EL DELITO DE ACCESO ABUSIVO A SISTEMA INFORMÁTICO EN COLOMBIA: UN ANÁLISIS SOBRE SUS ELEMENTOS

VALENTINA ALEJANDRA SOLANO CASTELLANOS

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
ESPECIALIZACIÓN EN DERECHO PENAL Y SISTEMA PENAL ACUSATORIO
VILLAVICENCIO
2023

EL DELITO DE ACCESO ABUSIVO A SISTEMA INFORMÁTICO EN COLOMBIA: UN ANÁLISIS SOBRE SUS ELEMENTOS

VALENTINA ALEJANDRA SOLANO CASTELLANOS

Trabajo de grado presentado como requisito para obtener el título de especialista en Derecho penal y sistema penal acusatorio

Asesor
Mg. JULIAN LEONARDO RIVEROS CRUZ
Abogado
Especialista en Derecho Penal
Magister en Justicia Criminal

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE DERECHO
ESPECIALIZACIÓN EN DERECHO PENAL Y SISTEMA PENAL ACUSATORIO
VILLAVICENCIO
2023

Autoridades Académicas

P. José Gabriel MESA ANGULO, O. P. Rector General

P. Eduardo GONZÁLEZ GIL, O. P.
Vicerrector Académico General

P. José Antonio BALAGUERA CEPEDA O.P.
Rector Sede Villavicencio

P. Rodrigo GARCÍA JARA, O.P.
Vicerrector Académico Sede Villavicencio

Adm. JULIETH ANDREA SIERRA TOBÓN
Secretaria de División Sede Villavicencio

PhD. RODRÍGO CORTÉS BORRERO
Decano Facultad de Derecho

El delito de acceso abusivo a sistema informático en Colombia: un análisis sobre sus elementos

Valentina Alejandra Solano Castellanos

Julián Leonardo Riveros Cruz (Dir)[***]

Resumen

La globalización ha generado una dependencia cada vez mayor de sistemas y redes informáticas en diversos sectores, como finanzas, salud, gobierno y comercio. Con el flujo constante de información y datos a través de estos canales digitales, también se intensifica el riesgo de ciberataques que buscan acceder ilícitamente a sistemas y comprometer la seguridad de la información. Las consecuencias pueden ser graves, desde la pérdida de datos hasta el robo de información confidencial, la interrupción de servicios críticos y daños a la reputación.

En este sentido, proteger la información y los datos ha adquirido un papel vital a nivel global, siendo un tema central en legislaciones y jurisprudencias. La promulgación de leyes relacionadas con la privacidad, ciberseguridad y propiedad intelectual desempeña un rol fundamental en preservar estos activos digitales.

El artículo 269A del Código Penal, mencionado en el texto, trata sobre el acceso abusivo a sistemas informáticos y refleja cómo los sistemas legales se están adaptando para enfrentar los desafíos de los ciberataques. Esta disposición legal tiene como objetivo sancionar y prevenir el acceso no autorizado a sistemas, independientemente de si el propósito es robar información, causar daños u otras actividades maliciosas. Esto subraya la necesidad de definir y abordar específicamente los delitos informáticos en el marco legal.

Palabras clave: Ciberataque, daños, información, globalización y sistemas informáticos.

[***] Asesor Articulo, Abogado Cum Laude USTA Seccional Villavicencio, Especialista en Derecho Penal USTA Bogotá; Máster en Justicia Criminal y Doctorando en Derecho Universidad Carlos III de Madrid. CVLAC: https://scienti.minciencias.gov.co/cvlac/visualizador/generarCurriculoCv.do?cod_rh=0000141243; Google sholar: https://scholar.google.com/citations?hl=es&authuser=1&user=_zUBfAcAAAAJ; ORCID: https://orcid.org/0000-0002-4890-7539

Abstract

Globalization has generated an increasing dependence on systems and computer networks in various sectors such as finance, healthcare, government, and commerce. With the constant flow of information and data through these digital channels, the risk of cyberattacks that aim to illicitly access systems and compromise the security of information also intensifies. The consequences can be severe, ranging from data loss to the theft of confidential information, disruption of critical services, and damage to reputation.

In this context, safeguarding information and data has taken on a vital role globally, becoming a central theme in legislation and jurisprudence. The enactment of laws related to privacy, cybersecurity, and intellectual property plays a fundamental role in preserving these digital assets.

Article 269A of the Penal Code, as mentioned in the text, deals with abusive access to computer systems and reflects how legal systems are adapting to address the challenges posed by cyberattacks. This legal provision aims to sanction and prevent unauthorized access to systems, regardless of whether the purpose is to steal information, cause damage, or engage in other malicious activities. This underscores the need to define and specifically address cybercrime within the legal framework.

Keywords: Cyberattack, damages, information, globalization, and computer systems.

Introducción

El texto aborda una temática altamente relevante en el contexto contemporáneo, que gira en torno a la interconexión entre la globalización, el ciberespacio y las cuestiones vinculadas a los ciberataques. En un mundo cada vez más digitalmente interrelacionado, el ciberespacio ha emergido como un nuevo escenario donde convergen diversas problemáticas y desafíos. Uno de estos desafíos de gran magnitud se refiere a la salvaguardia de la información y los datos en este entorno digital, los cuales han adquirido una importancia de proporciones exponenciales en la actual era digital.

La globalización ha propiciado una creciente dependencia de sistemas y redes informáticas en el funcionamiento de diversas esferas de la sociedad, abarcando desde ámbitos financieros y de salud hasta gubernamentales y comerciales. A medida que la información y los datos fluyen a través de estos canales digitales, se acrecienta también el riesgo de ciberataques, los cuales tienen como objetivo el acceso ilícito a sistemas con la intención de comprometer la seguridad de la información. Las consecuencias de estos ataques pueden ser gravísimas, desde la pérdida de datos hasta el robo de información confidencial, la interrupción de servicios esenciales y la mella en la reputación de las entidades afectadas.

En este contexto, la protección de la información y los datos ha emergido como un tema de enorme trascendencia a nivel global, situándose en el epicentro de legislaciones y jurisprudenciales en todo el mundo. La promulgación de leyes que abarcan la privacidad, la ciberseguridad y la propiedad intelectual desempeña un papel central en la salvaguardia de estos activos digitales.

El artículo 269A del Código Penal, mencionado en el texto, y que se refiere al acceso abusivo a un sistema informático, refleja claramente cómo los sistemas legales están evolucionando para abordar los ciberataques y sus implicaciones. Esta disposición legal busca sancionar y prevenir el acceso no autorizado a sistemas informáticos, independientemente de si la intención es el robo de información, la causación de daños o la realización de otras actividades maliciosas. Esta norma pone de manifiesto la necesidad imperante de definir y afrontar de manera específica los delitos informáticos en el marco legal.

En síntesis, el texto arroja luz sobre la vital importancia de la protección de la información y los datos en un contexto donde la globalización y la digitalización están estrechamente entrelazadas. Asimismo, subraya cómo los sistemas legales están respondiendo a esta nueva realidad, estableciendo marcos normativos y jurídicos que no solo aborden los desafíos actuales, sino que también allanen el camino para una era digital segura y confiable.

1. Precisiones conceptuales y contextuales sobre el tipo penal del artículo 269A

Para comprender el desarrollo del presente texto, es fundamental precisar conceptos enunciados en el artículo 269A del Código Penal, el cual corresponde al injusto de acceso abusivo a un sistema informático, en aras de comprender su funcionamiento y división para identificar qué se abarca en el delito previamente mencionado.

1.1. Sistema informático

El concepto de sistema informático es relativamente novedoso, pues ha tenido lugar con posterioridad al siglo XX; en este sentido, se entiende como la unidad de elementos físicos o hardware que son requeridos para que se materialice la explotación de las aplicaciones bien sean informáticas o de software.

El sistema informático consta de dos elementos principales: una unidad central encargada de procesar la información, conocida como ordenador, y una serie de dispositivos periféricos que permiten la entrada de datos para su procesamiento y la salida de los resultados obtenidos (Chacón, s.f).

Sin embargo, un sistema no se limita únicamente a la colección de herramientas, sino que estos recursos deben estar estructurados en función de un objetivo específico. En el ámbito de los sistemas informáticos, estos recursos son llamados hardware, mientras que la estructura que los emplea para lograr un objetivo determinado es conocida como software del sistema.

En su concepción como sistema de información es posible referir lo planteado por Montoyo y Marco (2012), quienes lo definen como un conjunto de componentes que actúan de forma interrelacionada para materializar un objetivo, interactuando por medio de elementos de entrada, salida, sección de transformación y mecanismos de control.

Los Sistemas Informáticos se componen de elementos interrelacionados, como software, hardware y la intervención humana, que operan en conjunto con un propósito específico: facilitar el procesamiento y almacenamiento de información (Hernández, 2003); la información interactúa através de codificación numérica por medio de diferentes sistemas, siendo: binario, octal y hexadecimal.

Para calificar como un sistema informático, es esencial contar con estos tres componentes, ya que la ausencia de alguno de ellos transformaría el sistema en un mero almacenador de datos, similar a una biblioteca o un archivo físico. Entre estos elementos, el software desempeña un rol fundamental, ya que es responsable de la gestión y el almacenamiento efectivo de los datos (Laudon y Laudon, 2004).

Un sistema informático es un conjunto interconectado de componentes que trabajan en conjunto para realizar tareas relacionadas con el procesamiento, almacenamiento y transmisión de información mediante el uso de tecnologías de la información y la comunicación (TIC). Estos sistemas pueden variar en tamaño y complejidad, desde simples dispositivos individuales hasta redes globales de computadoras interconectadas.

Los componentes principales de un sistema informático suelen incluir: Hardware, software, redes, datos, procesamiento,almacenamiento periféricos; se estructuran para la realización de diversas tareas informáticas que se extienden al procesamiento de datos a la comunicación de información.

Un sistema informático es una estructura que posibilita el almacenamiento y procesamiento de información a través de una serie de componentes interconectados, incluyendo hardware, software y recursos humanos. Estos tres elementos son esenciales para su funcionamiento. En términos simples, los sistemas informáticos engloban las metodologías que facilitan la preservación y protección de datos mediante sistemas automatizados.

El sistema informático asume la responsabilidad de coordinar los recursos del hardware y supervisar las aplicaciones, con el propósito de proporcionar al usuario una experiencia óptima durante su interacción con la computadora. Este logro se materializa a través de los siguientes componentes (Herrerías, 2016):

1. Gestión de memoria: La memoria, como recurso fundamental, es requerida por todos los programas y aplicaciones para su funcionamiento. Los sistemas operativos desempeñan la función de administrar y regular la capacidad de la memoria mientras los programas se encuentran en ejecución.

El "administrador de memoria", una parte integral del sistema operativo, realiza el seguimiento de las áreas de memoria en uso y las que no lo están, con el objetivo de asignar espacio en memoria a los procesos según sus necesidades y liberarla una vez finalizados. También es su responsabilidad gestionar el intercambio de datos entre la memoria principal y el disco cuando la memoria principal no puede satisfacer las demandas de todos los procesos.

2. Sistema de archivos: Un sistema de archivos abarca una serie de carpetas y directorios esenciales para el almacenam cfiento, organización, creación, manejo y acceso a los datos. Los sistemas operativos incorporan su propio sistema de archivos, que se representa visual o textualmente mediante administradores de archivos. Estos administradores facilitan el control de acceso a los archivos y permiten llevar a cabo actividades como copiar, eliminar, crear, mover y renombrar.

3. Gestión de procesos: Los procesos corresponden a los programas en ejecución, los cuales requieren una supervisión adecuada para funcionar sin problemas. Los sistemas operativos integran módulos que se encargan de gestionar los procesos, asegurando su ejecución mediante una planificación adecuada y considerando la concurrencia entre ellos.

4. Gestión de E/S (Entrada/Salida): Los dispositivos periféricos, que abarcan elementos de entrada y salida, son accesibles y utilizables a través de interfaces o abstracciones provistas por el sistema operativo. Estas interfaces se apoyan en controladores de dispositivos específicos del sistema operativo, los cuales facilitan el acceso y uso de los dispositivos hardware para las aplicaciones.

En síntesis, el sistema informático se encarga de orquestar los recursos, las aplicaciones y las interacciones del usuario en la computadora, asegurando un funcionamiento eficiente y fluido mediante la gestión de memoria, el sistema de archivos, los procesos y los dispositivos periféricos.

1.1.1. Hardware.

El Hardware es una parte esencial en los sistemas informáticos y por ello, es pertinente comprender su funcionamiento. El hardware se refiere a la pluralidad de componentes tangibles en la computadora tales como los eléctricos, electrónicos, electromecánicos y mecánicos.

Los componentes fundamentales que componen el hardware de una computadora colaboran de manera conjunta para permitir su operatividad. Algunos de estos componentes son externos a la caja o carcasa (dispositivos periféricos), mientras que la mayoría residen en el interior de dicha caja (dispositivos internos).

Así, permiten realizar transformación de datos introducidos a códigos binarios para el procesamiento de la computadora; se ejemplifica en: tarjeta madre, microprocesador, memoria RAM, fuente de poder, cables y unidades de almacenamiento (Pérez, 2010); estos componentes interactúan de manera coordinada para permitir que la tecnología funcione de manera efectiva.

A continuación, se detallan algunos de los elementos clave que integran el hardware y su importancia en el contexto de la informática (Moreno, 2019):

1. Unidad Central de Procesamiento (CPU): La CPU es el cerebro del sistema informático y realiza operaciones de procesamiento, cálculos y toma de decisiones. Es responsable de ejecutar instrucciones de software y coordinar el funcionamiento de los otros componentes.

2. Memoria: La memoria, tanto RAM como memoria de almacenamiento, es esencial para el rendimiento del sistema. La RAM proporciona espacio para que la CPU realice operaciones rápidas y temporales, mientras que el almacenamiento a largo plazo guarda datos y programas incluso cuando la computadora se apaga.

3. Dispositivos de entrada y salida: Los dispositivos de entrada, como teclados y ratones, permiten al usuario comunicarse con la computadora. Los dispositivos de salida, como monitores e impresoras, muestran la información procesada por la computadora de manera comprensible para los usuarios.

4. Placa Madre: Es la placa principal que conecta y comunica todos los componentes del hardware entre sí. Contiene conectores y circuitos que permiten que los componentes se comuniquen y funcionen en conjunto.

5. Tarjeta Gráfica: También conocida como GPU (Unidad de Procesamiento Gráfico), esta tarjeta se encarga del procesamiento de gráficos y es esencial para la visualización de imágenes y videos de alta calidad.

6. Dispositivos de Almacenamiento: Estos componentes almacenan datos a largo plazo. Los discos duros tradicionales y las unidades de estado sólido (SSD) son ejemplos comunes de dispositivos de almacenamiento.

7. Fuentes de Alimentación: Proporcionan la energía eléctrica necesaria para que todos los componentes funcionen adecuadamente.

8. Dispositivos Periféricos: Incluyen elementos como impresoras, escáneres, cámaras web y altavoces, que amplían la funcionalidad de la computadora para satisfacer necesidades específicas.

El hardware es esencial porque establece los cimientos sobre los cuales el software opera. Sin una infraestructura física adecuada, el software no puede ejecutarse ni brindar los resultados deseados. Además, el rendimiento y las capacidades de una computadora dependen en gran medida de la calidad y la compatibilidad de sus componentes hardware.

En los términos de Amengual (2007), se compone de elementos físicos que ingresan la información que será procesada con posterioridad a través de la ejecución del software que hace parte del sistema informático.

El hardware constituye la entidad física y concreta de un sistema informático, englobando la totalidad de los elementos tanto físicos como electrónicos que componen una computadora o dispositivo electrónico. En síntesis, el hardware constituye la estructura física que posibilita el funcionamiento y la ejecución de tareas de un sistema informático. **Figura 1**

Figura 1. *Esquema básico de hardware de un ordenador*

Nota: La figura evidencia la concepción de Díaz (2012, p. 06) en referencia al hardware de un sistema informático.

1.1.2. Software.

El término “software” se refiere al conjunto de elementos lógicos o soporte lógico que constituyen la base de un sistema informático. Este conjunto comprende los componentes lógicos necesarios para llevar a cabo tareas específicas, en contraste con los componentes físicos, denominados "hardware".

Dentro de estos componentes lógicos se encuentran las aplicaciones informáticas, como procesadores de texto, que permiten al usuario manipular contenido textual. Asimismo, se incluye el software de sistema, como el sistema operativo, que es esencial para que otros programas funcionen correctamente. Además de facilitar la interacción entre los componentes físicos y las aplicaciones, el sistema operativo proporciona una interfaz con el usuario (Sánchez, s.f).

> El término 'software' se refiere al conjunto de instrucciones de datos electrónicos del programa que lee un procesador de computadora para realizar una tarea o una operación. En contraste, el término 'hardware' se refiere a los componentes físicos que

> se puede ver y tocar, como el disco duro, el mouse y el teclado de la computadora (Quispe, 2019, p. 09).

La Interfaz Gráfica de Usuario (GUI, por sus siglas en inglés) aprovecha las capacidades gráficas de las computadoras para ofrecer un medio amigable de comunicación con ellas. Las GUI han eliminado la necesidad de memorizar listas de comandos, reemplazándolas por iconos, ventanas y barras de herramientas que permiten de manera intuitiva indicar a la computadora las acciones que deseamos que realice (Maida y Paciencia, 2015). El software es el componente lógico esencial en los sistemas informáticos, que abarca desde las aplicaciones hasta el sistema operativo y la interfaz gráfica de usuario, brindando la funcionalidad necesaria para la realización de tareas informáticas.

1.1.3. Recursos humanos e información.

La información también incluída en un sistema informático corresponde a los recursos humanos e información de los mismos, los cuales fungen como herramientas dadas para reunir, gestionar y organizar información y datos personales de las personas; principalmente, sobre aquellas que hacen parte de una organización.

En un sistema informático, los recursos humanos y la información desempeñan roles críticos para su funcionamiento eficiente y efectivo. Los recursos humanos en el contexto de un sistema informático se refieren al personal o individuos que operan, mantienen y gestionan el sistema.

Estos profesionales son responsables de la configuración, administración, soporte técnico y desarrollo del sistema informático. Es entonces extensivo a los programadores y desarrolladores crean software y aplicaciones que funcionan en el sistema informático, atendiendo a las necesidades específicas de los usuarios y las organizaciones.

Así también, contempla a los administradores de sistemas se encargan de mantener y gestionar los componentes de hardware y software del sistema. Esto incluye asegurarse de que el sistema esté funcionando sin problemas, implementar actualizaciones y parches, y garantizar la segurida, los equipos de soporte técnico brindan asistencia a los usuarios cuando encuentran problemas o dificultades con el sistema. Ayudan a resolver problemas técnicos, responder preguntas y ofrecer orientación sobre el uso adecuado del sistema.

Los profesionales en el campo de la gestión de datos se encargan de asegurar que la información se almacene, organice y recupere de manera eficiente y precisa. Esto puede

involucrar tareas como el diseño de bases de datos, la seguridad de los datos y la implementación de estrategias de respaldo.

Los recursos humanos gestionan y operan el sistema informático, mientras que la información fluye a través del sistema, se procesa y se utiliza para tomar decisiones y llevar a cabo tareas específicas. La colaboración entre estos dos elementos es esencial para el funcionamiento exitoso de cualquier sistema informático.

1.2. Acceso abusivo

Para conceptualizar "acceso abusivo", es posible llegar al mismo desde el concepto de "acceso indebido", el cual corresponde a la irrupción, acceso o preservación del logueo sin estar autorizado en algún bien jurídico tutelado que requiera autorización personal debido a que allí se encuentra información personal o un sistema de uso restringido.

1.3. Ciberataque

El concepto de ciberataque no ha sido debidamente definido, tal como es indicado por Lazar y Nicolae (2018):

> La dificultad en el ámbito ciberataques consiste, por un lado, en la falta de una definición regulada y, por otro lado, en la complejidad de este concepto, que se diferencia de otros tipos de ataques. El ciberespacio mismo genera esta complejidad. (p. 159).

Sin embargo, ha sido desarrollado doctrinalmente, puesto que ciberataque, según Figueroa (2022), se refiere a un ataque en medios cibernéticos meticulosamente diseñado y ejecutado por individuos o grupos con el objetivo de causar daño a un sistema informático o una red. Estos ataques se aprovechan de las debilidades en la seguridad humana para acceder al software de un dispositivo, explotando las posibles vulnerabilidades existentes. En el caso de ser víctima de un ciberataque, se desencadenan una serie de consecuencias y sucesos que tienen un profundo impacto en la integridad de la persona.

Los ciberataques pueden variar en sus objetivos y naturaleza, dependiendo de las intenciones del atacante. Pueden abarcar desde el robo hasta el sabotaje. Durante la ejecución de estos ataques, existe el riesgo de pérdida de información personal o confidencial, lo que puede resultar en pérdidas económicas o violaciones de la privacidad.

Esto también puede incluir el robo de fotos almacenadas utilizando credenciales obtenidas ilegalmente, el vaciamiento de cuentas bancarias, el hurto de contactos de teléfonos móviles para llevar a cabo engaños, y otras situaciones elaboradas con astucia y persuasión.

Los ciberdelincuentes emplean estrategias osadas y persuasivas que crean situaciones que atrapan a individuos desprevenidos en acciones perjudiciales. Los ciberataques son actos cuidadosamente planeados que explotan debilidades en la seguridad humana y tecnológica, ocasionando daños importantes en el ámbito personal y económico, y erosionando la confianza en el entorno digital.

En este sentido, Urueña (2015), permite comprender algunas de las modalidades del ciberataque: virus informático, envío masivo de correo no deseado, suplantación de remitentes de mensajes mediante Spoofing, envío de Keyloggers, uso de troyanos para control remoto de sistemas, uso de archivos BOT del IRC y Rootkits.

Un ciberataque se refiere a una acción meticulosamente concebida y llevada a cabo por individuos o grupos con el propósito de causar daño a un sistema informático o a una red. Estos ataques capitalizan las vulnerabilidades en la seguridad humana para acceder al software de un dispositivo, aprovechando las posibles debilidades existentes. En el caso de ser víctima de un ciberataque, se desencadenan una serie de consecuencias y acontecimientos que tienen un profundo impacto en la integridad de la persona afectada.

Los objetivos y la naturaleza de los ciberataques pueden variar según las intenciones de los atacantes. Estos pueden oscilar entre el robo de información y el sabotaje. Durante la ejecución de estos ataques, existe el riesgo de pérdida de información personal o confidencial, lo que puede dar lugar a pérdidas económicas o a la vulneración de la privacidad.

También puede incluir el robo de fotos almacenadas utilizando credenciales obtenidas de manera ilícita, el vaciamiento de cuentas bancarias, la sustracción de contactos de teléfonos móviles para llevar a cabo engaños, y otras situaciones diseñadas con astucia y persuasión.

Los ciberdelincuentes emplean estrategias audaces y convincentes que cautivan a la población colombiana, creando escenarios que atrapan a individuos desprevenidos en actos perniciosos. En síntesis, los ciberataques deben ser comprendidos como aquellas acciones cuidadosamente planeadas que explotan debilidades en la seguridad humana y tecnológica, causando daños significativos en los ámbitos personal y económico, y erosionando la confianza en el entorno digital.

2. Clasificación del tipo penal del delito de acceso abusivo a sistema informático

En el presente acápite se hace clasificación del delito mencionado en el artículo 269A del Código Penal (2000); en razón de ello, se enuncia el artículo a analizar:

> 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.

Es un tipo penal principal que cuenta con un sujeto activo indeterminado y monosubjetivo, el verbo rector de “acceder” y “mantenerse”, de tipo común, mera conducta, consumación instantánea, mono-ofensivo (la protección de la información y de los datos como bien jurídico tutelado), de mera conducta, autónomo y completo.

2.1. Definición del bien jurídico tutelado

Los delitos informáticos parecen que, en un principio, buscan proteger una parte de los sistemas informáticos, específicamente el software, sin embargo, afirmar que los delitos informáticos protegen al software "en sí mismo" no supera la abstracción y amplitud atribuidas a la tutela de la información (contenida en un sistema informático) "como tal".

Así también ha sido considerado por Mayer (2017): “la funcionalidad informática debe tutelarse en términos acotados, porque no es posible sancionar cualquier afectación de la operatividad de un sistema informático sin obstaculizar el normal desarrollo de diversas actividades de relevancia para las personas” (p. 255).

A esto se puede agregar una posible confusión entre el interés legal (presunto) del "software" y otros intereses legales, como la propiedad o los activos. En este sentido, si se asume que el software es un activo valioso sujeto a la disposición de una persona y con respecto al cual su titular tiene una relación reconocida o al menos tolerada por la ley, ¿qué aspectos adicionales abordarían los delitos informáticos en la protección del software que no estén cubiertos en otras secciones del marco legal penal, especialmente aquellas relacionadas con los delitos contra la propiedad o los activos? Lo mismo puede decirse si se equiparan los programas

de computadora con obras literarias, artísticas o científicas, y su impacto se considera específicamente como una infracción de la propiedad intelectual.

Además, la protección penal del software parece confundir dos conceptos que deberían diferenciarse: el objeto material y el objeto legal del delito. En esta línea de pensamiento, un programa de software podría ser el objeto material de ciertos delitos informáticos, de manera similar a cómo un documento puede ser el objeto material de un fraude, o una billetera puede ser el objeto material de un robo. Sin embargo, esto aún no aborda el interés legal protegido por estos comportamientos.

La funcionalidad en el ámbito de la informática es un requisito fundamental para llevar a cabo diversas actividades de gran importancia tanto para individuos como para instituciones en un Estado democrático de derecho. Esto se refiere al conjunto de condiciones que permiten que los sistemas informáticos ejecuten de manera eficiente tareas que involucran el almacenamiento, procesamiento y transferencia de datos, todo dentro de un nivel de riesgo aceptable.

El reconocimiento de la funcionalidad informática como un interés legal distinto y estrechamente vinculado al campo de la informática encuentra justificación cuando los delitos informáticos, además de afectar el software de un sistema informático, abarcan el uso de redes computacionales.

En este contexto, la funcionalidad informática representa, por un lado, un interés cuyo significado y alcance deben definirse de manera dinámica, considerando los mecanismos operativos de las redes computacionales que actúan como plataformas para interconexiones remotas y extensas entre individuos. Por otro lado, la funcionalidad informática es un interés legal instrumental de naturaleza colectiva, que requiere una protección penal específica y precisa.

2.2. Identificación del ingrediente normativo

El ingrediente normativo que se encuentra dentro del artículo 269A corresponde aque el sujeto activo de la acción:

I. Acceda al sistema informático sin una autorización que así lo determine.
II. Exceda de las facultades otorgadas por el titular legítimo del derecho que autorizó su acceso y, en este sentido, se mantenga dentro del sistema informático.

Este artículo establece los parámetros legales que definen la conducta prohibida en relación con el acceso y permanencia en sistemas informáticos, exigiendo que el acceso sea autorizado y que el sujeto no exceda los permisos concedidos, lo cual busca prevenir y sancionar actividades ilícitas en el ámbito digital.

3. Desarrollo jurisprudencial

Para comprender los elementos del delito de acceso abusivo a un sistema informático, es posible recurrir al desarrollo jurisprudencial de la Corte Suprema de Justicia en su sala Penal, sede de casación.

3.1. Sentencia SP 030 de 2023

La Corte Suprema de Justicia establece, por medio de la sentencia SP 030 de 2023 en la que la dra. Myriam Ávila Roldán es ponente, que este tipo penal se estructurado a partir de los siguientes elementos:

I. El sujeto activo no es calificado
II. El sujeto pasivo es la persona titular de los datos informáticos, el tratamiento de información, sus partes o componentes lógicos, indistintamente de ser persona natural o persona jurídica.
III. Materializa una lesión sobre los bienes jurídicos tutelados: la información, los datos y la intimidad.
IV. Es un delito de mera conducta.
V. Se ejecuta únicamente en la modalidad dolosa.
VI. Identifica que su ingrediente normativo es la carencia o limitación sobre la facultad o autorización para la realización de acciones como el acceso o el mantener el mismo al sistema informático.

La Sala concluyó que el acusado era cómplice de los delitos de acceso abusivo a un sistema informático y daño informático agravados. Esto se debió a que contribuyó a la comisión de estos actos delictivos al pasar por alto las irregularidades detectadas en el proceso de un expediente y al dirigir que el caso fuera asignado a su propia oficina judicial.

3.2. Sentencia SP 2685 de 2022

En la presente sentencia, la Corte reitera su postura sobre los elementos y la clasificación objetiva del tipo, puesto que permite evidenciar que el delito de acceso abusivo a un sistema informático será agravado en el caso en el que el sujeto activo sea un servidor público y se encontrare en ejercicio de sus funciones. Su reproche recae en la vinculación que dicha precisión realiza con el Estado en la materialización y consumación del injusto en cuestión.

Así también, se denota que los sistemas informáticos en el escenario de los servidores públicos, específicamente miembros de la Rama Judicial, suelen llevar a cabo este delito en plataformas como TYBA, Siglo XXI o SARJ.

3.3. Sentencia SP 592 de 2022

La Corte emitió un fallo respecto a la casación y doble conformidad de una sentencia de la Sala Penal del Tribunal Superior de Medellín. Esta sentencia había confirmado una condena por el delito de concierto para delinquir, y había revocado absoluciones previas por los delitos de acceso abusivo a sistema informático y concierto para delinquir.

Durante su análisis, la Corte examinó los elementos y características de los delitos mencionados, y determinó que no se modificaría la condena. Sin embargo, la Corte identificó un error en la dosificación de las penas de prisión y multa por debajo de lo requerido, aplicadas en relación con la totalidad de los hechos por los cuales se había condenado. Esto se hizo con el fin de asegurar el principio de reformatio in pejus, evitando que la pena impuesta sea más perjudicial para el condenado en la apelación.

El delito se caracteriza por varios elementos:

1. El autor, que no requiere una condición especial para acceder sin autorización a un sistema informático o mantenerse conectado conscientemente si tiene la autorización.
2. La víctima, que es el individuo o entidad propietaria del sistema informático.
3. Lesiona múltiples bienes jurídicos, como la información, los datos y la privacidad, convirtiéndose en un delito pluriofensivo.

4. Solo se considera la intención consciente (dolo) por parte del ciberdelincuente.
5. Se trata de un delito de pura acción, ya que la simple intrusión en una red informática, bajo las condiciones establecidas, afecta el bien protegido.
6. Involucra dos acciones principales o verbos rectores: acceder o mantener.
7. Como aspecto normativo, requiere que el perpetrador: a) acceda al sistema informático sin autorización, o b) incluso si tiene el permiso del dueño legítimo del derecho, permanezca dentro del sistema, excediendo los poderes otorgados.

3.4. Sentencia SP 4573 de 2019

En la presente sentencia, la Corte analiza la realización del delito de acceso abusivo a un sistema informático y como el mismo puede encontrarse relacionado a conductas punibles como el constreñimiento ilegal, la pornografía con menores de 18 años, la utilización o facilitación de medios de comunicación, entre otros.

En esta ocasión, el acceso abusivo a sistema informático recayó sobre la red social Facebook fue el medio por medio del cual el autor tuvo acceso a información privada e íntima de la víctima, evidenciando que es un delito pluriofensivo puesto que el bien jurídico tutelado no son los datos en sí mismos, sino que en algunos casos es extensivo al buen nombre, honra e integridad de una persona.

4. Toma de posición

Finalmente, se encuentra que el delito de acceso abusivo a sistema informático en Colombia fue implementado de forma tardía debido a que tuvo lugar hasta hace alrededor de quince años; sin embargo, se encuentra como un delito necesario en la tipificación puesto que la realización del mismo indica, prácticamente, la certeza de la existencia de delitos posteriores y de mayor gravamen.

Así también, las personas tanto naturales como jurídicas tienen la obligación de gestionar los incidentes resultantes del acceso abusivo a los sistemas de información desde una perspectiva técnica, jurídica y administrativa. Así también implementar mejores políticas y aumentar el presupuesto en educación sobre tecnología para que mayores cantidades de personas se instruyan y aumente la probabilidad de regular y controlar la delincuencia en medios virtuales, principalmente en aplicaciones e interfaces de uso de banca, salud o bursatil.

La evolución de las tecnologías de la información y la comunicación ha simplificado el acceso a los productos, canales y servicios ofrecidos por las instituciones financieras, reemplazando la necesidad de la presencia física en sus oficinas a nivel nacional con la opción de la banca virtual. No obstante, esta transformación también conlleva ciertos riesgos que pueden causar pérdidas para la industria financiera. Por tanto, se vuelve esencial adoptar cada una de las recomendaciones e instrucciones detalladas aquí para abordar adecuadamente esta circunstancia.

Conclusiones

En última instancia, el delito de acceso abusivo a sistema informático conlleva importantes implicaciones en la esfera digital y legal. Esta infracción se caracteriza por la penetración no autorizada en sistemas informáticos con la finalidad de obtener, alterar o sustraer información valiosa. En un mundo cada vez más interconectado y dependiente de la tecnología, esta conducta representa una amenaza significativa, ya que compromete tanto la confidencialidad de datos como la privacidad de individuos y entidades.

La relevancia de este delito radica en la vulneración de sistemas tecnológicos que almacenan y gestionan información sensible, incluyendo datos personales, financieros y comerciales. Los avances tecnológicos han proporcionado innumerables beneficios, pero también han dado lugar a nuevas formas de delincuencia que aprovechan las vulnerabilidades en la seguridad cibernética. El acceso no autorizado a sistemas informáticos puede tener un impacto devastador, desde la pérdida de datos hasta la interrupción de servicios críticos y el robo de propiedad intelectual.

En respuesta a esta problemática, la legislación y la jurisprudencia deben evolucionar de manera continua para abordar los desafíos del ciberespacio. La creación y aplicación de leyes específicas, así como la formación de precedentes judiciales, son esenciales para establecer un marco legal sólido y claro en torno a este delito. Además, la cooperación entre gobiernos, organismos internacionales y la industria tecnológica es crucial para desarrollar medidas de seguridad y prevención efectivas.

La lucha contra el acceso abusivo a sistemas informáticos no solo se centra en la persecución de los responsables, sino también en la prevención y mitigación de los riesgos. Las empresas y las instituciones deben implementar protocolos de seguridad robustos, realizar auditorías regulares y educar a sus usuarios sobre las mejores prácticas de seguridad en línea.

La conciencia y la capacitación en ciberseguridad son componentes clave en la defensa contra este tipo de delito.

En resumen, el delito de acceso abusivo a sistema informático presenta un desafío complejo en la era digital actual. La protección de la información, la privacidad y la integridad de los sistemas informáticos requiere una colaboración multidisciplinaria entre el ámbito legal, tecnológico y social. La evolución constante de la legislación, la formación en seguridad cibernética y la adopción de medidas de prevención son elementos esenciales para enfrentar de manera efectiva esta problemática en constante evolución.

Referencias bibliográficas

Amengual Argudo, J. (2007). Hardware del PC. Informática básica. Recuperado de: https://repositori.uji.es/xmlui/handle/10234/168308

Chacón, J. (s.f). Sistemas informáticos: Estructura y funciones. Elementos de “hardware”. Elementos de “software”. Revista Preparadores de Oposiciones para la Enseñanza. Génova.

Congreso de la República. (2000). Ley 599 del 2000. Por medio de la cual se expide el Código Penal Colombiano. Diario Oficial No. 44.097. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Corte Suprema de Justicia. (2, marzo de 2022). Sentencia SP 592 de 2022. M.P. Diego Eugenio Corredor Beltrán. https://cortesuprema.gov.co/corte/index.php/2022/04/01/acceso-abusivo-a-un-sistema-informatico-concepto/

Corte Suprema de Justicia. (24, octubre de 2019). Sentencia SP 4573 de 2019. M.P. Eugenio Fernández Carlier. https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1nov2019/SP4573-2019(47234).PDF

Corte Suprema de Justicia. (27, julio de 2022). Sentencia SP 2685 de 2022. M.P. Fabio Ospitia Garzón. https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1ago2022/SP2685-2022(55313).pdf

Corte Suprema de Justicia. (8, febrero de 2023). Sentencia SP 030 de 2023. M.P. Myriam Avila Roldán. https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2023/SP030-2023(58252).pdf

Díaz Herrera, S. (2012). Hadware de una computadores. Universidad Autónoma del Estado de Hidalgo. https://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/hardware.pdf

Figueroa Cubillos, T. (2022). Ciberataques, riesgos y consecuencias que han afectado a la población colombiana entre los años 2018 y 2020. E[Trabajo de grado, Universidad Nacional Abierta y a Distancia]. Repositorio. https://repository.unad.edu.co/handle/10596/51582

Hernández Trasobares, A. (2003). Los sistemas de información: Evolución y desarrollo. Universidad de Zaragoza. Revista de relaciones laborales. (10-11). 149-465. https://dialnet.unirioja.es/descarga/articulo/793097.pdf

Herrerías Rey, J. (2006). Hardware y componentes. Editorial. Anaya Multimedia.

Laudon, K. y Laudon J. (2004). Sistemas de Información Gerencial. Octava Edición. Prentice

Maida, E. y Paciencia, J. (2015). Metodología de desarrollo de software. [Trabajo de grado, Pontificia Universidad Católica Argentina]. Repositorio. https://repositorio.uca.edu.ar/handle/123456789/522.

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. Revista Chilena de Derecho. 44(1). 261-285. https://www.scielo.cl/pdf/rchilder/v44n1/art11.pdf

Montoyo, A. y Marco, M. (2012). Tema 2: Sistemas de información. Universidad de Alicante. https://rua.ua.es/dspace/bitstream/10045/18830/6/Tema_2_-_Sistemas_de_Informacion.pdf

Moreno Pérez, J. (2019). Fundamentos del Hardware. Editorial Síntesis.

Pérez Chávez, C. (2010). Informática para preparatoria. https://infocobachczm.files.wordpress.com/2017/05/informc3a1tica-2-ceciliapc3a9rez-chc3a1vez.pdf.

Quispe Delgado, F. (2019). Software libre: Concepto y definición de Software libre, historia y evolución, características de los Software libre, Software libre y la educación, aplicaciones. [Trabajo de grado, Universidad Nacional de Educaión]. Repositorio. https://repositorio.une.edu.pe/bitstream/handle/20.500.14039/4616/Software%20libre.pdf?sequence=1&isAllowed=y

Sánchez López, J. (s.f). Software 1: Sistema Operativo. Software de Aplicación. https://proyectocirculos.files.wordpress.com/2013/11/software.pdf

Urueña Centeno, F. (2015). Ciberataques, la mayor amenaza actual. Instituto Español de Estudios Estrategicos. https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf