analizarse de forma integral, combinando tanto los elementos materiales –la acción de trasladar y, en consecuencia, vulnerar la integridad del sistema– como los elementos intencionales, que configuran el dolo necesario para la aplicación del delito de daño informático. (CSJ SP2699-2022, rad. 59733).

En sentencia SP473-2023, emite una decisión que involucra los delitos de acceso abusivo a sistemas y falsedad material en documento público. La Sala, analiza el comportamiento de Sandra Liliana Espinosa Villamizar, quien ingresó sin autorización al Sistema Integrado de Gestión (SIG) del CTI en Pamplona, con el objetivo de introducir prórrogas inexistentes en diversas investigaciones. La Corte se centra en determinar que la conducta imputada encaja con el delito de acceso abusivo, previsto en el artículo 269A del Código Penal, ya que la acusada utilizó de forma reiterada el usuario y la contraseña del coordinador seccional del CTI, sin contar con la autorización expresa requerida, lo que “constituye una vulneración del control de acceso que salvaguarda la integridad de la información” (CSJ SP473-2023, rad. 57922).

La sentencia profundiza en el análisis de los elementos objetivos del delito, subrayando que, aunque la defensa intentó justificar el acceso mediante una

supuesta autorización "tácita", la prueba testimonios de los funcionarios –como el coordinador del CTI, Jairo Mogollón– y los informes periciales demuestran que el ingreso a la plataforma se realizó de manera irregular y sin respaldo formal. La Corte aclara que “la autorización para ingresar al SIG se otorga de forma excepcional y, en el caso de la acusada, no se constató tal autorización en las 77 ocasiones en que accedió al sistema” (CSJ SP473-2023, rad. 57922).

Asimismo, en lo que respecta al delito de falsedad material en documento público, la Corte destaca que la introducción de datos falsos en el SIG afecta no solo la veracidad de la información, sino la confianza pública depositada en los sistemas institucionales. La decisión enfatiza que la modificación indebida de las órdenes de trabajo –sin contar con el formato de Comunicación con el Cliente exigido– constituye una alteración que perjudica la integridad del documento electrónico y, por ende, el bien jurídico tutelado de la fe pública. La Sala sostiene que “el acceso sin autorización y la posterior falsificación de datos en el SIG vulneran de manera directa el mecanismo de control y supervisión que el sistema debiera garantizar” (CSJ SP473-2023, rad. 57922).

La interpretación de la Corte Suprema de Justicia en esta sentencia se orienta a reafirmar la necesidad de proteger los sistemas informáticos mediante la aplicación estricta de los tipos penales previstos para el acceso abusivo y la falsedad documental, destacando que la conducta dolosa de la acusada atenta contra la seguridad de la información y la fe pública. La decisión, con un análisis riguroso de los elementos del tipo y de la prueba aportada, reafirma la postura de que la integridad del sistema informático y la veracidad de los documentos electrónicos constituyen bienes jurídicos de especial protección en el contexto de la criminalidad digital.

En la sentencia SP479-2023, se pronuncia sobre la acusación de daño informático en el contexto del proceso sucesoral que involucró al juez Ricardo Estrada Morales. La Sala de Casación Penal, encabezada por la Magistrada ponente Myriam Ávila Roldán, analiza si la conducta denunciada –es decir, la

supuesta manipulación del Sistema Integrado de Gestión (SIG) para alterar el reparto de expedientes– encaja en el delito tipificado en el artículo 269D del Código Penal.

La Corte interpreta que, para configurar el delito de daño informático, es esencial demostrar que la acción del agente alteró de forma significativa la integridad o la disponibilidad de los datos o del sistema de tratamiento. En este caso, se observó que, en el momento de la asignación del expediente, el número de asuntos se discontinuó (pasó de 217 a 0 y luego a 218), sin embargo, "no se probó de forma directa que el juez Estrada Morales hubiese intervenido en la manipulación del sistema, ni que su accionar causase un daño efectivo al bien jurídico protegido" (CSJ SP479-2023, rad. 59538).

La sentencia profundiza en los elementos estructurales del tipo penal, enfatizando que la mera alteración de la “puerta electrónica” –como metáfora del mecanismo de reparto– debe traducirse en una perturbación tangible del funcionamiento del sistema para imputarse el delito. En este sentido, la Sala subraya que "la alteración del sistema debe repercutir de forma directa en la operatividad de este, y en el presente caso la evidencia pericial no evidenció tal perturbación"(CSJ SP479-2023, rad. 59538), lo que justifica la absolución respecto del daño informático.

Además, la Corte contextualiza su análisis en el marco normativo internacional, haciendo referencia al Convenio sobre la Ciberdelincuencia de Budapest y señalando que, si bien Colombia adoptó disposiciones inspiradas en dicho instrumento, el análisis debe centrarse en la demostración de un daño material real en el sistema. Así, se reafirma que, para incurrir en el delito de daño informático, es necesario que la conducta alteradora afecte de manera sustancial la integridad y disponibilidad de los datos o del sistema, condición que no se cumplió en el caso examinado.

Esta interpretación, sustentada en un riguroso examen de la prueba y en los fundamentos doctrinales y normativos, reafirma la coherencia del ordenamiento penal en la protección de los sistemas informáticos, integrando los elementos propios del ciberespacio con los principios tradicionales de la tipicidad.

En la sentencia SP903-2024, ofrece un análisis detallado de los delitos informáticos en el contexto de la manipulación del sistema de reparto de expedientes. En dicha decisión se examinan, de forma conjunta, tres tipos penales que involucran elementos cibernéticos: utilización ilícita de redes de comunicaciones, acceso abusivo a un sistema informático agravado y daño informático agravado.

En primer lugar, la Sala puntualiza que la conducta imputada en el delito de utilización ilícita de redes de comunicaciones consiste en el uso indebido de equipos terminales conectados a la red, lo que permitió la modificación fraudulenta de la base de datos del Sistema de Administración Reparto Judicial (SARJ). La Corte destaca que "la conducta imputada se fundamenta en el uso ilícito de equipos que facilitan el acceso y la manipulación de datos, afectando la integridad del proceso de reparto" (CSJ SP903-2024, rad. 65376).

Respecto al delito de acceso abusivo a un sistema informático agravado, la sentencia señala que el procesado, mediante el uso de credenciales no autorizadas –en este caso, a través del usuario y la contraseña asignados de manera irregular–, facilitó el ingreso al sistema de reparto de la Rama Judicial. La Sala subraya que "la participación del acusado, en tanto que determinador del acceso, se materializa en la utilización de medios electrónicos para entrar a un sistema protegido, sin contar con la autorización correspondiente" (CSJ SP903-2024, rad. 65376).

En cuanto al delito de daño informático agravado, la Corte explica que la alteración de la base de datos y la posterior eliminación de registros en la memoria del sistema 'BITÁCORA' constituyen actos que afectan de forma directa la integridad y disponibilidad de los datos. La Sala enfatiza que "para la configuración del delito

de daño informático es indispensable que la conducta cause un perjuicio material en el funcionamiento del sistema, lo cual se evidenció en la manipulación manual y la supresión de registros" (CSJ SP903-2024, rad. 65376).

Asimismo, la sentencia profundiza en los elementos subjetivos de estos delitos, remarcando que la participación del acusado como servidor público en ejercicio de sus funciones implica un conocimiento y voluntad inequívoca de obrar ilícitamente –la Corte examinó los elementos del dolo y determinó que existía en este caso—, utilizando su posición para favorecer a terceros. La integración de estos elementos permite a la Corte concluir que el plan criminal, ideado para manipular el reparto del proceso judicial, vulneró de forma sistemática la seguridad de las comunicaciones oficiales y la integridad del sistema informático.

En definitiva, la interpretación de la Sala se orienta a confirmar que, para incurrir en los delitos informáticos aquí analizados, es fundamental demostrar tanto la acción antijurídica –mediante la utilización y manipulación indebida de los sistemas electrónicos– como el daño efectivo a los bienes jurídicos protegidos. Este enfoque integrador y sistemático refuerza la coherencia del ordenamiento penal en la protección de la administración de justicia en el entorno digital (CSJ SP903-2024, rad. 65376).

DOCTRINA SOBRE DELITOS INFORMÁTICOS

Así como para la Corte Suprema de Justicia, el tema de los “ciber-tipos penales” es también uno que se ha planteado revisar la doctrina. Actualmente en Colombia existen dos obras que reflejan los pensamientos que nacen producto de la combinación entre los delitos y la informática. Es menester también dar un breve repaso por estas dos obras.

EL CIBERCRIMEN Y SUS EFECTOS EN LA TEORÍA DE LA TIPICIDAD

Este texto plantea que los cibercrímenes presentan características distintas a los delitos tradicionales, lo que genera desafíos para la teoría del delito y la tipicidad penal. Posada Maya argumenta que la teoría de la tipicidad debe ser replanteada

debido a la naturaleza deslocalizada y virtual de estos delitos, los cuales involucran cada vez menos intervención humana directa.

El autor señala que el desarrollo del derecho penal ha estado históricamente basado en la imputación causal objetiva y subjetiva en el mundo físico, lo que se ve desafiado por los delitos informáticos. Se destaca la necesidad de redefinir los bienes jurídicos protegidos en el entorno digital, incluyendo la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos (Posada Maya, 2017, p. 74).

Además, se advierte que el cibercrimen ha traído consigo nuevos riesgos delictivos que no pueden ser abordados de manera efectiva con la teoría del "delito analógico", debido a la complejidad y automatización de los delitos digitales. Posada Maya sugiere que se deben replantear los criterios de imputación y las categorías dogmáticas del derecho penal para abordar estas nuevas formas de criminalidad (Posada Maya, 2017, p. 77).

CIBERCRIMEN: DERECHO PENAL Y NUEVAS TECNOLOGÍAS

Este libro recopila investigaciones de varios doctrinantes sobre la relación entre el derecho penal y las nuevas tecnologías, centrándose en los desafíos normativos y criminológicos del Título VII Bis del Código Penal colombiano.

Uno de los principales aportes proviene de Helmut Satzger, quien compara el derecho penal colombiano y alemán en materia de delitos informáticos. Destaca que ambos sistemas han tomado como referencia el Convenio de Budapest de 2001 para armonizar sus legislaciones, aunque con diferencias en la tipificación penal. Satzger enfatiza que "en una sociedad de la información no pueden existir espacios libres de derecho, por lo que las normas penales deben adaptarse a las nuevas circunstancias del ciberespacio" (Satzger, 2016, p. 12).

Por su parte, Fernando Miró Llinares aborda la "cibercriminalidad 2.0", explicando cómo el delito ha evolucionado en el entorno digital. Resalta que la ciberdelincuencia no solo se expande debido a la tecnología, sino que también

plantea un problema criminológico único: "El cibercrimen transforma radicalmente el espacio y el tiempo, eliminando las barreras físicas del delito tradicional" (Miró Llinares, 2016, p. 59).

Otro aspecto relevante es la perspectiva de Fernando Velásquez Velásquez, quien reflexiona sobre la responsabilidad penal en el ciberespacio. Afirma que el derecho penal debe evitar caer en un "expansionismo punitivo" que sacrifique garantías fundamentales bajo la excusa de la ciberseguridad (Velásquez, 2016, p. 353).

El análisis del marco normativo y jurisprudencial en materia de delitos informáticos evidencia que, si bien Colombia ha avanzado en la regulación de estas conductas, aún persisten vacíos y desafíos en su aplicación y en su regulación a nivel doctrinal y jurisprudencial que, si bien son criterios auxiliares, pueden ayudar a subsanar esos “descuidos” que pudo tener el legislador. La evolución tecnológica y la sofisticación de la ciberdelincuencia requieren una actualización constante del ordenamiento jurídico para garantizar una protección efectiva de los bienes jurídicos involucrados, es por esto que se pretende evaluar en los próximos capítulos las herramientas típicas, antijurídicas y culpables que salvaguardan el bien jurídico de la “protección de la información y los datos”.

CAPÍTULO II: TIPIFICACIÓN PENAL DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

INTRODUCCIÓN

En la era digital, la seguridad informática se ha convertido en una preocupación central para gobiernos, empresas y ciudadanos. El acceso indebido a sistemas informáticos representa una amenaza creciente, que abarca desde actos de exploración no autorizada hasta sabotajes con graves consecuencias económicas y sociales. En Colombia, la regulación del intrusismo informático se materializa a través de la Ley 1273 de 2009 (Congreso de la República, 2009), que

introdujo nuevas tipificaciones penales para enfrentar los delitos informáticos y fortalecer la protección de los sistemas digitales.

DELITOS INFORMÁTICOS: DEFINICIÓN

El desarrollo de las tecnologías de la información y la comunicación ha propiciado la aparición de nuevas formas de criminalidad, entre ellas los delitos informáticos. La doctrina ha ofrecido diversas definiciones para caracterizar estas conductas ilícitas, coincidiendo en que se trata de acciones delictivas que involucran el uso indebido de medios electrónicos, sistemas computacionales o el tratamiento automatizado de información.

Desde una perspectiva amplia, Callegari define los delitos informáticos como "aquellos que se dan con la ayuda de la informática o de técnicas anexas" (Conde O'Donnell, González & Heredia, 2009). En una línea similar, el Departamento de Investigación de la Universidad de México considera que estos delitos abarcan "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático" (Conde O'Donnell et al., 2009).

Otros autores destacan el papel de la computadora dentro de la estructura del delito. El italiano Carlos Sarzana señala que el delito informático puede comprender "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo" (Conde O'Donnell et al., 2009). Por su parte, María de la Luz Lima diferencia entre "delitos electrónicos", entendidos como cualquier conducta criminógena que involucra tecnología electrónica, y "delitos informáticos", los cuales se definen estrictamente como "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin" (Conde O'Donnell et al., 2009).

Un aporte más estructurado es el del profesor Renato Jijena Leiva, quien enfatiza la relación entre los delitos informáticos y la dogmática penal. En su obra Chile, La protección penal a la intimidad y el delito informático, afirma que estos

ilícitos deben entenderse como "toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado" (Leiva Jijena, 1992, p. 225).

Desde una visión más contemporánea, Cuenca Espinoza sostiene que los delitos informáticos constituyen "toda actividad en la cual se utilizan medios computacionales, telemáticos o electrónicos para el cometimiento de un delito; delitos que constituyen nuevas formas penales que incluyen como elementos primogénitos al internet como instrumento abstracto y a la computadora como instrumento físico" (Cuenca Espinoza, 2013, p. 220).

Con base en estas definiciones, se logra evidenciar que el delito informático no solo abarca conductas que afectan la integridad de los sistemas computacionales, sino también aquellas en las que la tecnología actúa como medio facilitador de delitos tradicionales. Esta distinción resulta clave para la clasificación doctrinal de estos ilícitos.

DISPOSICIONES DE LA LEY 1273 DE 2009 Y SUS GENERALIDADES

Tal y como se ha mencionado antes, el Título VII Bis del Código Penal abarca un conjunto de tipos penales que pueden agruparse en dos grandes categorías: (i) ataques contra la confidencialidad, integridad y disponibilidad de la información y los sistemas informáticos, y (ii) fraudes y otros delitos que emplean medios informáticos como instrumento de comisión; es decir que hay un grupo en donde la conducta típica, antijurídica y culpable se relaciona con el actuar de una sujeto activo que busca de manera dolosa el causar un injusto respecto de los sistemas informáticos y otro grupo donde la conducta enmarca el actuar de un sujeto activo que comete conductas que buscan proteger otros bienes jurídicos pero que usan medios informáticos para la comisión de los delitos.

Este capítulo se va a centrar en analizar dos grandes grupos de conductas penales, estas son: (i) el sabotaje informático, que se refiere a aquellas conductas

que perjudican sistemas informáticos; y (ii) el intrusismo informático, que agrupa aquellas conductas que captan datos informáticos de los sistemas sin autorización.

SABOTAJE INFORMÁTICO

DEFINICIÓN

El sabotaje informático puede ser entendido como una conducta delictiva que tiene como finalidad la afectación, interrupción o alteración del funcionamiento de sistemas informáticos, redes de telecomunicaciones o datos almacenados. Su impacto puede ir desde la paralización de servicios esenciales hasta la destrucción de información crítica en infraestructuras estratégicas. A diferencia de otros delitos informáticos, el sabotaje no necesariamente persigue un beneficio económico o una apropiación indebida de información, sino que su objetivo principal es causar un perjuicio en la operatividad de los sistemas, incluso al punto de que estos queden inutilizables – por largos periodos de tiempo – o de plano inservibles.

Doctrinalmente, diversos autores han abordado el concepto, Fernando Miró Llinares, por ejemplo, define el sabotaje informático como “cualquier conducta orientada a dañar, inutilizar o interferir en el funcionamiento de un sistema informático, independientemente de si la acción se ejecuta desde dentro o fuera del sistema” (Miró Llinares, 2016, p. 55). En el mismo sentido, Renato Jijena Leiva sostiene que esta figura se configura cuando una persona “realiza una alteración no autorizada de un sistema informático con la finalidad de afectar su operatividad o disponibilidad, sin necesidad de que exista una apropiación de información” (Jijena Leiva, 1992, p. 225). Ambos autores enfatizan la naturaleza destructiva del sabotaje y su distinción con otras formas de cibercriminalidad como el fraude informático o la interceptación de datos.

El impacto del sabotaje informático ha cobrado especial relevancia en el contexto de los ataques dirigidos contra infraestructuras críticas, como los servicios de energía, agua, telecomunicaciones y salud. María Concepción Gorjón Barranco destaca que el reto jurídico actual radica en determinar la gravedad del daño y su

impacto en la seguridad nacional, dado que muchos ataques pueden parecer de baja intensidad, pero tienen consecuencias significativas en el funcionamiento de servicios esenciales (Barranco, 2021, p. 80). Así mismo, Samuel Malamud Herrera enfatiza la importancia de incluir el daño grave como elemento fundamental para diferenciar el sabotaje informático de otras formas de afectación a los sistemas informáticos. Para este autor, la alteración de datos y sistemas no siempre tiene la misma relevancia penal, por lo que es crucial definir qué tipo de daño justifica una mayor intervención del derecho penal (Herrera, 2018, p. 145).

A continuación, se analizarán los tipos penales que están relacionados con el sabotaje informático con la finalidad de establecer si su regulación es suficiente o no para cubrir las posibles conductas punitivas que se pueden producir actualmente gracias a los avances tecnológicos.

ARTICULO 269B

El Código Penal Colombiano (Congreso de la República, 2000), a través de la Ley 1273 de 2009 (Congreso de la República, 2009), incorporó el Artículo 269B, el cual establece sanciones para quienes impidan o dificulten el funcionamiento de sistemas informáticos o redes de telecomunicaciones sin autorización. Esta disposición busca proteger la disponibilidad y operatividad de las infraestructuras digitales, castigando conductas que, aunque no impliquen destrucción de datos, pueden generar interrupciones significativas en el acceso y uso de la información. El texto del artículo dispone lo siguiente:

> *Articulo 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 la República, 2000)

Analizando los elementos del tipo penal, el sujeto activo es "El que", lo que indica que es un delito de sujeto activo común y puede ser cometido por cualquier persona sin necesidad de una calidad específica, facilitando así la imputación sin limitarla a sujetos con conocimientos técnicos avanzados. El sujeto pasivo puede ser una persona natural, jurídica o el Estado, ya que el daño puede recaer sobre entidades privadas o públicas que dependen de sistemas informáticos y redes de telecomunicaciones.

La conducta punible se encuentra delimitada por los verbos rectores "impedir" y "obstaculizar. Ambos verbos amplían el espectro del delito, permitiendo sancionar tanto ataques completos como acciones que solo degraden el rendimiento del sistema.El objeto de la acción es amplio, ya que abarca sistemas informáticos, datos contenidos en ellos y redes de telecomunicaciones. Esto permite incluir una variedad de ataques informáticos, desde ataques de denegación de servicio (DDoS) hasta interferencias en redes de telecomunicaciones.

La conducta típica debe realizarse "sin estar facultado para ello", lo que introduce un elemento normativo que requiere verificar si el sujeto tenía o no autorización para realizar la acción. En cuanto al resultado, no se exige un daño concreto, ya que basta con la afectación al acceso o funcionamiento del sistema.Se trata de un delito de mera conducta, lo que significa que se sanciona la acción en sí misma sin necesidad de que se produzca un daño económico o informático medible. La culpabilidad exige dolo, ya que el sujeto debe conocer que está impidiendo u obstaculizando el sistema sin facultad para ello. No se contempla la posibilidad de comisión culposa, lo que excluye errores técnicos involuntarios.

A pesar de la estructura de este tipo penal, existen varios vacíos normativos que pueden generar problemas de interpretación y aplicación. En primer lugar, los verbos rectores "impedir" y "obstaculizar" presentan ambigüedad, ya que no se define con precisión qué nivel de interferencia se considera "obstaculización". Esto puede generar incertidumbre sobre si un ataque DDoS masivo que ralentiza un sistema durante unos minutos se sanciona de la misma forma que una interferencia

mínima en la conectividad, o si la sanción debiese ser la misma para el caso de un ataque de Secuestro de Sesión donde solo se efectúa una intervención de carácter Man-in-the-Middle (MitM) que para el caso del ya mencionado DDoS masivo donde pueden interferir una botnet de millones de computadores infectados.

Otro problema es la falta de claridad sobre el alcance de la expresión "sin estar facultado para ello". No se especifica qué se considera "facultado", lo que puede generar dificultades en entornos corporativos o académicos donde ciertas pruebas de seguridad informática pueden implicar acciones que "obstaculicen" un sistema, aunque estas se realicen con autorización implícita. Además, el artículo 269B omite la modalidad culposa, lo que deja fuera casos en los que el sujeto actúa con imprudencia o negligencia y genera una afectación grave al sistema. Por ejemplo, un técnico que, sin intención, desactiva un firewall y expone un sistema a un ataque podría quedar sin sanción penal, a pesar del daño causado.

Por último, el tipo penal parece centrarse en ataques externos, dejando fuera los denominados "insider threats" o amenazas internas. Empleados desleales o administradores de sistemas con acceso autorizado pueden obstaculizar intencionalmente sistemas informáticos como parte de sabotajes internos. Un empleado con acceso legítimo que deliberadamente ralentiza un sistema antes de renunciar podría no ser sancionado bajo este artículo, ya que formalmente está "facultado" para operar sobre el sistema.

ARTICULO 269D

El Código Penal Colombiano, mediante la Ley 1273 de 2009 (Congreso de la República, 2009), introdujo el Artículo 269D, el cual establece sanciones para quienes, sin autorización, afecten la integridad de los datos informáticos o sistemas de información. Este delito busca proteger la confiabilidad y disponibilidad de la información, castigando acciones que comprometan la estructura de los sistemas digitales, ya sea mediante su destrucción, alteración o eliminación. El texto del artículo dispone lo siguiente:

> *Artículo 269D. Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes* (Congreso de la República, 2000).

El sujeto activo es "El que", lo que indica que se trata de un delito común, es decir, puede ser cometido por cualquier persona sin necesidad de una calidad técnica o especial. El sujeto pasivo puede ser una persona natural, jurídica o el Estado, ya que los daños a la infraestructura informática pueden afectar tanto a individuos como a entidades privadas y públicas.

Este tipo penal es compuesto, se enfoca en múltiples conductas que buscan prevenir la consumación de la conducta punible. Según la jurisprudencia de la Corte Suprema de Justicia y el Informe Explicativo del Convenio de Budapest: "Destruir" implica la eliminación total de los datos o del sistema, haciendo que desaparezcan y sean irreconocibles. "Dañar" y "deteriorar" se refieren a una alteración negativa de la integridad o del contenido de la información, los datos o programas. "Borrar" es equivalente a la destrucción de un objeto corpóreo, eliminando los datos de forma que desaparezcan por completo. "Suprimir" significa cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al sistema. "Alterar" implica la modificación de los datos existentes (Citar el convenio y la sp 2022).

El objeto de la acción comprende tanto datos informáticos como sistemas de tratamiento de información o sus componentes lógicos, lo que permite la protección desde archivos individuales hasta infraestructuras tecnológicas más complejas, lo que, a su vez, permite castigar varios niveles de ataques informáticos. En cuanto a la modalidad de comisión, la norma exige que la acción se realice "sin estar facultado para ello", lo que introduce un elemento normativo que requiere evaluar si el sujeto activo tenía autorización para realizar la conducta.

El resultado del delito no exige necesariamente una afectación económica o técnica medible, ya que basta con la alteración o eliminación de los datos o sistemas. Se trata de un delito de mera conducta, lo que significa que se castiga la simple realización de la acción sin que sea necesario demostrar un perjuicio concreto. Se requiere dolo, ya que el sujeto debe conocer que está afectando datos o sistemas sin tener autorización para ello. Tampoco contempla la comisión culposa, lo que excluye la posibilidad de sancionar negligencias o errores técnicos involuntarios.

Uno de los principales problemas es la ambigüedad en los verbos rectores. El artículo emplea términos como "destruir", "dañar", "borrar", "deteriorar", "alterar" y "suprimir", pero no establece criterios objetivos para diferenciar entre ellos. Por ahora, la Corte Suprema de Justicia en sede de Casación ha analizado una sola vez el conflicto entre los verbos borrar y suprimir, pero no propone una conclusión exhaustiva. Otro vacío importante es la falta de claridad sobre el alcance del "sin estar facultado para ello". No se especifica, tal como se había expuesto en el tipo 269B, qué significa estar "facultado", para realizar una modificación en un sistema.

Hay también un problema que nace al comprobar la omisión de la modalidad culposa. El tipo penal solo contempla la comisión dolosa, lo que deja por fuera casos en los que un sujeto, por negligencia o imprudencia, genera un daño significativo en sistemas informáticos.

INTRUSISMO INFORMÁTICO

DEFINICIÓN

El intrusismo informático, también conocido como hacking, se define como la acción de acceder sin autorización a un sistema informático, violando las medidas de seguridad establecidas para impedirlo (Turégano, 2016). Esta conducta puede clasificarse dentro de los delitos contra la seguridad informática, ya que busca quebrantar la integridad de los sistemas y acceder a información privada o restringida (Turégano, 2016).

Desde una perspectiva doctrinal, el intrusismo informático comprende no solo el acceso no autorizado, sino también la interferencia indebida en las comunicaciones electrónicas y el uso ilícito de sistemas informáticos o redes (Gutiérrez Francés, 1996). En este sentido, se puede distinguir entre hackers, quienes acceden por curiosidad o para demostrar vulnerabilidades, y crackers, quienes persiguen fines ilícitos como la obtención de información, el espionaje o el sabotaje (Gutiérrez Francés, 1996).

ARTÍCULO 269A

El Código Penal Colombiano (Congreso de la República, 2000) establece en el Artículo 269A el delito de acceso abusivo a un sistema informático, el cual fue incorporado mediante la Ley 1273 de 2009 (Congreso de la República, 2009) con el objetivo de proteger la integridad y seguridad de los sistemas informáticos. Esta disposición penaliza el ingreso no autorizado a sistemas informáticos, ya sea que cuenten con medidas de seguridad o no, así como la permanencia indebida dentro de estos en contra de la voluntad del titular legítimo. El texto del artículo dispone lo siguiente:

> *Artículo 269A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.* (Congreso de la República, 2000)

El sujeto activo de este delito es "El que", lo que indica que se trata de un delito común y puede ser cometido por cualquier persona sin necesidad de una cualificación técnica, lo que facilita su aplicación a diversos contextos, desde hackers hasta empleados que acceden indebidamente a sistemas internos. El sujeto pasivo es el titular legítimo del sistema informático, que puede ser una persona natural, jurídica o el Estado.

La acción punible está determinada por dos verbos rectores importantes, estos son “Acceder” y “Mantener”. Para el primero de estos verbos existen una especie de condicionales que podemos desglosar: (i) "acceder sin autorización" implica entrar en un sistema informático sin permiso, ya sea porque no se tienen credenciales legítimas o porque se eluden medidas de seguridad y (ii) "acceder por fuera de lo acordado" ocurre cuando un usuario con acceso legítimo excede los límites de su autorización. Respecto del segundo verbo también hay una condicional, este habla de "Mantenerse dentro del sistema en contra de la voluntad de quien tiene derecho a excluirlo" y se configura cuando una persona accede legítimamente a un sistema, pero permanece en él después de que se le haya revocado el permiso.

El objeto de la acción es un sistema informático, que puede estar protegido o no con medidas de seguridad. Esta redacción amplía la aplicabilidad del tipo penal, ya que no se requiere que el sistema tenga mecanismos de autenticación avanzados – como claves One-Time-Password (OTP), claves físicas, etc – para que la conducta sea punible. La modalidad de comisión se basa en el acceso sin autorización o en el incumplimiento de los límites previamente acordados. Esto introduce un elemento normativo que requiere evaluar si el acceso fue efectivamente indebido según las políticas del sistema.

El resultado del delito no exige un daño concreto, sino que se sanciona el acceso o la permanencia indebida en sí misma, lo que lo convierte en un delito de mera conducta. No es necesario que se produzca una afectación adicional a los datos o al funcionamiento del sistema para que la conducta sea penalmente relevante. En cuanto a la culpabilidad, el delito requiere dolo, es decir, que el sujeto conozca que está accediendo o manteniéndose en el sistema sin autorización. No se contempla la modalidad culposa, lo que excluye a quienes ingresan por error o por fallos del sistema.

Uno de los principales inconvenientes se encuentra en la falta de claridad sobre la protección de sistemas sin medidas de seguridad. El artículo penaliza el

acceso a sistemas protegidos o no protegidos con medidas de seguridad, lo que implica que incluso sistemas abiertos pueden generar responsabilidad penal. Esto podría llevar a la criminalización del acceso a información pública en línea si el propietario del sistema alega que el usuario ingresó sin su autorización.

Adicionalmente, el tipo penal no diferencia con precisión entre el acceso inicial y la permanencia indebida en el sistema. No se establecen criterios claros para distinguir ambas conductas ni para determinar cuándo un usuario ha sido legítimamente excluido. Puede haber casos en los que una persona no sea notificada de la revocación de su acceso y aun así sea imputada por la comisión de dicha conducta. Por ejemplo, si una empresa despide a un trabajador, pero no desactiva su cuenta de usuario de inmediato, y este ingresa sin saber que ya no tiene autorización, ¿comete el delito?

En suma, el tema de la omisión de la modalidad culposa también representa un problema. El tipo penal solo contempla la comisión dolosa, lo que excluye a quienes acceden por error o por desconocimiento de restricciones. Esto podría generar lagunas en la protección de infraestructuras críticas, ya que no se sanciona el ingreso accidental a un sistema. Por ejemplo, un usuario que introduce mal una URL y accede a un sistema sin saber que es privado, ¿queda exento de responsabilidad, aunque acceda a información sensible?

ARTÍCULO 269C

El Código Penal Colombiano (Congreso de la República, 2000) establece en el Artículo 269C el delito de interceptación de datos informáticos, el cual fue introducido mediante la Ley 1273 de 2009 (Congreso de la República, 2009) con el propósito de proteger la confidencialidad y seguridad de la información digital. Esta norma sanciona a quien, sin autorización judicial, intercepte datos informáticos en tránsito o almacenados en un sistema informático, así como las emisiones electromagnéticas asociadas a su transmisión. El texto del artículo dispone lo siguiente:

> *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 la República, 2000)

El sujeto activo de este delito es "El que", lo que, como los anteriores tipos penales, lo califica como un delito común. Esto facilita su aplicación en distintos escenarios, desde individuos que realizan espionaje personal hasta organizaciones dedicadas a la vigilancia ilícita. El sujeto pasivo es cualquier persona o entidad cuyos datos informáticos sean objeto de interceptación ilegal, lo que incluye tanto a personas naturales, jurídicas como al Estado.

La acción punible se configura a partir del verbo rector “interceptar”. La primera modalidad de conducta que debemos examinar se trata de "interceptar datos informáticos en su origen", esto implica captar información en el momento en que es generada o enviada por un usuario – El ataque Man-in-the-Middle donde una persona ajena a la conexión usuario – servidor puede ver todo el tráfico que entre estos hay, es una forma de esta conducta –. Otra modalidad de conducta se da al "interceptar datos informáticos en su destino" hace referencia a captar información en el momento en que está llegando al destinatario previsto. Una tercera modalidad es aquella que se refiere a "interceptar datos informáticos en el interior de un sistema informático" consiste en captar información que se encuentra almacenada dentro de un sistema digital. Por último, la cuarta conducta habla de "interceptar emisiones electromagnéticas provenientes de un sistema informático", esto implica la captación de señales inalámbricas que transportan datos, como redes Wi-Fi, comunicaciones Bluetooth o señales satelitales.

El objeto de la acción son los datos informáticos y las emisiones electromagnéticas que los transportan, lo que amplía la protección penal más allá de los archivos almacenados, incluyendo comunicaciones en tiempo real y señales

digitales transmitidas de forma inalámbrica. La modalidad de comisión exige que la interceptación se realice sin orden judicial previa, lo que introduce un elemento normativo que requiere verificar si la acción fue realizada sin el respaldo judicial correspondiente, un claro ejemplo de esto fue el famoso caso conocido como el “Escándalo de las chuzadas del DAS”.

El resultado del delito no exige un daño concreto, ya que se sanciona la mera interceptación de los datos, lo que lo convierte en un delito de mera conducta. No es necesario que el atacante use la información interceptada o la difunda para que la conducta sea punible.En cuanto a la culpabilidad, el delito requiere dolo, es decir, que el sujeto conozca y tenga la intención de interceptar los datos sin autorización. No se contempla la modalidad culposa, lo que excluye situaciones en las que una interceptación ocurre de manera accidental o por fallos técnicos.

Uno de los principales problemas es la falta de diferenciación entre interceptación y acceso no autorizado. El artículo no establece una clara distinción entre interceptar datos y acceder indebidamente a un sistema informático, lo que puede generar confusión en la aplicación del delito. No queda claro si la conducta debe sancionarse bajo el artículo 269A (acceso abusivo a un sistema informático) o el artículo 269C (interceptación de datos informáticos) – un hacker que accede a un servidor y copia correos electrónicos sin autorización, ¿comete acceso abusivo o interceptación de datos? –, es cierto que bajo principios del Derecho Penal se podría llegar eventualmente a una conclusión al respecto, sin embargo, en estos casos de delitos informáticos, es bueno preguntarse hasta qué punto debemos emplear dichos principios.

La omisión de la modalidad culposa también representa un vacío normativo. El delito solo contempla la comisión dolosa, es decir, requiere que el sujeto tenga la intención de interceptar datos sin autorización. Sin embargo, no se sanciona la interceptación culposa, lo que deja sin cobertura ciertos escenarios. Si una persona configura incorrectamente un sistema de monitoreo y, sin intención, capta datos de terceros, la conducta no sería punible. Un administrador de red que, por error,

almacena datos de empleados sin su conocimiento, ¿queda exento de responsabilidad penal?

CONCLUSIÓN

El intrusismo informático es una problemática creciente en el mundo digitalizado, y su regulación en Colombia ha representado un avance significativo en la protección de la seguridad informática. Sin embargo, persisten desafíos en la interpretación y aplicación de las normas, lo que subraya la necesidad de una revisión legislativa para evitar lagunas jurídicas y garantizar un equilibrio adecuado entre la protección de los sistemas y el respeto a los derechos digitales de los ciudadanos.

CAPÍTULO III: DESAFÍOS CONTEMPORÁNEOS DE LA CIBERCRIMINALIDAD

INTRODUCCIÓN

El fenómeno del sabotaje y el intrusismo informático, especialmente a través del uso de software malicioso, representa uno de los mayores desafíos jurídicos y técnicos en el contexto de la cibercriminalidad contemporánea. El presente capítulo analiza cómo estas prácticas, que comprometen la integridad, confidencialidad y disponibilidad de los sistemas informáticos, han evolucionado hasta convertirse en amenazas de alto impacto para individuos, empresas y entidades públicas. A partir de un enfoque técnico-jurídico, se revisa el comportamiento del malware como agente infeccioso digital y se evidencia la necesidad urgente de que la legislación colombiana responda con mayor precisión frente a estas conductas. Aunque la Ley 1273 de 2009 representó un avance importante al introducir el artículo 269E al Código Penal, aún persisten vacíos normativos, ambigüedades terminológicas y dificultades interpretativas que afectan la eficacia de su aplicación. Esta sección se centra, por tanto, en descomponer los elementos estructurales del tipo penal, evaluar su alcance frente a nuevas realidades tecnológicas y destacar las tensiones que surgen entre la protección jurídica y el desarrollo de actividades legítimas en el ámbito de la ciberseguridad. La tipificación del uso de software malicioso será

analizada en detalle como punto de confluencia entre el sabotaje y el intrusismo, en un intento de comprender la complejidad normativa que representa.

SABOTAJE E INTRUSISMO INFORMÁTICO: SOFTWARE MALICIOSO

Desde el punto de vista técnico, el malware es un tipo de programa creado con la intención de dañar, alterar o interferir con el funcionamiento normal de un sistema informático. Este tipo de software puede robar información, bloquear el acceso a archivos, borrar datos o incluso permitir que otras personas accedan sin permiso a un sistema. Según el modelo epidemiológico MalSEIRS propuesto por Calderón Acero et al. (2022), los virus informáticos se comportan de forma similar a los virus biológicos, ya que pueden expandirse rápidamente en redes informáticas y causar daños masivos. Este enfoque ayuda a comprender el riesgo que representa el malware para los sistemas digitales y la necesidad urgente de que la legislación penal lo regule de forma eficaz.

Por otro lado, estudios comparativos sobre los delitos informáticos en Colombia han resaltado que, aunque el marco legal ha avanzado con normas como la Ley 1273 de 2009, aún existen desafíos importantes en la precisión y aplicación de tipos penales relacionados con el software malicioso. Bolaño y Tarriba (s.f) señalan que uno de los mayores obstáculos para aplicar efectivamente el tipo penal es la dificultad para definir y probar el carácter "malintencionado" del software involucrado. Esta ambigüedad puede generar inseguridad jurídica y disparidad en las decisiones judiciales.

Asimismo, Castañeda et al. (2021) advierten que, en Colombia, a pesar del reconocimiento normativo del delito, la legislación enfrenta problemas de actualización frente a nuevas modalidades de ataques digitales y herramientas tecnológicas. Ello implica que muchos casos de uso o distribución de malware no se encuadran fácilmente en la descripción típica del artículo 269E, lo que puede llevar a una subutilización del tipo penal o a interpretaciones judiciales restrictivas. Es necesario interpretar el artículo teniendo en cuenta tanto los avances

tecnológicos como los principios básicos del derecho penal, para que la protección de la información digital sea efectiva y acorde con los desafíos actuales.

Después de analizar de manera separada los delitos de intrusismo y sabotaje informático, es necesario destacar que el artículo 269E del Código Penal colombiano representa una especie de culminación normativa que articula ambos fenómenos. Mientras que el intrusismo sanciona el acceso indebido a sistemas y el sabotaje penaliza la afectación de su operatividad, el uso de software malicioso integra ambas conductas en un mismo esquema delictivo: permite el ingreso no autorizado y, al mismo tiempo, facilita la alteración o daño de los sistemas informáticos. De esta forma, el legislador reconoce que las herramientas tecnológicas no solo son medios de intrusión, sino también de destrucción, y responde a esta nueva dinámica criminal mediante una tipificación que cubre de manera integral las amenazas más complejas del entorno digital.

ARTÍCULO 269E

El Código Penal Colombiano (Congreso de la República, 2000) contempla en el Artículo 269E el delito de uso de software malintencionado, introducido mediante la Ley 1273 de 2009 (Congreso de la República, 2009) como parte de la estrategia normativa para enfrentar las nuevas amenazas que surgieron con el auge de la cibercriminalidad. Esta figura penal sanciona a quienes, sin autorización, intervienen en la creación, comercialización o distribución de programas informáticos diseñados para causar daño, comprometiendo así la integridad, disponibilidad o confidencialidad de los sistemas informáticos. El texto del artículo dispone lo siguiente:

> *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 mensuales vigentes.* (Congreso de la República, 2000)

Esta disposición busca combatir la propagación de herramientas diseñadas para afectar infraestructuras digitales, proteger la seguridad de la información, y frenar la expansión de fenómenos como el malware, el ransomware y otros ataques automatizados que ponen en riesgo a individuos, empresas y entidades públicas.

El sujeto activo de la conducta es "el que", enunciación que identifica a este delito como común, permitiendo que cualquier individuo, independientemente de su nivel de especialización técnica, pueda ser sujeto de imputación penal. Esto abarca desarrolladores de software, intermediarios comerciales y usuarios que gestionen software malicioso. El sujeto pasivo se extiende a la colectividad en su conjunto, protegiéndose la seguridad y la integridad de los sistemas informáticos, así como de los datos que en ellos residen o transitan, incluyendo infraestructuras críticas tanto de entidades privadas como públicas.

La acción típica comprende una diversidad de conductas, expresadas en los verbos rectores "producir", "traficar", "adquirir", "distribuir", "vender", "enviar", "introducir" y "extraer" software malicioso, abarcando toda la cadena de generación y propagación del malware. "Producir" involucra el diseño, programación o desarrollo de software con intención de causar perjuicio; "traficar" implica su comercialización o transacción; "adquirir" refiere a la obtención de estos programas; "distribuir" se entiende como la diseminación a terceros; "vender" como su transferencia onerosa; "enviar" como su transmisión a través de canales digitales, y "introducir o extraer" como las actividades de importación o exportación, respectivamente, dotando al tipo penal de una dimensión transnacional.

El objeto material de la conducta es el software malicioso o cualquier otro programa informático que, por su diseño o uso, comprometa la integridad, disponibilidad o confidencialidad de los sistemas. La modalidad de comisión exige la ausencia de facultad o autorización legítima, excluyéndose, por ende, aquellas actuaciones amparadas por funciones legales, tales como las pruebas de penetración autorizadas. El objeto material de la conducta es el software malicioso o cualquier otro programa informático que, por su diseño o uso, comprometa la

integridad, disponibilidad o confidencialidad de los sistemas. La modalidad de comisión exige la ausencia de facultad o autorización legítima, excluyéndose, por ende, aquellas actuaciones amparadas por funciones legales, tales como las pruebas de penetración autorizadas.

Se trata de un delito de mera conducta, en tanto no se requiere la producción de un resultado material de daño efectivo para su configuración. Desde el punto de vista subjetivo, exige dolo, en su modalidad directa o eventual, y excluye la posibilidad de su comisión por imprudencia o negligencia. Uno de los principales vacíos radica en la ambigüedad terminológica respecto a "software malicioso" y "programas de efectos dañinos", conceptos que no son definidos por la legislación penal, generando incertidumbre sobre su alcance. Este problema hermenéutico puede derivar en la tipificación extensiva de herramientas informáticas que, si bien pueden ser utilizadas para actos ilícitos, también poseen aplicaciones lícitas en ciberseguridad, como las herramientas de pentesting. Asimismo, el tipo penal omite diferenciar entre finalidades lícitas e ilícitas de las conductas típicas. Ello puede conllevar a sancionar a profesionales de la ciberseguridad que manejan software malicioso bajo contextos de evaluación y fortalecimiento de sistemas informáticos.

Otro problema significativo es la omisión de la modalidad culposa. Al exigir exclusivamente dolo, se excluyen de la sanción supuestos en los que, por negligencia o impericia, se produzca o distribuya software que cause graves afectaciones a la seguridad informática; para ejemplificar lo anterior propongo el siguiente ejemplo:

Supóngase un ingeniero en sistemas que, en el marco de su actividad profesional, desarrolla una aplicación destinada a gestionar comunicaciones internas en una organización empresarial. En el proceso de diseño e implementación del software, el programador omite, de manera negligente, la incorporación de medidas elementales de ciberseguridad, tales como protocolos de cifrado de datos o sistemas de autenticación robusta, pese a que, por su formación y experiencia, tenía la capacidad técnica para prever tales riesgos. A consecuencia

de dicha omisión, un tercero malintencionado logra explotar las vulnerabilidades del programa y propaga a través de la aplicación un malware que compromete la confidencialidad y disponibilidad de la información crítica de la empresa. Si bien el ingeniero no actuó con dolo —pues su propósito no era permitir o facilitar un ataque informático— su actuar imprudente creó un riesgo jurídicamente desaprobado que se concretó en un daño efectivo a sistemas informáticos protegidos.

Desde una perspectiva de política criminal, este supuesto ilustra la laguna punitiva que surge de la omisión de la modalidad culposa en el artículo 269E. La estricta exigencia de dolo impide sancionar conductas gravemente negligentes que, sin constituir manifestaciones de voluntad dolosa, lesionan bienes jurídicos de elevada importancia en el ámbito de la ciberseguridad. Tal vacío normativo debilita el principio de protección efectiva y exige reconsiderar la estructura típica del delito, incorporando la responsabilidad penal culposa para supuestos de imprudencia grave que comprometan la integridad de los sistemas informáticos.

La proporcionalidad en la respuesta penal también se ve comprometida, ya que el tipo sanciona de manera homogénea conductas que presentan grados de lesividad y peligrosidad manifiestamente distintos. Igualar penalmente al mero adquirente ocasional de malware y al productor de ciberarmas de alta sofisticación atenta contra principios fundamentales del derecho penal moderno.

Finalmente, el tipo adolece de una falta de adaptación a las nuevas manifestaciones tecnológicas del software malicioso, como los desarrollos basados en inteligencia artificial, deepfakes maliciosos y ataques automatizados mediante algoritmos de aprendizaje automático, quedando desfasado respecto de las técnicas contemporáneas de ataque digital.

GUSANOS Y VIRUS INFORMÁTICOS

Los virus y gusanos informáticos representan dos de las formas más comunes y peligrosas de malware, y su comprensión resulta clave para el análisis jurídico del uso de software malicioso. Un virus informático es un programa diseñado

para replicarse insertándose en otros programas legítimos, de modo que se activa al ejecutarse el archivo huésped. Por ejemplo, puede adherirse a una hoja de cálculo, ejecutándose al mismo tiempo que esta, y reproduciéndose al infectar nuevos archivos del sistema. Su presencia suele pasar inadvertida hasta que genera daños concretos, como la pérdida de información, la corrupción de archivos, la ralentización del sistema o la caída de servicios esenciales (Jaiswal, 2017). Además, muchos virus están diseñados con temporizadores o condiciones específicas que activan su carga maliciosa, lo que dificulta aún más su detección temprana (Jaiswal, 2017).

Por su parte, un gusano es una pieza de software autónomo que se autorreplica utilizando redes y vulnerabilidades de seguridad para propagarse de un equipo a otro sin necesidad de intervención humana. A diferencia del virus, no requiere alojarse en un archivo anfitrión ni interacción del usuario para iniciar su actividad, lo que le permite expandirse con gran rapidez por entornos conectados (Jaiswal, 2017). Este comportamiento ha llevado a que algunos gusanos causen interrupciones masivas en redes corporativas, gubernamentales y personales. De hecho, algunos de los ataques cibernéticos más destructivos de las últimas décadas, como el gusano "WannaCry", se han originado por este tipo de malware. Además, Jaiswal (2017) subraya que tanto virus como gusanos pueden diseñarse para ocultarse del software antivirus tradicional, lo cual aumenta su peligrosidad y dificulta su contención o eliminación oportuna.

Tanto virus como gusanos tienen la capacidad de comprometer seriamente la seguridad informática, alterar la disponibilidad de la información, vulnerar la privacidad y generar pérdidas económicas y reputacionales significativas. Desde una perspectiva jurídica, su relevancia es evidente, ya que son herramientas clave empleadas en conductas que pueden configurar delitos como sabotaje, acceso abusivo o daño informático, y, particularmente, en la producción, distribución o utilización de software malicioso como lo prevé el artículo 269E del Código Penal colombiano.

ATAQUE A XZ UTILS COMO ANTECEDENTE

El ataque a XZ Utils ha sido uno de los incidentes más sofisticados de los últimos años en materia de ciberseguridad, particularmente en el ámbito del software libre. Este caso evidencia cómo una pieza aparentemente secundaria del sistema —la utilidad de compresión XZ Utils— puede convertirse en el vector de una amenaza de gran alcance, capaz de comprometer miles de servidores y dispositivos a nivel global.

Este ataque se llevó a cabo mediante una cuidadosa infiltración en el ecosistema de desarrollo del proyecto. Como explican Przymus y Durieux (2025), el atacante fue integrándose de forma progresiva en la comunidad de desarrollo desde 2021, ganando la confianza de los mantenedores y asumiendo progresivamente tareas de traducción, documentación y mantenimiento. Esta estrategia de largo plazo permitió que, en 2024, el atacante introdujera una puerta trasera en las versiones 5.6.0 y 5.6.1 del paquete, sin que el código malicioso estuviera visible en el repositorio principal. La vulnerabilidad permitía la ejecución remota de comandos y la omisión del proceso de autenticación en servicios SSH, comprometiendo la seguridad de cualquier sistema Linux que lo utilizara (Przymus & Durieux, 2025).

El descubrimiento fue posible gracias a la pericia de Andrés Freund, ingeniero de Microsoft, quien detectó anomalías en el comportamiento de su sistema tras una actualización aparentemente rutinaria. Freund notó un retardo anómalo en el proceso SSH, lo cual lo llevó a una investigación más profunda que reveló un uso inusual de recursos por parte del servicio sshd. Siguiendo el rastro hasta la librería liblzma, encontró allí el código de la puerta trasera (Gentile, 2024).

Lo que hace este caso especialmente alarmante es que la manipulación no se limitó al código fuente. El atacante modificó el proceso de compilación del software para introducir el código malicioso únicamente en los paquetes distribuidos públicamente, manteniendo limpio el repositorio visible para desarrolladores. Esta táctica dificultó su detección y refleja un conocimiento profundo del funcionamiento

del software libre y de las herramientas de construcción utilizadas por las distribuciones de Linux (Gentile, 2024; Przymus & Durieux, 2025).

El ataque pone de manifiesto la vulnerabilidad de proyectos críticos mantenidos por individuos o pequeños equipos, así como la necesidad de implementar medidas más rigurosas de verificación en los ciclos de desarrollo de software libre. Como lo señalan los investigadores, esta intrusión representa una nueva generación de amenazas a la cadena de suministro digital, donde los atacantes no solo manipulan el código, sino también las prácticas comunitarias y los procesos de desarrollo (Przymus & Durieux, 2025).

ESTRATEGIAS DE MEJORAMIENTO

El contexto colombiano presenta desafíos particulares frente a los delitos informáticos, lo cual exige estrategias de mejoramiento que reconozcan tanto sus limitaciones estructurales como su incipiente capacidad institucional para responder a amenazas sofisticadas como el uso de software malicioso. Aunque aún no se han registrado ataques de gran escala como el ocurrido con XZ Utils a nivel internacional, esto no significa que el país esté exento de estos riesgos, sino que el atraso tecnológico y la falta de infraestructura adecuada generan una falsa sensación de seguridad.

En primer lugar, se requiere una actualización normativa que permita identificar y sancionar de forma efectiva las nuevas formas de cibercriminalidad. Según Parra (2024), la Ley 1273 ha sido efectiva en algunos aspectos, pero presenta vacíos frente a amenazas contemporáneas como el ransomware, el espionaje digital y la manipulación de sistemas críticos. La reforma debería incluir una mayor precisión en los tipos penales relacionados con el uso de software malicioso, garantizando que figuras como los "gusanos" o "troyanos" tengan una sanción clara y diferenciada, alineada con su capacidad destructiva y propagación autónoma.

En segundo lugar, se necesita una estrategia nacional de fortalecimiento institucional, que implique formación especializada para jueces, fiscales y cuerpos técnicos de investigación en delitos informáticos. Como lo destaca el estudio de Parra (2024), muchas investigaciones se ven obstaculizadas por el desconocimiento técnico de los operadores judiciales o por la falta de pruebas electrónicas debidamente recolectadas. En este sentido, es fundamental implementar protocolos estandarizados para la recolección y análisis forense de evidencia digital, así como fomentar la cooperación interinstitucional y con el sector privado.

Asimismo, resulta crucial articular mecanismos de colaboración internacional. Pese a que Colombia ha ratificado el Convenio de Budapest, su implementación efectiva aún es incipiente. La experiencia comparada muestra que el combate al cibercrimen exige cooperación transnacional para rastrear operaciones distribuidas a través de múltiples jurisdicciones. Tal como señala Parra (2024), Colombia debe avanzar en su integración a redes internacionales de ciberseguridad y fortalecer los canales de intercambio de información con agencias como INTERPOL, Europol y la OEA.

Finalmente, se propone el desarrollo de una política pública de prevención y alfabetización digital. Si bien se ha mejorado la cobertura tecnológica en el país, el uso responsable y seguro de los sistemas informáticos sigue siendo una tarea pendiente. Es imprescindible que el Estado impulse campañas de concienciación sobre el uso de contraseñas seguras, la actualización de sistemas, el reconocimiento de fraudes comunes, y la denuncia de delitos informáticos. La investigación de Parra (2024) advierte que la ciudadanía aún desconoce los mecanismos de protección disponibles y tiende a no denunciar estos hechos, lo que alimenta la impunidad.

Colombia necesita un enfoque integral que combine reformas legislativas, fortalecimiento institucional, cooperación internacional y cultura ciudadana para afrontar de forma efectiva los desafíos que plantea el uso de software malicioso y,

en general, la criminalidad informática. Aunque el país aún no enfrenta escenarios como el de XZ Utils, prepararse desde ya es indispensable para evitar consecuencias futuras de gran escala.

CONCLUSIÓN

El análisis del delito de uso de software malicioso revela importantes tensiones entre la necesidad de proteger eficazmente los sistemas informáticos y los límites que impone el derecho penal moderno. El artículo 269E del Código Penal colombiano, aunque introducido como respuesta al auge del cibercrimen, presenta deficiencias significativas en su redacción y aplicación, como la falta de definición de términos clave, la omisión de la modalidad culposa y la escasa diferenciación entre conductas de diversa gravedad. Estas falencias generan riesgos de criminalización excesiva, afectando incluso a profesionales que actúan dentro de marcos legales, como los expertos en seguridad informática.

Asimismo, la homogeneidad en la sanción penal no respeta los principios de proporcionalidad ni de mínima intervención. Por ello, se hace necesario replantear la estructura de este tipo penal, incorporando mecanismos que permitan una persecución más justa y efectiva de las conductas verdaderamente lesivas, sin obstaculizar el desarrollo técnico ni vulnerar garantías fundamentales. El software malicioso, como herramienta de ataque digital, debe ser abordado no solo desde su capacidad destructiva, sino también desde su compleja inserción en un ecosistema tecnológico en constante evolución.

CONCLUSIONES

A partir del análisis realizado, se evidencia que la aplicación efectiva de la Ley 1273 de 2009 enfrenta limitaciones estructurales que deben ser superadas mediante un enfoque integral. En primer lugar, uno de los mayores obstáculos radica en la falta de formación técnica por parte de los operadores jurídicos encargados de investigar y juzgar los delitos informáticos. Muchos fiscales y jueces no cuentan con los conocimientos necesarios para comprender la lógica técnica que subyace a

estas conductas, lo cual genera errores en la tipificación, deficiencias probatorias y, en consecuencia, altos índices de impunidad. Por ello, resulta fundamental implementar programas de formación continua y crear unidades especializadas en delitos informáticos dentro del aparato judicial, integradas por profesionales del derecho y expertos en tecnologías de la información.

Ahora bien, esta carencia técnica no es el único desafío. La segunda conclusión relevante es que la Ley 1273, si bien fue pionera en su momento, hoy resulta insuficiente frente a las dinámicas actuales del cibercrimen. Su enfoque limitado al sabotaje, al intrusismo y al daño informático deja por fuera nuevas manifestaciones delictivas como el ciberacoso, la suplantación digital o el uso de software malicioso con capacidades autónomas. Este desfase normativo no solo limita la respuesta del Estado, sino que también genera incertidumbre jurídica y obstaculiza la aplicación del principio de legalidad. Se requiere, en consecuencia, una reforma legislativa que redefina los tipos penales informáticos incorpore nuevas figuras delictivas y contemple los bienes jurídicos emergentes propios del entorno digital.

A lo anterior se suma que, si bien la Ley 1273 contempla penas importantes, estas no han logrado un efecto disuasivo, en gran parte por la baja tasa de judicialización y condenas efectivas. Esta tercera conclusión pone de relieve la necesidad de reforzar la capacidad operativa del Estado mediante mayor inversión en infraestructura tecnológica, herramientas de análisis forense digital, y mecanismos de articulación entre las autoridades judiciales, la Policía Nacional y las entidades privadas. De lo contrario, las sanciones previstas seguirán siendo meramente simbólicas y la percepción de impunidad persistirá.

En ese mismo sentido, no basta con actualizar el marco legal ni con mejorar las capacidades institucionales: también se requiere una política pública de prevención y educación digital que prepare a la ciudadanía frente a los riesgos del entorno virtual. Esta cuarta conclusión resalta la importancia de promover una cultura de la ciberseguridad desde el sistema educativo, fomentar el uso

responsable de la tecnología y garantizar el acceso a información clara sobre cómo prevenir, detectar y denunciar conductas informáticas delictivas. Solo a través de la formación ciudadana se podrá fortalecer la resiliencia social frente a estos fenómenos.

Por último, la naturaleza transnacional de muchos delitos informáticos obliga a Colombia a adoptar una visión estratégica en materia de cooperación internacional. Esta quinta y última conclusión enfatiza que el país debe avanzar no solo en la ratificación y aplicación efectiva de tratados como el Convenio de Budapest, sino también en la integración a redes globales de ciberinteligencia, coordinación judicial y asistencia técnica. La prevención y persecución del uso de software malicioso, el ransomware o los ataques a infraestructuras críticas no pueden depender exclusivamente de esfuerzos internos, sino de una articulación sólida con organismos multilaterales y otros Estados.

En suma, la mejora del marco normativo colombiano frente a los delitos informáticos requiere mucho más que reformas legislativas aisladas: implica un rediseño profundo del modelo institucional, educativo y cooperativo con el que el Estado enfrenta las amenazas del mundo digital. Estas conclusiones, entrelazadas, ofrecen una hoja de ruta que puede guiar tanto la política pública como la discusión académica y legislativa sobre el futuro del derecho penal informático en Colombia.

REFERENCIAS

1. Acuerdo PCSJA24-12185. (2024, mayo 27). Consejo Superior de la Judicatura. https://actosadministrativos.ramajudicial.gov.co/GetFile.ashx?url=~%2FApp_Data%2FUpload%2FPCSJA24-12185.pdf
2. Barranco, M. C. G. (2021). Sabotaje informático a infraestructuras críticas: Análisis de la realidad criminal recogida en los artículos 264 y 264 bis del Código Penal. Especial referencia a su comisión con finalidad terrorista. Revista de Derecho Penal y Criminología, (25), 77-124.

3. Bolaño, I. M., & Tarriba, F. J. (s.f.). Caracterización de los delitos informáticos en Colombia. Characterization of cybercrime in Colombia.
4. Castañeda, R. R. E., Ramírez, H. H. F., & Lorzo, E. M. C. (2021). Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado. Ius Comitiãlis, 4(8), 252–276.
5. Conde O'Donnell, H., González P., C., & Heredia M., A. (2009). El delito informático. Consultado en: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf
6. Corte Suprema de Justicia, Sala de Casación Penal. (2011, septiembre 13). Auto Interlocutorio Penal, Rad. 37.145 [MP. Fernando Alberto Castro Caballero]. URL no disponible.
7. Corte Suprema de Justicia, Sala de Casación Penal. (2012, agosto 14). Sentencia SP39160-2012, Rad. 39160 [MP. Julio Enrique Socha Salamanca]. https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1sep2012/39160(14-08-12).doc.
8. Corte Suprema de Justicia, Sala de Casación Penal. (2015, febrero 11). Sentencia SP1245-2015, Rad. 42724 [MP. Eyder Patiño Cabrera]. https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015(42724).doc.
9. Corte Suprema de Justicia, Sala de Casación Penal. (2016, octubre 5). Sentencia SP 14302-2016, Rad. 41517 [MP. Luis Guillermo Salazar Otero]. URL no disponible.
10. Corte Suprema de Justicia, Sala de Casación Penal. (2022, agosto 3). Sentencia SP2699-2022, Rad. 59733 [MP. Fernando León Bolaños Palacios]. https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1ago2022/SP2699-2022(59733).pdf.
11. Corte Suprema de Justicia, Sala de Casación Penal. (2023, noviembre 11). Sentencia SP473-2023, Rad. 57922 [MP. Diego Eugenio Corredor].

https://cortesuprema.gov.co/corte/wp-content/uploads/2023/12/SP475-2023.pdf.

12. Corte Suprema de Justicia, Sala de Casación Penal. (2023, noviembre 22). Sentencia SP479-2023, Rad. 59538 [MP. Myriam Ávila Roldán]. URL no disponible.
13. Corte Suprema de Justicia, Sala de Casación Penal. (2024, abril 24). Sentencia SP903-2024, Rad. 65376 [MP. Myriam Ávila Roldán]. https://cortesuprema.gov.co/wp-content/uploads/2024/06/SP903-202465376.pdf.
14. Cuenca Espinoza, A. (2013). El delito informático en el Ecuador. Revista Ruptura, (56), 220.
15. Gentile, N. (2024, junio 2). El Hackeo que casi INFECTA al MUNDO ENTERO | La puerta trasera de xzutils [Video]. YouTube. https://www.youtube.com/watch?v=mTpDmhF4BSw
16. Gutiérrez Francés, M. L. (1996). El intrusismo informático (Hacking): ¿Represión Penal Autónoma?. Informática y derecho: Revista iberoamericana de derecho informático, (12), 1163-1184.
17. Herrera, S. M. (2018). Sabotaje informático: La exigencia de daño grave como elemento del injusto. Revista Jurídica del Ministerio Público, 72, 143-171.
18. Jaiswal, M. (2017). *Computer Viruses: Principles of Exertion, Occurrence and Awareness*. International Journal of Creative Research Thoughts (IJCRT), 5(4), 648–651.
19. Leiva Jijena, R. (1992). Chile, la protección penal de la intimidad y el delito informático. Chile: Editorial Andrés Bello, p. 225.
20. Ley 1090 de 2006. (2006, septiembre 6). Congreso de la República. Diario oficial No. 46.383. http://www.secretariasenado.gov.co/senado/basedoc/ley_1090_2006.html
21. Ley 1150 de 2007. (2007, julio 16). Congreso de la República. Diario oficial No. 46.691. https://www.suin-juriscol.gov.co/viewDocument.asp?id=1674903

22. Ley 1273 de 2009. (2009, enero 5). Congreso de la República. Diario oficial No. 47.223. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699
23. Ley 2213 de 2022. (2022, junio 13). Congreso de la República. Diario oficial No. 52.064. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30044248
24. Ley 527 de 1999. (1999, agosto 21). Congreso de la República. Diario oficial No. 43.673. https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013
25. Ley 599 de 2000. (2000, julio 24). Congreso de la República. Diario oficial No. 44.097. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1663230
26. Ley 962 de 2005. (2005, septiembre 6). Congreso de la República. Diario oficial No. 46.023. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1671809
27. Martínez Martínez, I., Florián, A. F., Díaz López, D. O., & Calderón Acero, C. A. (2022). MalSEIRS. Un modelo epidemiológico para predecir el comportamiento de virus informáticos.
28. Parra, J. (2024). Determinar la eficacia de la Ley 1273, entre el año 2010 – 2022 en el departamento de Risaralda. Universidad Cooperativa de Colombia, Facultad de Derecho, Derecho, Cartago. Disponible en: https://hdl.handle.net/20.500.12494/56751
29. Posada Maya, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Revista Nuevo Foro Penal, 13(88), 72-112. Universidad EAFIT.
30. Przymus, P., & Durieux, T. (2025). Wolves in the Repository: A Software Engineering Analysis of the XZ Utils Supply Chain Attack. arXiv preprint arXiv:2504.17473.
31. Satzger, H., Morón Lerma, E., Miró Llinares, F., Gutiérrez Francés, M. L., Balmaceda Hoyos, G., Posada Maya, R., Picotti, L., Ambos, K., Jiménez, J.

D., & Velásquez Velásquez, F. (2016). Derecho Penal y Nuevas Tecnologías. A propósito del Título VII Bis del Código Penal. Universidad Sergio Arboleda.

32. Turégano, M. A. C. (2016). El delito de intrusismo informático tras la reforma del CP español de 2015. Revista Boliviana de Derecho, (21), 210-229.