COLEGIO MAYOR NUESTRA SEÑORA DEL ROSARIO

FACULTAD DE JURISPRUDENCIA

UNIVERSIDAD DEL ROSARIO

EL ACCESO ABUSIVO A SISTEMAS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO COLOMBIANO: PROBLEMÁTICAS Y PROPUESTA PARA SU SUPERACIÓN.

Monografía para obtener el título de abogada

Presentado por:

Angie Beltrán Báez

Juliana Carrillo Carrascal

Director:

Majer Abushihab

Bogotá D.C. Septiembre de 2017

Índice

1. Introducción

"Vivimos en un mundo que, siguiendo la expresión de Nicolás Negroponte, se ha vuelto digital".

(Castells, 2002, p. 2)

1.1 Planteamiento

En las últimas décadas la ciencia y la tecnología han avanzado a pasos exponenciales al punto que hoy se pueden llevar a cabo actividades que cincuenta años atrás no se hubiesen pensado posibles. Todo este desarrollo, además de facilitar el transcurrir diario de la ciudadanía, se ha vuelto indispensable en las formas de vida de la sociedad contemporánea.

Tal situación se evidencia a través de la introducción cada vez más frecuente, y del nivel de incidencia de las herramientas y medios tecnológicos que han permeado todos los aspectos de la vida de una persona, desde el plano económico y profesional hasta el personal, en asuntos tan cotidianos como decidir qué transporte y ruta tomar hacia determinado destino o cuándo comprar divisas de acuerdo a la tasa de cambio que reporte el mercado en tiempo real.

Y es en el afán del ser humano por relacionarse con su entorno, junto con su esfuerzo por ser más productivo y afrontar los retos que traen las nuevas sociedades, que nacen los grandes flujos de información, la necesidad de saber y de contar qué está pasando. Es también en este mundo globalizado, donde se desvanece y se traspasa todo tipo de fronteras para dar paso a una comunicación eficaz que supera hasta las distancias más largas, gracias a las tecnologías de la información y la comunicación que hoy en día se conoce como las TICs.

Pero en términos concretos, ¿qué debe entenderse por *TICs*? y ¿en qué consiste ese desarrollo o proceso tecnológico? Pues bien, por tecnología se entiende no sólo aquellas formas de telecomunicaciones y transmisiones de información, sino también las máquinas que hacen posibles dichos procesos como los computadores y los programas que a estos se le incorporan; en

cuanto al desarrollo, se puede indicar que se trata del proceso de transformación tecnológica en el que la información se genera, almacena, recupera, procesa y transmite.

Las nuevas tecnologías de la información no solo constituyen aquellos recursos y medios que permiten manipular información, máquinas, programas informáticos sino que también implican todo su desarrollo, para obtener el fin último que es convertir, administrar, transmitir y almacenar dicha información.

En tal sentido, es indudable el papel transformador que los desarrollos tecnológicos recientes han tenido y tienen en la sociedad, así como su impacto en la generación, procesamiento y difusión o forma de comunicación de información y datos, que nos convierten en una verdadera *sociedad de la información,* definida ésta por Camacho (como se citó en Salazar, 2009) como "(…) un conjunto de actividades comerciales, comportamientos sociales, actividades individuales y formas de organización política y administrativa que comparten el mismo medio de transmisión de la información, las redes de la comunicación" (p.92).

Ahora bien, de una forma u otra todas las personas tienen contacto con las TICs, ya sea como creadores o productores, o simplemente como usuarios; el creador es quien controla la tecnología, en el sentido que es quien tiene el poder de decidir qué le va a entregar al público y a qué le va a permitir acceder; y el usuario es quien determina qué uso les da. Resulta importante aclarar que por tecnologías no sólo se debe entender el uso de su computador o máquinas sino también del "Internet" que es una herramienta para procesamiento, almacenamiento y difusión de información.

Estas y otra serie de actividades, dan origen a nuevos riesgos tal y como lo ha demostrado la historia ante inminentes cambios sociales. El ser humano, por ejemplo, ha descubierto y

potencializado otro tipo de tecnologías que han mejorado su calidad de vida; sin embargo, de estas construcciones previas se han derivado riesgos ocasionados por su mal uso o manejo, tal y como ocurrió con la energía nuclear.

Los nuevos avances tecnológicos no escapan de ese escenario. La sociedad actual, en su afán por acceder, procesar y transmitir información, creó "el ciberespacio"[1]; un lugar que aunque sirve para satisfacer las necesidades actuales, no excluye la posibilidad de ser usado para fines con impacto negativo, ya que precisamente al tratarse de un espacio artificial, su control resulta más laborioso, sumado a que se trata de una herramienta en pleno desarrollo (tanto en su uso como en su alcance) lo que ha facilitado la formación del "cibercrimen"[2] cometido a su vez por los "ciberdelincuentes"[3].

Y de la necesidad de entrar a regular este nuevo riesgo y con la intención de disminuirlo, es que los Estados han tomado medidas como la Ciberseguridad entendiendo por ella "todas esas acciones que ponen en marcha tanto el Estado como el sector privado para minimizar los riesgos de amenaza que puedan sufrir entidades de cualquier naturaleza y el ciudadano del común" (Cortes, 2015, p.8).

---

[1] Al respecto de la definición de "ciberespacio", véase Cortes (2015) cuando señala: "El Ciberespacio es el espacio artificial creado por el conjunto de (…) [Sistemas de Información y Telecomunicaciones que utilizan las tic o Tecnologías de la Información (informática) y las Comunicaciones (telecomunicaciones)] es decir de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial. El ciberespacio es pues mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio" (p.8).

[2] En cuanto al concepto de "cibercrimen", véase Miró (2012) cuando afirma: "Al hablar de cibercriminalidad, lo hago en sentido amplio como concepto englobador de cualquier delito cometido mediante el uso (esencial) de las TIC. Esto nos debe servir para comprender la variedad de delitos de naturaleza distinta que conforman tal categoría y, por tanto, y a los efectos que ahora nos interesan, la variedad de objetivos sobre los que pueden actuar las, por su parte, diferentes tipologías de cibercriminales y, por ende, la multiplicidad de víctimas de la cibercriminalidad que existen" (p. 261).

[3] Respecto a la definición de "ciberdelincuentes", véase Ojeda, Rincón, Arias, & Daza (2010): "Aquellos que se introducen en este mundo virtual con el fin de realizar actuaciones fraudulentas, las cuales son cada vez más frecuentes y variadas respondiendo al desarrollo tecnológico" (p.45).

Una de las maneras en las que el Estado plasma y desarrolla esas políticas de ciberseguridad se refleja en el Derecho penal vigente en sus ordenamientos, ya que:

> Con el advenimiento de la Sociedad de la Información, el derecho ha tenido que amoldar sus disposiciones de última ratio, a efectos de crear sanciones a quienes atenten contra los medios informáticos, o cuando se valen de estos para la comisión de delitos ya descritos en la ley penal. (Salazar, 2009, p.97)

Sin embargo, dichas disposiciones establecidas por los Estados en ocasiones no cumplen con el objetivo para el cual fueron creadas y el ejercicio legislativo se torna deficiente.

1.2 Problema jurídico

Nuestro análisis se da respecto de uno de los tantos riesgos que trajo la sociedad de la información: el Hacking, en palabras de Sieber (2008) "la penetración en los sistemas informáticos, la cual no es llevada a cabo con la intención de manipular, sabotear o espiar, pero si por el placer de transgredir las medidas de seguridad" (p.9), nominado desde el Derecho Penal colombiano como el acceso abusivo a sistemas informáticos, y a su vez del nuevo bien jurídico que se crea y pretende proteger con la consagración de este tipo penal, que al ser la puerta de entrada de la cibercriminalidad se le conoce como el delito informático[4] por excelencia.

El enfoque en el acceso abusivo a sistemas informáticos, ya que en el ámbito académico colombiano es poco el conocimiento y desarrollo que se tiene frente al tema a pesar de ser un

[4] En la definición de "delito informático", véase Suarez (citado en Ojeda et al, 2010) quien al respecto señala: "El delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información per se cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales" (p. 49).

delito tan común. Y es que la sociedad lo ha aceptado como una conducta o práctica habitual en su cotidianidad llegando incluso en ocasiones a ignorar su ilegalidad; de esta manera tampoco existe conciencia acerca de los efectos que conlleva dicha conducta.

El hacking trae consigo una diversidad de consecuencias, algunas de las cuales son de relevancia para el Derecho penal según los supuestos de hecho y el contexto en el que se enmarque, por lo cual en este análisis se estudiará la forma en que está tipificado el delito en la Ley 599 de 2000 (adicionada en lo pertinente por la ley 1273 de 2009), y el impacto que dicha tipificación trae especialmente en el plano de la antijuricidad.

En este orden de ideas, este trabajo se encamina a resolver el siguiente problema jurídico:

Tal como está consagrado el artículo 269A de la ley 599 de 2000 *¿se satisface el principio de lesividad y en consecuencia la antijuricidad material*?

1.3 Objetivo

El objetivo de esta monografía gira en torno al análisis de la forma en la que ha sido consagrado el tipo penal de *acceso abusivo a sistemas informáticos* en la ley penal colombiana y si esta cumple con la finalidad político criminal por la cual el legislador colombiano ha seguido lo expuesto por el Derecho internacional.

Así las cosas, con el fin de solucionar el problema jurídico planteado, el análisis se dará respecto de la configuración de cada uno de los elementos del tipo de *acceso abusivo a sistema informático* a la luz de la antijuricidad y la satisfacción del principio de lesividad del bien jurídico tutelado, lo cual permitirá identificar falencias y proponer posibles soluciones frente a estas.

1.4 Metodología

El trabajo investigativo se basará en un *método dogmático*, ya que primero se revisará el componente normativo del tipo penal en mención, tanto en Colombia como en el Derecho comparado; y su aplicación, para lo cual se hará uso de diferentes fuentes, teniendo como principales el ordenamiento jurídico colombiano, la doctrina y jurisprudencia al respecto, así como fuentes auxiliares de Derecho comparado junto con los instrumentos internacionales vigentes sobre la materia.

Sin embargo esta monografía no se limita a un trabajo meramente descriptivo sino que comprende un análisis sobre el objeto de la norma y si la forma en la que fue concebida por el legislador colombiano cumple con el fin deseado. Tratándose entonces, también de una investigación a través del uso de los métodos inductivo y deductivo (Baquero de la Calle & Gil, 2015).

Lo anterior, dado que se aplicarán las normas generales vigentes a supuestos de hecho concretos lo cual ayudará a evidenciar cómo funciona la norma, "Complementándose con el análisis de varias situaciones particulares que nos permitan sacar conclusiones generales" (Baquero de la Calle y Gil, 2015, p. 31), sobre el tratamiento que se le está dando al delito de acceso abusivo a sistemas informáticos y de esta manera encontrar falencias tanto en la consagración como en la aplicación del tipo penal, con el fin de poder plantear las posibles soluciones.

2. Abstracto

El propósito de ésta investigación es analizar el tipo penal acceso abusivo a sistema informático, las nociones sobre éste, su regulación, su tipificación y cómo ésta impacta en el ámbito de la antijuricidad material.

Para tal próposito se hace uso de referentes como los instrumentos internacionales, derecho comparado y doctrina, se exponen los elementos objetivos y subjetivos del tipo, los requisitos de la antijuricidad material y el principio de lesividad analizando la aplicación de estos a casos concretos con el fin de determinar las posibles falencias de la redacción del tipo penal y sugerir una propuesta que logre superarlas.

Palabras claves: Derecho penal; Delito informático; Acceso Abusivo; Sistema informático; Antijuricidad; Principio de Lesividad; Peligro; Riesgo; Lesión; Bien jurídico.

Abstract

The purpose of this research is to analyze the criminal figure abusive access to computer system, its notions, regulation, classification and how it impacts in the field of antijuricity.

In order to achieve this objective, international instruments, comparative law and doctrine are used as reference, the objective and subjective elements of the figure, requirements of the antijuricity are exposed and analazyng the application of these to specific cases so as to establish the possible shortcomings of the drafting of the criminal figure and to suggest a proposal that can overcome theme.

Keywords: Criminal law; Computer crime; Abusive access; Computer system; Antijuricity; Offensive material; Danger; Risk; Trespass; Legal good.

3. Capítulo I. Hacking: nociones generales

3.1 Aproximación al bien jurídico de la información

Antes de continuar, resulta oportuno aclarar lo que para efectos de este trabajo se entiende por cibercriminalidad, que es, todas las conductas punibles que involucran para su comisión el uso esencial de las TICs; a su vez, de ella pueden derivarse dos clases de delitos, aquellos que ya están descritos en la ley penal y que para su comisión se valen de alguna herramienta derivada de las TICs (como medio), y por otro lado aquellas conductas que se realizan contra los medios informáticos (teniéndolos como fin) lo que el derecho penal ha nominado como "delitos informáticos"[5] en sus esfuerzos por abarcar nuevas situaciones de riesgo derivadas de los avances tecnológicos[6].

De esta manera, según Suárez (citado en Ojeda, Rincón, Arias, & Daza, 2010):

> El delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información *perse* como bien jurídico tutelado, diferente de los intereses jurídicos tradicionales. (p.49)

De la definición de Suárez-Sánchez, cabe resaltar que el bien jurídico tutelado por esta clase de delitos es la "información", y es que si bien estos tipos penales pueden llegar a proteger

[5] En este caso, se habla de medios informáticos como medio para llevar a cabo otro tipo de conductas y medios informáticos como el fin de la conducta desplegada.

[6] Sin embargo a diferencia de lo que afirma (Miró, 2012) otros doctrinantes consideran que si bien hay una diferencia entre criminalidad informática y delitos informáticos, la cibercriminalidad solo hace referencia a estos últimos. Así autores como Posada exponen que por cibercriminalidad debe entenderse únicamente los delitos que tienen como objeto vulnerar los medios informáticos (Posada, 2013a).

"intereses jurídicos tradicionales" como lo explica el autor, su fin principal no es otro que velar por "la Protección de la información y de los datos"[7].

Por lo anterior, dentro del desarrollo de la creación de este nuevo interés jurídico a tutelar fue necesario determinar su naturaleza y así decidir de qué manera se entraría a proteger. En este sentido -traemos a colación el *análisis de la información como bien jurídico*[8] hecho por Pablo Marquez- donde se evidenció una problemática acerca de la categoría que el Derecho debía darle a la información ya que no encajaba en las categorías tradicionales de los bienes civiles; sin embargo, se optó por equipararlo a un bien incorporal, aunque la "información" no cumpliera a cabalidad con la definición jurídica de lo que se entiende por éste concepto.

Ahora bien, a pesar de no poderse clasificar dentro de una de las categorías existentes en los ordenamientos, se reconoció sobre este interés el derecho a la propiedad, lo que ofreció una respuesta a dicho problema, pues al reconocer el derecho a la propiedad se reconoce la "información" como un bien, sin necesidad de que jurídicamente se encuentre nominado como tal.

En dicho estudio, se encontró otra característica atribuible a la información en términos económicos, la de bien no rival, "el hecho de que un bien sea no-rival implica que su consumo por parte de un individuo no reduce la cantidad del bien que puedan disponer los demás" (Márquez, 2002, p.72), esta característica se asemeja en el ámbito jurídico a los bienes no-consumibles, así mismo otra cualidad es que puede ser excluyente o no.

---

[7] La Ley 599 de 2000 le da esa nominación.

[8] Dicho análisis se encuentra contenido en el libro "El delito informático, la información y la comunicación en la esfera penal conforme con el nuevo código penal", donde el autor realiza un estudio sobre los bienes jurídicos que puede llegar a afectar un delito informático.

La anterior precisión se vuelve importante, dadas las facultades derivadas del derecho de propiedad, como el usufructo, uso y disposición, pues "esto determina que, en tanto que los bienes informáticos son no-rivales, toda persona tiene potencialidad de uso e incluso de disfrute pero no del derecho de disposición" (Márquez, 2002, p.72).

Por lo tanto el derecho de disposición de la información como bien depende de su naturaleza de exclusiva o no, cuando se trata de ésta como bien público, no existe exclusividad alguna y en consecuencia las protecciones legales y constitucionales permiten su disposición, mientras que al hablar de la información como bien privado, dicha disposición es de un titular determinado, excluyendo a quienes no ostenten tal calidad (Márquez, 2002).

Esta es la diferencia entre el dominio de la información como bien incorporal y de los bienes civiles tradicionales, por lo cual, en aras de una protección especial, el derecho penal tutela estos nuevos intereses jurídicos y en algunos casos crea incluso nuevos bienes jurídicos específicos como "la información"[9] que indiscutiblemente sería "intermedio", pues también protege ya sea directa o indirectamente otros bienes jurídicos tradicionales.

Dentro de la variedad de bienes jurídicos tradicionales, uno de los más importantes es la intimidad; es así como el autor Mario Madrid Malo quien a su vez sigue al autor Novoa Monreal expone:

> La intimidad es el espacio de la personalidad de los sujetos que no puede llegar a ser por ningún motivo de dominio público, salvo la propia elección, así la intimidad busca proteger el espacio privado, y se estructura como un derecho

[9] De la necesidad de velar por los nuevos intereses que aún no se encontraban protegidos por los ordenamientos, algunos países como Colombia crearon un nuevo bien jurídico independiente que se encarga de su protección, sin embargo otros ordenamientos como España decidieron incluir esos intereses en bienes jurídicos ya existentes en su ordenamiento como la intimidad.

> protector frente al Estado y los particulares en el campo privado. (Como se citó en Gonzales, 2010, pp.47-48)

Por lo tanto, dado el desarrollo de las TICs y el impacto que éstas han generado en la sociedad, entran en colisión las "libertades informáticas" (Márquez, 2002, p. 46) con la esfera privada de las personas, haciéndose necesario ampliar el ámbito de protección del derecho fundamental de la intimidad y el espacio personal.

Lo mismo sucede con bienes jurídicos como el orden económico y social, la vida, la integridad personal, la libertad y el patrimonio económico (Márquez, 2002; Posada, 2013a). Claro está que la afectación a los diferentes bienes jurídicos dependerá de la conducta que se realice y el tipo penal específico en el que se enmarque.

Al tratarse de un bien jurídico intermedio, los delitos informáticos tienen la calidad de ser pluriofensivos "es decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo". En conclusión no se afecta un solo bien jurídico sino una diversidad de ellos" (Acurio del Pino, s.f., p.21)

Las nuevas tecnologías no solo sirvieron para crear nuevos bienes jurídicos, tales como:

> La calidad, pureza e idoneidad de la información en cuanto tal y de los productos que de ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa. (Acurio, s.f., p.22)

Sino que dicho desarrollo tecnológico también conllevo a ampliar el espectro de protección de otros bienes jurídicos preexistentes en los ordenamientos, que pudieran ser potencialmente afectados por estas. En este sentido y tal como lo afirma Pardini (2002):

> Retomando la noción del ámbito en el cual se mueve el hombre, posibilitado aquel por la aparición de Internet, es fácil advertir que esta nueva dimensión trae aparejada una nueva categoría de derechos a proteger. Entendiendo que existen nuevos bienes jurídicos a tutelar, se deduce que estos presentan nueva o especial vulnerabilidad. Asimismo, estos bienes, y los tradicionales pueden ser objeto de nuevos ataques, en virtud de lo cual aparecen una categoría distinta de ejecutores. (p.64)

Siguiendo este orden de ideas, proteger estos nuevos bienes jurídicos implica a su vez la temprana tutela de bienes jurídicos tradicionales, ya que se adelantan las barreras de protección de éstos para evitar su puesta en peligro por los nuevos riesgos surgidos en la sociedad de la información.

3.2 Concepto de hacking y diferencia con el cracking

En cuanto al delito informático objeto de este estudio -el Hacking-, la doctrina ha sugerido la siguiente definición:

"El término hacking se usa para describir la penetración en los sistemas informáticos, la cual no es llevada a cabo con la intención de manipular, sabotear o espiar, pero si por el placer de transgredir las medidas de seguridad" (Sieber, 1998, p.145). Lo que quiere decir que quienes realizan esta conducta ingresan sin el consentimiento de quien tenga el legítimo derecho sobre el

sistema informático, incluso violando medidas de seguridad en los casos en los que sea necesario, pero sin tener ninguna intención de causar un daño diferente al simple acceso.

Es entonces dicha finalidad la que diferencia el “hacking” del “cracking” ya que:

> En el caso de querer dolosamente dañar el sistema, alterar o suprimir información, se estaría ante un supuesto de cracking, que es una figura que subsume al hacking. Es decir, en el cracking, además de configurarse un acceso ilegítimo al sistema de información, se lo daña o se lo altera con voluntad dolosa de provocar dicho daño, sin que se produzca un concurso ideal de figuras. (Pinochet, 2006, p. 495)

4. Capítulo II: Marco normativo

4.1 Instrumentos Internacionales

4.1.1 Convenio de Budapest 2011.

Es de tal gravedad el efecto que actividades como el hacking y el cracking pueden generar en las sociedades, que incluso han despertado preocupación en la comunidad internacional, tanto así que se hizo necesaria su regulación, recogiéndolas en una normatividad a la que hoy se le conoce como el Convenio de Budapest de 2001 o Convenio sobre Cibercriminalidad[10], instrumento internacional que nace en el seno del Consejo de Europa siendo el primero en combatir la cibercriminalidad[11] al establecerla como un deber de los estados firmantes (Consejo de Europa, 2001).

Ya que se trata del Convenio sobre Cibercriminalidad, para efectos de esta investigación, se atienden aquellas conductas que atentan contra los sistemas informáticos y la información contenida en éstos, más no aquellas que solo los utilizan como medio o instrumento.

En este sentido se crearon obligaciones claras y precisas como la tipificación de los delitos informáticos, ofreciendo incluso en su contenido definiciones que sirven como pautas para el desarrollo legislativo de los ordenamientos jurídicos de los Estados parte, al punto que incluso para quienes no son firmantes se ha convertido en su referente principal[12].

---

[10] Entró en vigencia el 1 de Julio de 2004 siendo estados parte Albania, Croacia, Estonia, Hungría, Lituania, Rumania, para posteriormente adherirse Alemania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Bulgaria, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Finlandia, Francia, Islandia, Italia, Letonia, Macedonia-Antigua República de Yugoslavia, Noruega, Países Bajos, Portugal, República de Moldavia, Serbia y Ucrania.

[11] Entendiendo por ella tanto criminalidad informática como delitos informáticos.

[12] Entre los Estados no firmantes del Convenio se encuentra Colombia, si bien el tratado no es vinculante para

De esta manera, en sus esfuerzos por brindar unas directrices a los Estados, el Convenio establece unas definiciones generales en su Capítulo I – Terminología- Articulo 1 Definiciones, sin embargo de este catálogo se estudiarán sólo aquellas que guardan relación con el objeto de estudio del presente trabajo, el acceso abusivo a sistemas informáticos, las cuales se consagran en los siguientes términos:

A los efectos del presente Convenio:

> Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa. Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función (…). (Consejo de Europa, 2001, p. 4)

Los anteriores conceptos hacen parte entonces, de la tipificación del delito de acceso abusivo a sistemas informáticos consagrada en el capítulo II –Medidas que deberán adoptarse a nivel nacional- Sección 1- Derecho Penal sustantivo- Título I – Delitos contra la Confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, en su artículo 2 denominado "acceso ilícito" que establece:

> Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir

---

nosotros, la consagración del delito en nuestro ordenamiento jurídico nos permite evidenciar la influencia que ha tenido el Convenio de Budapest.

> que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con sistema informático conectado a otro sistema informático. (Consejo de Europa, 2001, p. 4)

En cuanto al Título I, si bien el Convenio no consagra expresamente la protección del bien jurídico información, este título refiere que el interés a proteger por los Estados mediante la tipificación de este delito será la confidencialidad, la integridad y la disponibilidad de los datos y el sistema informático. Resulta entonces relevante definir el alcance de estos conceptos en los siguientes términos:

- Por integridad se entiende, que se vela por la autenticidad de la información, en el sentido de que se mantenga en el mismo estado en que fue depositada por el legítimamente autorizado, garantizando que no sea modificada por quien no lo está (Aguilera, 2010).
- Por confidencialidad, según la Organización para la Cooperación y el Desarrollo económico, La OCDE, se entiende como "el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada" (Aguilera, 2010, p. 10). Es decir que el titular de la información se encuentra en la libertad de decidir quienes se encuentran autorizados y en qué términos lo están.
- Por disponibilidad, se entiende que es la facultad que tiene el usuario autorizado de acceder a la información en el momento que lo desee (Aguilera, 2010).

De esta manera cuando se configura el supuesto de hecho de un acceso abusivo a sistema informático, se debe examinar si se vulnera la confidencialidad, integridad y disponibilidad de los

datos y el sistema informático, punto que resulta ser uno de los más importantes en este estudio que al ser integral, no solo debe tener en cuenta la tipicidad a la hora de la configuración del delito sino también su antijuricidad.

En lo que respecta a la tipificación del acceso ilícito, se puede observar que el primer inciso del artículo 2, solo ofrece un concepto general acerca del delito de acceso abusivo a sistemas informáticos, define como elementos esenciales el mero acceso y la ausencia de consentimiento para configurar un acceso ilegítimo.

Ahora bien, en el inciso siguiente, cuando el Convenio expone: "(…) Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con sistema informático conectado a otro sistema informático" (Consejo de Europa, 2001, p. 4).

Se deja entonces, a disposición de los Estados definir en sus ordenamientos jurídicos si estos elementos circunstanciales serán necesarios o no para configurar el tipo.

4.1.2 Decisión marco 222/2005.

El 23 de febrero el Consejo de Europa[13] suscribió la Decisión Marco sobre los ataques a los sistemas de información, que consagra en su artículo 2:

> 1. Cada Estado Miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o una parte de un sistema de

[13] Las decisiones marco son proferidas por el Consejo de Europa derivada de su facultad legislativa, entendidas como instrumento de desarrollo legislativo vinculante para los Estados parte de la Unión Europea.

> información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.
>
> 2. Cada Estado Miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad. (Consejo de Europa, 2005, p. 3)

En este caso el concepto de acceso mantiene los mismos elementos esenciales enunciados en el Convenio de Budapest, en cuanto que se trata de un acceso doloso y sin autorización, sin embargo introduce un elemento subjetivo respecto de la gravedad de la conducta, cuando expresa "al menos en los casos que no sean de menor gravedad", lo que tiene como objetivo que los Estados condenen aquellas conductas que resulten de tal gravedad que sean relevantes para el Derecho Penal.

A rasgos generales se puede decir que la Decisión Marco en un principio intenta cerrar el ámbito de aplicación del concepto, pero si se estudia con detenimiento puede concluirse que dicha disposición genera un vacío, ya que no determina qué se entiende por una conducta menos grave y una grave, dejando así a discrecionalidad de cada ordenamiento jurídico su delimitación.

4.2 Hacking en el Derecho comparado

En pro del cumplimiento de las obligaciones internacionales que imponen estos instrumentos (BUDAPEST y la DM), los Estados han tipificado en sus ordenamientos jurídicos el delito de acceso ilícito o ilegal a sistemas informáticos. La discrecionalidad de cada Estado para

determinar los elementos circunstanciales trae como consecuencia que estos varíen según el Estado del que se trate.

Por lo anterior, mostraremos las iniciativas de diferentes países en el marco del Derecho Comparado, desde la comunidad europea hasta Latinoamérica:

4.2.1 Francia.

Las primeras regulaciones francesas tuvieron lugar con la modificación del Código Penal en el año 1988 al entrar en vigencia la ley 88-19 "Loi Godfrain", con la cual se creó un capítulo nuevo para el Código Penal que se denominó "Sobre ciertas infracciones en materia informática", e intentó recoger toda la actividad criminal fruto de las nuevas tecnologías de la información (Loiseau & Canales, 2004).

Sin embargo posterior a esto, con la ley 92-683 que entró en vigencia en 1994, se realizaron modificaciones a las disposiciones informáticas existentes, quedando finalmente contemplado el acceso fraudulento en sistemas informáticos dentro del Libro III, Título II, Capítulo III denominado *"*De los atentados contra los sistemas de tratamiento automatizado de datos", en el artículo 323-1 del Código Penal Francés de la siguiente forma (Loiseau & Canales, 2004):

> Artículo 323-1. El hecho de acceder en forma fraudulenta a la totalidad o parte de un sistema de tratamiento automatizado de datos, o de mantenerse en él, será castigado con un año de prisión y multa de 15.000 euros.
>
> Si de ello resultare, bien la supresión o la modificación de datos contenidos en el sistema, o una alteración del funcionamiento de este sistema, la pena será de

> dos años de prisión y de 30.000 euros de multa. (Sáenz & De la Cuesta. 2005, p. 82)

El tipo no exige entonces, una finalidad determinada que acompañe el acceso para que se configure el delito, no obstante sí agrava la sanción cuando como consecuencia de dicho acceso se suprimen o modifican los datos contenidos en el sistema, o cuando por su comisión se altera el funcionamiento de éste.

En este capítulo se estipula que el sujeto activo de la conducta no sólo incurrirá en una pena general sino además en penas accesorias, las cuales varían según se trate de una persona natural o jurídica, de acuerdo a lo contenido en los artículos 323-5 y 323-6.

Así mismo, acoge la posibilidad de tentativa para los tipos penales tipificados en el capítulo al disponer en el *"*Artículo 323-7. "La tentativa de los delitos previstos por los artículos 323-1 a 323-3-1 será castigada con las mismas penas asignadas a ellos*"* (Sáenz & De la Cuesta. 2005, p. 83).

4.2.2 Italia.

Tras la ratificación del convenio de Budapest mediante la ley italiana de 18 de marzo No. 48 de 28, por la cual se modifica del Código Penal Italiano aprobado por decreto No. 1398 de 19 de octubre de 1930, se modificó el delito de acceso abusivo a sistemas informáticos contenido en el título 15 "de los delitos contra la persona", sesion IV "de los delitos contra la inviolabilidad del domicilio", artículo 615-ter "acceso abusivo a sistema informatico o telematico" el cual establece:

> Quien abusivamente se introduzca en un sistema informático o telemático protegido por medidas de seguridad o se mantenga en él contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo, será castigado con prisión de hasta tres años. (Rueda, 2010, p.166)

Como se observa en la tipificación de este artículo, el legislador italiano no solo se preocupó por castigar la conducta del acceso a sistemas informáticos sino que también amplío el tipo a los sistemas telemáticos; así mismo estableció como elemento objetivo, que los sistemas cuenten con medida de seguridad.

Finalmente, la tipificación contempla la conducta de quien se mantenga en alguno de los sistemas mencionados en contra de la voluntad ya sea expresa o tácita de su titular.

El artículo establece que la pena aumentará en los siguientes casos:

> 1). si el delito es cometido por un funcionario público o una persona encargada de un servicio público, con abuso de poder o violación de las obligaciones inherentes a la función o servicio, o la que ejerce de forma abusiva la profesión de detective privado, o con abuso de la calidad de operador del sistema (...). (Policía de Estado de Italia, 1930, p.10)

En este primer numeral, el agravante se da entonces, en razón de un criterio de calidad especial del sujeto, pues aumentará la pena cuando el sujeto activo de la conducta se encuentre inmerso en esas circunstancias u ostente tales calidades.

En segundo lugar consagra que también aumentará la pena “2). Si el culpable para cometer el hecho usa violencia contra las cosas o las personas, o está claramente armado” (*Policía de Estado*

de Italia, 1930, p.10). Y por último dentro del catálogo de agravantes, en el numeral tres dispone:

> 3). Si de la conducta se deriva la destrucción o el daño del sistema informático o la interrupción total o parcial de su funcionamiento, o la destrucción o el daño de datos, de la información o de los programas que este contenga. (Policía de Estado de Italia, 1930, p.10)

Por lo tanto la legislación italiana al igual que muchas otras, establece como agravante, no la finalidad o intención, sino con la producción del resultado de dañar los sistemas, interrumpir su funcionamiento o destruir los datos, información o programas contenidos en el mismo, es decir, el delito consagra una modalidad básica del delito amparada en una actividad de mera conducta, para igualmente establecer una segunda modalidad de resultado, verificada en la destrucción, interrupción, daño, etc. de los sistemas.

En este sentido la doctrina italiana ha expuesto que el acceso sin autorización no tiene una categoría uniforme, pues se puede dar en varias modalidades, primero como el simple acceso con fines recreativos conocido como la piratería informática, segundo como aquel que tiene por objeto dañar la información contenida en el sistema o parte del mismo y por último el acceso que tiene como finalidad llevar a cabo otras conductas punibles (Genghini & Rocca, 2002).

No obstante lo anterior, en la forma en que Italia tipificó el tipo se trata de un delito de peligro, por lo cual se trata de un actuar delictivo independientemente de que se dé o no una vulneración traducida en un daño, en consecuencia, la lesión efectiva es solo una circunstancia de agravación.

4.2.3 Portugal.

En el marco de la comunidad europea, Portugal fue uno de los primeros países en elevar a nivel constitucional la protección de sus ciudadanos frente a los riesgos que surgieron a partir de las nuevas tecnologías y la sociedad informática (Bazán, 2005).

Tras un largo periodo de desarrollo legislativo, con la promulgación de la Ley No. 10 de 1991:

> "Protección de datos personales frente a la informática" se sentaron bases muy importantes para el derecho informático y la legislación posterior sobre el tema, pues "(...) establece que el uso de la informática debe procurarse de forma transparente y con estricto respeto por la reserva de la vida privada y familiar de los derechos, libertades y garantías fundamentales del ciudadano (…) (Bazán, 2005, p. 94).

Así las cosas, siguiendo los mandatos constitucionales, los postulados del Convenio de Budapest y la Decisión Marco, Portugal consagra la tipificación del delito de acceso abusivo a sistemas informáticos en la Ley No. 109 de 1991, "sobre criminalidad informática" (Rueda, 2010, p. 166) en su artículo 7 en los siguientes términos:

> 1. Quien acceda de cualquier modo, no estando autorizado y con la intención de obtener, para sí o para otro, un beneficio o ventaja ilegítimos, a un sistema o red informáticos será castigado con la pena de prisión, de hasta un año o con la pena de multa, de hasta 120 días. (Rueda, 2010, pp.166-167)

El tipo penal entonces, exige una finalidad, y es que el sujeto activo desarrolle la conducta con el fin de conseguir un beneficio ilegítimo para él o para un tercero.

El mismo artículo establece en los dos siguientes numerales como agravantes del tipo:

> 2. La pena será de prisión de hasta tres años o multa si el acceso se consigue con la infracción de medidas de seguridad. 3. La pena será de prisión de uno a cinco años cuando: a) a través del acceso, el sujeto haya tenido conocimiento de un secreto comercial o industrial o de datos confidenciales, protegidos por ley; b) el beneficio o ventaja patrimonial obtenidos sean de valor considerablemente elevado. (Rueda, 2010, p.167)

Como se evidencia, a diferencia de otras legislaciones, Portugal trató el tema de la transgresión de las medidas de seguridad de una manera muy particular, pues si bien no lo estableció como elemento esencial del tipo, tampoco lo dejó de lado al consagrarlo como uno de los supuestos que aumentan la pena, así mismo ésta aumenta cuando derivados del acceso se den los resultados descritos por el numeral 3.

Finalmente en el tipo se estipula:

> 4. Se castiga la tentativa", y se advierte que se trata de un delito querellable cuando el artículo 7 dispone en su numeral 5 "5. En los casos previstos en los números 1, 2 y 4 el procedimiento penal depende de querella. (Rueda, 2010, p.167)

En conclusión Portugal en virtud de los parámetros que establece el Convenio de Budapest para tipificar el acceso abusivo a sistemas informáticos, hace uso de su autonomía legislativa al establecer una finalidad y transgresión de medidas de seguridad en los términos ya expuestos.

4.2.4 Estados Unidos.

La primera ley federal que reguló al respecto tuvo lugar en 1986 con el "Federal Abuse and Fraud Act" permitiendo por primera vez la penalización de los llamados "delitos informáticos" (Hoscman, 2013).

Sin embargo la anterior fue derogada en 1994 cuando la legislación estadounidense adoptó el "*Computer Fraud and Abuse Act*", al agregarla al "*United States Code*" donde se recopila toda la normatividad federal vigente (Hoscman, 2013).

Dicha ley de fraude y abuso informático dispuso en su título "obtener[14] información de un acceso no autorizado a computador" los accesos ilegítimos en los siguientes términos:

> 1) hacking (acceso ilegítimo) seguido de descubrimiento de información protegida por razones de seguridad nacional o relaciones con el extranjero o información de circulación restringida por ley.
>
> 2) hacking con el objeto de hacerse de un archivo financiero de una entidad financiera o de un usuario de tarjeta o de un archivo de un consumidor que esté en poder de una consumer reporting agency.

[14] Respecto a la definición del término "obtener", véase Doyle & Bartlett (1986) cuando señala que según el senado de Estados Unidos se debe entender como la observación o simple lectura de la información, sin necesidad de que sea copiada, transportada o que efectivamente se remueva de su lugar de origen.

> 3) hacking con el objetivo de obtener información de un departamento o agencia del Estado estadounidense.
>
> 4) hacking con el objeto de obtener información de una computadora protegida (exclusivamente a disposición de una entidad financiera o del gobierno de los Estados Unidos).
>
> 5) Hacking accediendo ilegítimamente a una computadora, con la intención de defraudar, y cuyo accionar logra efectivamente su objetivo, siempre que dicha defraudación supere los cinco mil dólares obtenidos en un período menor a un año.
>
> 6) (...)
>
> 7) Acceso ilegítimo a una computadora que negligentemente cause un daño.
>
> 8) Acceso a una computadora protegida que cause objetivamente un daño (Hoscman, 2013, p. 274).

La reforma se dio gracias a:

> El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques (Borghello, 2011, p.14).

Como se puede observar esta tipificación contempla aquel acceso ilegítimo o hacking que se da en el ámbito de las instituciones financieras y en el sector estatal, lo que evidencia que las conductas enmarcadas en este contexto son las que resultan de mayor reproche para el Derecho penal estadounidense.

Así mismo la ley contempla una variedad de accesos, desde la obtención o simple acceso sin generar daño alguno hasta aquellos que sí lo concretan.

Dos de los casos más conocidos a nivel nacional que impulsaron tal cambio son:

Shadowhawk:

> Se trata de un joven de 16 años que operaba bajo el seudónimo de <<Shadowhawk>> quien violó el acceso a AT&T y los sistemas del departamento de defensa, siendo condenado en 1989 por el cargo de Fraude Computacional y Abuso, ya que destruyó archivos y copias de programas avaluados en millones de dólares; además publicó contraseñas e instrucciones que servían para violar la seguridad de los sistemas computacionales. (Palomá, 2012, p.205)

Wau Holland y Steffen Wenery:

> El 2 de Mayo de 1987, un par de jóvenes, Wau Holland y Steffen Wenery, logran entrar desde Alemania a las instalaciones VAX del cuartel general de la NASA, al ingresar sin autorización a su sistema central. Sin embargo evitaron ser judicializados al enviar un telex a los técnicos de la central, donde

> advirtieron que su ingreso había sido resultado de la debilidad del sistema al expresar:
>
> Tememos haber entrado en el peligroso campo del espionaje industrial, el crimen económico, el conflicto este-oeste y la seguridad de los organismos de alta tecnología. Por eso avisamos y paramos el juego. (Palomá, 2012, pp.205-206)

4.2.5 Chile.

Para hacer cara a los riesgos informáticos Chile decide convertirse en uno de los primeros países latinoamericanos en crear una tipificación de los delitos informáticos, contenida en la ley 19223 de 1993 “Ley contra los delitos informáticos” (Narváez, 2015, p. 7), dicha ley trae consigo la creación de un nuevo bien jurídico “la claridad, pureza e idoneidad de la información en cuanto a tal, como contenida en un sistema automatizado de tratamiento de la misma y de los productos que de sus operación se obtengan” y en consecuencia su protección (Palomá, 2012, p.215).

La ley se encuentra integrada por cuatro artículos relativos a ataques informáticos, dentro de estos el artículo 2 cobija el hacking en los siguientes términos:

> Artículo 2: El que con el ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio. (Palomá, 2012, p.215)

Como se observa, la legislación chilena consagra además de la conducta de acceder, las de interceptar e interferir, ampliando así los verbos rectores de la conducta; por otro lado agrega como elemento subjetivo del tipo una finalidad especial al enunciar "El que con el ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma*",* en este orden de ideas, la conducta se configura cuando se cumpla con alguno de los verbos rectores y se haya desplegado con cualquiera de las finalidades enunciadas en el artículo, pues "ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito" (Borghello, 2011, p.13).

Finalmente, La pena puede variar según los supuestos de hecho en los que se enmarque la conducta, "si un hacker, por ejemplo, ingresa indebidamente a un sistema para conocer información sin autorización, puede recibir desde 61 días hasta 3 años de presidio" (Acurio, 2015, p. 39), en estos casos la dosificación punitiva se mueve dentro de dichos mínimos y máximos.

4.2.6 España.

Este país no tiene tipificado un catálogo de delitos informáticos por lo que el delito del acceso abusivo a sistema informático se encuentra inmerso dentro de las diferentes conductas que atentan contra la intimidad, razón por la cual el análisis resulta más extenso.

El Código Penal Español ley orgánica 10/95, en el Título X "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en su Capítulo primero "Del descubrimiento y revelación de secretos" aborda las conductas que nos interesan, consagradas en los artículos 197 y 197 Bis.

En primer lugar hablaremos del artículo 197 Bis ya que es propiamente el delito del acceso abusivo a sistema informático, conocido en España como intrusión informática y descrito en los siguientes términos,

> Artículo 197 Bis:
>
> El que, por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo ejercicio a excluirlo, será castigado con la pena de prisión de seis a dos años. (Jefatura de Estado de España, 2015, s/p)

Resulta evidente que la legislación española hizo uso de la prerrogativa expuesta por el Convenio de Budapest y la DM al incorporar en la tipificación del delito "vulnerando las medidas de seguridad establecidas para impedirlo", convirtió entonces un elemento circunstancial del delito en uno esencial.

De esta manera sus tribunales han desglosado cada uno de los elementos que componen el tipo penal, "que el sistema de seguridad posea medidas de seguridad que impida el acceso a terceras personas no autorizadas para ello; que el acceso lo sea sin autorización; y que se acceda a datos o programas informáticos" (Diario del Derecho de España, 2015, s/p).

Por otro lado se encuentran en el tipo penal verbos rectores o conductas alternativas, al consagrar tanto el acceso como el mantenimiento en el sistema. Así el acceso se refiere entonces a entrar sin consentimiento al sistema y el mantenimiento sin autorización, este último referido a

los casos en los que en principio se accede con autorización sin vulnerar las medidas de seguridad, lo que implica que en ese momento la acción es legítima, pero el autor decide permanecer en éste contra la voluntad del titular.

Frente a este delito resulta importante aclarar dos cosas:

La primera de ellas, en la ley 10/1995 en el Título X, los bienes jurídicos que se buscan proteger son la intimidad, la propia imagen y la inviolabilidad del domicilio, tratándose específicamente del artículo 197 Bis el bien jurídico a proteger es la intimidad personal, es decir, la privacidad en el ámbito de la informática (Lefebvre, s.f.).

Y la segunda, que el objeto sobre el cual recae la acción es el sistema informático, ya sean los datos o los programas informáticos que hagan parte del mismo.

La jurisprudencia española se pronunció en la sentencia 88/2015 proferida por la audiencia provincial de Murcia con ponente Juan del Olmo Gálvez, sobre el delito de intrusión informática, por los siguientes hechos:

En el año 2011 la empresa Tahe Productos Cosmésticos, S.L. contaba con un sistema informático (protegido por medida de seguridad) con el propósito de ejercer control en su funcionamiento, de igual manera le proporcionaba a cada empleado un correo electrónico de uso profesional. Así a través del sistema, la empresa conoció sobre accesos inusuales al mismo y se constató que una de sus empleadas, quien se encontraba en incapacidad laboral, accedió desde un computador externo de manera ilegítima a los correos de otras tres trabajadoras, accediendo así a los datos y programas del sistema informático (Diario del Derecho de España, 2015).

Tras la apelación interpuesta contra la sentencia del 2 de Octubre del 2003 donde se condenó a la trabajadora por el delito de intrusión informática, la Sala estableció que sí se habían configurado todos los elementos del tipo y procedió a resolver el recurso confirmando el fallo en los siguientes términos:

- Es un acceso no consentido porque *"*la acusada no estaba autorizada en el momento de ejecución de los hechos, lo cual viene a ser reconocido por el propio recurso de apelación*"* (Diario del Derecho de España, 2015, s/p).
- La vulneración de las medidas de seguridad informáticas, no interesa si son débiles pues basta con:

  > (...) la existencia de un previo sistema de seguridad informático (exigencia del tipo), que puede ser soslayado con mayor o menor dificultad dependiendo de las habilidades, conocimientos u otros factores concurrentes en el sujeto activo del delito, pero que no por ello desmerecen la realidad de las medidas de seguridad (Diario del Derecho de España, 2015, s/p).

- El acceso a datos o programas informáticos contenidos en un sistema informático, se acredita, ya que la recurrente entró a los correos profesionales de otras tres trabajadores de la Empresa THAE, accediendo a los datos y programas contenidos en el sistema informático de la misma.

La jurisprudencia española también se ha pronunciado acerca de los supuestos en que las empresas ejercen control sobre los correos corporativos asignados a sus empleados, es así como el Tribunal constitucional, Sala 1ra se pronunció en la sentencia EDJ 2013/182887 del día 7 de octubre de 2003, en "el caso Alcaliber". Los supuestos de hecho que dan lugar a esta controversia son los siguientes:

Uno de los empleados de la empresa "Alcaliber S.A", la cual desarrolla una actividad químico industrial, fue despedido cuando se descubrió que estaba pasando información confidencial a otra entidad de manera ilegítima a través del correo corporativo y el móvil proporcionado por la empresa. El empleado presentó una demanda solicitando la improcedencia del despido, donde alegó que las pruebas en su contra eran nulas pues se obtuvieron producto de un acceso ilegítimo por parte de la empresa a su correo y móvil.

En primera instancia se desestimó la nulidad de la prueba pues en el estatuto de trabajadores, se permite ese tipo de prácticas cuando se tienen sospechas del comportamiento de un trabajador[15]. Así mismo se declaró improcedente el despido por ser una medida desproporcionada.

Sin embargo la empresa Alcaliber interpuso recurso de suplicación contra la anterior providencia buscando la procedencia del despido, dicho recurso fue concedido por lo cual el trabajador interpuso demanda de amparo ante Tribunal constitucional, que se resolvió en los siguientes términos:

Primero, el Tribunal se pronunció acerca del alcance que tiene el derecho a la intimidad al declarar que incluso permea el escenario de las relaciones laborales y se determinó que el contenido de los mensajes electrónicos integra su esfera de protección.

> "(...) que el cúmulo de información que se almacena por su titular en un ordenador personal -entre otros datos sobre su vida privada y profesional- forma parte del ámbito de la intimidad constitucionalmente protegido; también

[15] Así, el XV convenio colectivo de la industria química consagra en su artículo 59.11 como falta leve "la utilización de los medios informáticos propiedad de la empresa (correo electrónico, intranet, internet, etc.) para fines distintos de los relacionados con el convenio de la prestación laboral" (CCOO Federación de Industria Textil –Piel, Químicas y Afines, 2007).

> que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado el derecho a la intimidad personal -en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado (FJ 3). (Tribunal Constitucional de España, Sentencia EDJ 2013/182887. M.P. Andrés Ollero, 2013, p.12)

Igualmente trajo a colación la siguiente premisa,

> Los correos electrónicos enviados desde el lugar del trabajo están incluidos en el ámbito de protección del art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales EDL 1979/3822, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada (§ 41 y 44). (Tribunal Constitucional de España, Sentencia EDJ 2013/182887. M.P. Andrés Ollero, 2013, p.13)

Así el Tribunal Constitucional expuso que si bien el derecho a la intimidad es fundamental, no es absoluto y por esto se hace necesario analizar "la expectativa razonable de intimidad"[16] existente en el caso concreto. En su análisis siguió el criterio del Tribunal Superior de Justicia de Madrid, cuando advierte que los empresarios pueden realizar registros y controles en la información que se halle en los ordenadores, no obstante dicha facultad es limitada, pues es obligación del empleador dar aviso previo a los trabajadores sobre la existencia del control empresarial y de las condiciones en que este se da, evitando vulneraciones a la expectativa

[16] Es decir, por expectativa se entiende aquella que pudiera llegar a tener una persona de que no habrá una intromisión ilegítima por un tercero, y por razonable que cualquier persona en la misma situación tendría una expectativa semejante.

razonable de intimidad y accesos ilegítimos (Tribunal Constitucional de España, Sentencia EDJ 2013/182887. M.P. Andrés Ollero, 2013).

Sin embargo, por la actividad químico industrial de la empresa, el convenio colectivo de la industria química, donde se establece el uso del correo para fines laborales y por lo tanto su control, resultaba vinculante para las partes, en consecuencia el acceso al correo corporativo por parte de la empresa era legítimo y no se debía cumplir con el aviso previo[17].

En segundo lugar, dado que la ley española ha creado otra serie de tipos penales los cuales tienen como modus operandi la intrusión informática, hablaremos del delito de descubrimiento y revelación de secretos del artículo 197:

> "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
>
> 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o

[17] En este caso el trabajador debía saber independientemente de que la empresa se lo haya comunicado o no, que el correo era de uso laboral y que sería una falta leve de no ser así. Respecto de los datos que se tomaron del registro del teléfono móvil al no estar contemplados en el Convenio, si se necesitaba que se hubieran establecido previamente las directrices sobre su uso y control para que los mensajes de texto que se obtuvieron de este constituyeran una prueba legítima y por lo tanto no se considerará vulnerado el derecho a la intimidad.

registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas

> previstas en su mitad superior. (...). (Jefatura de Estado de España, 2015, s/p) (Subrayado fuera del texto)

Cabe resaltar que el tipo penal de descubrimiento y revelación de secretos, en su artículo 197 está compuesto por diferentes apartados que consagran una variedad de conductas, por lo cual se estudiarán las que resulten relevantes para el tema de este trabajo. Así las cosas, se procede a exponer la conducta del apartado 1:

> 197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. (Jefatura de Estado de España, 2015, s/p) (Subrayado fuera del texto)

Esta tipificación del delito comprende su realización derivada de tres modalidades, la interceptación de comunicaciones, la utilización de artificios y el apoderamiento, siendo ésta última la que nos ocupa.

El apoderarse consiste en apropiarse de papeles, cartas, mensajes de correo electrónico o documentos[18] de otro sin su consentimiento, y con la finalidad específica de descubrir sus secretos o vulnerar su intimidad, elementos que son necesarios para la comisión del delito.

[18] Esta modalidad resulta importante para efectos de esta investigación, al contener dentro del objeto material los mensajes de correo electrónico, ya que al apoderarse de información contenida en este tipo de herramientas es necesario que se dé el acceso a un sistema informático que cuenta con unas medidas de seguridad, que para este caso

Así, “El bien jurídico protegido es la intimidad personal, más concretamente, el derecho fundamental a la inviolabilidad de las comunicaciones consagrado en Const art.18.3 como parte integrante del derecho a la intimidad personal del individuo” (Lefebvre, sf, p.3).

Se hallan relevantes los casos de apoderamiento de los mensajes de correo electrónico con el fin de descubrir secretos, que se dan en el marco de una intrusión informática, pues casi siempre se encuentran precedidos por un acceso ilegítimo, sin embargo la conducta reprochable para este tipo penal es el apoderamiento y no propiamente el acceso.

Respecto a lo anterior ya se encuentran pronunciamientos en la jurisprudencia española, entre estos el caso que falló el Tribunal supremo, sala de lo penal con ponente Miguel Colmenero Menendez de Luarca, STC 1807/ de 2007, el cual se dio bajo los supuestos de hecho donde un señor para verificar el consumo de internet de su casa instaló en el ordenador un programa que vigilaba la actividad informática y la red, por el que le llegaban informes de las comunicaciones dadas en el mismo, fue así que descubrió que su esposa mantenía conversaciones con distintos hombres y en consecuencia decidió interceptar sus correos electrónicos para aportarlos como prueba de la infidelidad en su proceso de divorcio.

El Tribunal resolvió que era legítimo instalar programas de control en su ordenador, lo que realmente resultaba reprochable era el acceso a las conversaciones privadas de su esposa, seguido de su apoderamiento, al tratarse de un acceso con dolo se configuró la intención de descubrir los secretos y se vulnero la intimidad, independiente de que la finalidad principal fuese aportarlas al proceso de divorcio (Tribunal Supremo de Madrid, 2007).

---

sería la misma contraseña, y el hecho de que la finalidad sea conocer un secreto del sujeto pasivo evidencia la falta de consentimiento por parte del mismo.

En la exposición de esta sentencia y tras su análisis, se puede ver que la argumentación del Tribunal siempre estuvo dirigida al apoderamiento, por lo que se aclara que uno de los elementos esenciales para configurar el tipo penal no es la simple apertura de correspondencia o el acceso a correo electrónico (como lo sería en el delito de intromisión) sino que debe estar acompañada del efectivo apoderamiento de esta información.

Siguiendo el análisis del tipo penal de "Descubrimiento y Revelación de Secretos" en su integridad, la segunda conducta que recoge el artículo 197, relevante para el tema central de este trabajo, es la del apartado 2 que abarca "los abusos informáticos sobre datos automatizados relativos a la intimidad" (Bustos, 2008, p.248).

> 197.2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. (Jefatura de Estado de España, 2015, s/p) (Subrayado fuera del texto)

Lo primero que se debe resaltar es el bien jurídico que protege el segundo numeral de este artículo, según Agustín Jorge Barreiro "la libertad informática o "habeas data", es decir (...) "de los delitos que atentan contra la intimidad de las personas, haciendo uso ilegítimo de los datos personales, insertos en un programa informático" (Barreiro, 1995, p.113).

En este sentido, la legislación española busca proteger una de las dimensiones de la intimidad como lo es la libertad informática, para evitar el uso ilegítimo de los datos que las personas consignan en programas informáticos, por lo tanto de dicha libertad deriva el derecho de la persona a controlar esos datos en orden a que no se le dé un uso distinto al permitido (Barreiro, 1995).

En tanto la conducta descrita por el tipo penal está compuesta por diferentes verbos rectores, nos enfocaremos en el segundo inciso del artículo 197.2 donde se enuncian los verbos acceder, alterar y utilizar. Siendo el acceso la conducta que nos ocupa, ésta se refiere al simple conocimiento u obtención de toda información o dato que está registrado (Barreiro, 1995).

A diferencia de la intrusión del artículo 197 Bis que tiene como objeto de la conducta los sistemas informáticos, en el acceso del artículo 197.2 se trata de los "datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado" (Jefatura de Estado de España, 2015, s/p); por tanto no solo se limita a los sistemas informáticos sino que se amplía a los que tengan otra naturaleza, siempre y cuando la información registrada por el titular sea de carácter reservado, personal y familiar.

Finalmente, el artículo en su tipificación exige como elemento subjetivo del tipo, que las conductas descritas se realicen con la finalidad de provocar perjuicio a un tercero.

Los Tribunales en su jurisprudencia se han pronunciado sobre el delito, bajo los siguientes supuestos de hecho:

- En los meses de noviembre y diciembre de 2002, Miguel, quien era funcionario del Cuerpo Nacional de Policía, a través de las aplicaciones "Perpol y Objetos de la Policía Nacional", realizó consultas sobre datos del padre y hermano de la señora Amanda. Esto con el fin de obtener información sobre la empresa "La Despensa de Monxi", así mismo información personal de las personas en mención. Dichos datos fueron proporcionados a un hombre que posteriormente intentó secuestrar a Amanda el 29 de Abril de 2003 (Tribunal Supremo de Madrid, Sentencia 123/2009. M.P. Luciano Varela Castro, 2009).

- La Audiencia de instancia condenó a Miguel por el delito de Descubrimiento y Revelación de secretos, se formuló recurso de casación, pues alegaban que no se había interceptado ni difundido información reservada de carácter personal y familiar, por otro lado, que los archivos contenían información de acceso público y no se configuraba el elemento que exige un perjuicio a un tercero (Tribunal Supremo de Madrid, Sentencia 123/2009. M.P. Luciano Varela Castro, 2009).

En su análisis, el Tribunal estableció que los datos que el policía había comunicado a los otros hombres, eran públicos y de general acceso, así mismo información que era "cognoscible por todos", por lo que no deja de aclarar que el registro al que accedió Miguel, por supuesto contenía información reservada, personal y familiar de las víctimas, pero no se probó que la información cedida por Miguel, también haya sido la que está revestida de tal naturaleza; sin embargo no se excluye que haya habido un acceso a esa información en los términos del artículo 197.2 (Tribunal Supremo de Madrid, Sentencia 123/2009. M.P. Luciano Varela Castro, 2009).

Así mismo el Tribunal recuerda que al tratarse de un simple acceso no se exige como elemento para configurar el tipo, la intención de causar un perjuicio a un tercero, sino que dicha

finalidad sólo se exige respecto de las otras conductas contempladas en el mismo artículo (Tribunal Supremo de Madrid, Sentencia 123/2009. M.P. Luciano Varela Castro, 2009).

Así las cosas:

> En consecuencia cabe establecer las dos conclusiones siguientes: a) que existió acceso en las condiciones típicas, es decir sin legitimación y con independencia de si causó o no perjuicio a otras personas, y b) que, si bien el acceso lo fue a datos reservados de naturaleza personal, también alcanzó a otros datos, (...). (Tribunal Supremo de Madrid, Sentencia 123/2009. M.P. Luciano Varela Castro, 2009, s/p) (Subrayado fuera del texto)

Con lo anterior, se confirma entonces la condena al recurrente por las conductas descritas en el apartado número 2 del artículo 197 del segundo inciso el "mero acceso".

El artículo 197, tiene como agravantes los siguientes:

> 197.4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:
>
> a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registro" …
>
> 198. La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con

> las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años. (Jefatura de Estado de España, 2015, s/p)

Estos agravantes se dan en razón de la calidad que ostente el sujeto activo que despliega la conducta, por otro lado se establece un agravante en razón de la naturaleza de la información.

> 197.5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior. (Jefatura de Estado de España, 2015, s/p)

Se debe aclarar como lo pone de presente la doctrina y jurisprudencia, que no se debe confundir la información de carácter reservado del apartado 197.2 con la información sensible de la persona, aquella que hace parte del núcleo duro de la privacidad.

Al respecto Barreiro (1995) afirma:

> No resulta muy afortunada la referencia del legislador a los datos personales o familiares "reservados", pues todos los datos personales en cuanto son introducidos en un fichero automatizado son sensibles y estarán protegidos por el art. 197.2 del CP 59. El único sentido que puede darse a la mencionada exigencia legal, de que los datos personales o familiares han de ser "reservados", es la de entender que esos datos deben afectar a la intimidad

> personal, es decir, como “secretos” o “no públicos”, no conocidos por quien ilegítimamente accede a los mismos y teniendo en cuenta que el sujeto pasivo no desea que se conozcan. (p 118)

Tras este recorrido por el ordenamiento jurídico español, queda por decir que en esta legislación los tipos penales no se encuentran nominados, simplemente están delimitados por el bien jurídico que se pretende proteger y por títulos generales dentro de los cuales hay un listado de conductas, como lo es el capítulo primero del título X “Del Descubrimiento y Revelación de secretos”, así las nominaciones de cada tipo penal expuestas acá, vienen precedidas del desarrollo jurisprudencial.

4.3. Precisiones.

Tras este recorrido normativo que nos permitió evidenciar el estado actual del delito, se identificó que los estudios realizados giran alrededor del proceso legislativo y la tipificación en los diferentes Estados, de cómo ésta debe interpretarse y la aplicación que los Tribunales le han dado. Se encuentra que si bien el Derecho ha evolucionado y se han empezado a regular conductas que se dan como fruto de los avances tecnológicos, tales regulaciones se han preocupado más por la tipicidad, es decir, porque dichas conductas se establezcan como un delito, pero ha dejado de lado la precisión que requiere el ejercicio legislativo, y en consecuencia el impacto que puede tener los términos de la tipificación con relación a la afectación del bien jurídico protegido.

De esta manera no se observa que exista un desarrollo frente a la antijuricidad material de estos delitos, es decir, no se analiza hasta qué punto un supuesto de hecho que configure la conducta típica también satisface el principio de lesividad; los criterios para determinarlo no son claros ya que se debe hacer un estudio de interpretación desde la tipicidad de cada Estado, sin que tampoco en algunos de estos se haya encontrado gran desarrollo sobre el escenario de la antijuricidad más allá de la formal.

Sin embargo, cabe resaltar que en México se presenta una aproximación al estudio de la antijuricidad sobre las conductas contempladas como delitos informáticos. Así en el ordenamiento jurídico mexicano, son antijurídicas aquellas conductas que vayan en contravía de los preceptos jurídicos allí consagrados y de los valores que el legislador establece en pro del interés que las personas tienen en proteger su información y los medios informáticos en los que está contenida, en consecuencia en el Estado de Sinaloa se tiene que las conductas de delitos informático no solo son típicas por estar consagradas en el código penal, sino que cumplen con la antijuricidad formal pues por estar allí resultan contrarias al ordenamiento jurídico, no obstante se determinó que dichas conductas serán antijurídicas cuando opere una causal de justificación o de licitud (Montaño, 2008).

Se evidencia con estas causales que se admiten para los delitos informáticos, que se está teniendo en cuenta un estudio sobre la antijuricidad del delito, en el entendido que:

> Existe una causa de licitud, cuando la conducta o hecho siendo típicos, son permitidos, autorizados o facultados por la ley, a virtud de ausencia de intereses o de la existencia de un interés preponderante, para este autor, la conducta o hecho siendo típicos, son permitidos por la ley, en virtud de ausencia de interés

> o por existir un interés preponderante, es decir, es aquella especial situación en la que un hecho que normalmente está prohibido por la ley penal, no constituye delito por la existencia de una norma que lo autoriza o lo impide (Montaño,2008,p.202-203).

Así las cosas en el ordenamiento jurídico mexicano se habla de antijuricidad a la luz de una causal que torna la conducta atípica o que la justifica; a diferencia de Colombia donde la antijuricidad abarca otros escenarios, en palabras de Sampedro (2008) “la conducta que lesiona o pone en peligro el bien jurídico penal”(p.330).

5. Capítulo III: Acceso abusivo a sistema informático en Colombia

5.1 Nociones generales

A continuación se hará una aproximación doctrinal al concepto de acceso abusivo a sistema informático o hacking.

Para los autores chilenos Huerta y Líbano:

> Acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor. (Márquez, 2002, p.152)

Según los términos del profesor Palazzi (como se citó en Castro, 2008) "consiste en el acceso no autorizado a un sistema de datos a través de un proceso de datos a distancia, cometido sin intención fraudulenta ni de sabotaje o espionaje" (p.629). En esta misma línea los autores Aboso & Zapata (como se citó en Castro, 2008) afirman que:

> Esta conducta, denominada <<computerhacking>>, significa ingresar en el sistema informático de otro, sin el propósito de manipularlo, sabotearlo o espiarlo, sino de <<pasear<< o interiorizarse sobre las medidas técnicas de seguridad del sistema. Queda claro que esta acción se presenta, en muchos casos, como la puerta de ingreso para la comisión de otro tipo de delitos más graves (p. 629).

Se puede inferir de las anteriores definiciones dadas por doctrinantes reconocidos en la materia, que este tipo penal debe contener como elementos esenciales, un acceso ilegítimo, es decir, una ausencia de consentimiento al entrar a un sistema informático o tratamiento de información; y por otro lado no exige que la conducta se despliegue con una finalidad determinada sino que basta con la simple intención de querer acceder.

Tales conceptos además coinciden con la tipificación que otorga la convención de Budapest, al no disponer que se requiera de un elemento subjetivo específico, bastando el mero deseo de entrar al sistema informático, sin desconocer la posibilidad de que eventualmente se pueda exigir otra intención delictiva. Es así como queda a disposición de cada ordenamiento tipificar la conducta en los términos que considere deba ser sancionada por el Derecho penal (teniendo en cuenta que este derecho es de última ratio)[19].

Así las cosas, se estudiarán los términos actuales en los que el ordenamiento jurídico colombiano tipifica el acceso abusivo a sistema informático.

5.2 Marco normativo.

5.2.1 Antecedentes.

La sociedad de la información no se limita solo a los países más desarrollados sino que ha alcanzado países menos tecnológicos e industrializados como Colombia, por esta razón nos sumamos a la lista de países que han tenido que evolucionar en términos jurídicos desarrollando

[19] Y es que en principio los ordenamientos jurídicos en caso de desearlo, al no considerar que el simple acceso resulte relevante para el derecho penal bajo su concepción de última ratio, podrían abrirle campo en otra área del derecho que consideren más conveniente y menos restrictiva, como por ejemplo el derecho administrativo sancionador.

normas que permitan responder a esas nueva necesidades derivadas del desarrollo tecnológico (Salazar, 2009).

En sus esfuerzos por adecuar el derecho a las nuevas prácticas y desarrollos, el legislador colombiano introdujo en el año 2000 en la Ley 599, la primera sanción para quienes ataquen los medios informáticos; así en el libro II, del título III Delitos contra la Libertad individual y otras Garantías, Capítulo VII De la violación a la intimidad, reserva e interceptación de telecomunicaciones, artículo 195, se tipifica el delito de "Acceso Abusivo a un Sistema Informático": "Artículo 195. Acceso Abusivo a un Sistema Informático. El que abusivamente se introduzca a un sistema informático, protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene Derecho a excluirlo, incurrirá e multa" (Congreso de Colombia, Ley 599 de 2000, p. 181) (Código Penal Colombiano, derogado por el art. 4. de la Ley 1273 de 2009).

Este artículo tuvo una vigencia en el ordenamiento jurídico Colombiano de nueve (9) años, sin embargo, no cumplió su objeto como norma, ya que en la práctica judicial no fue utilizada (Ojeda, Rincón, Arias & Daza, 2010).

Lo anterior evidencia la poca trascendencia que tuvo la conducta, por un lado para el legislador, quien la consideró incluso no merecedora de pena privativa de la libertad, a la hora de proteger el sistema informático, pues asumió que una simple multa en primer lugar era proporcional al interés que estaba en riesgo; y quien no supo generar el impacto necesario para desincentivar la comisión de la conducta. Por otro lado, el desinterés de la justicia, pues no se generaron actividades investigativas y sanciones efectivas convirtiendo la norma en obsoleta por desuso.

5.2.2 Ley 1273/2009.

5.2.2.1 Proyecto de ley.

Este proyecto de ley se da como resultado de la investigación realizada por Alexander Díaz García y todo su equipo de trabajo, integrado por los doctores Fernando Velásquez Velásquez, Jarvey Rincón y Gabriel Roldán Restrepo, acerca de los delitos informáticos (Congreso de Colombia, Ley 1273 de 2009).

En éste proyecto, finalmente se pretendía modificar el Código Penal para adicionar el "título VII BIS" el cual además de crear el bien jurídico "de la protección de la información" con la intención de que fuera tutelado por el derecho penal, también tipifica todas las conductas que tienen como fin la afectación de la información (Díaz, 2010).

En principio la idea de crear nuevos tipos penales que abarcaran situaciones de "nuevos riesgos" no fue recibida con agrado por quienes tenían en sus manos la posibilidad de iniciar el proyecto, por dos razones principalmente: la primera consistía en considerar que no resultaba necesario modificar el código penal para integrar nuevas tipificaciones que incluyeran dichos riesgos (desconociendo de plano todos los avances derivados de la convención de Budapest); y la segunda, que se trataba de una modificación procedimental y no sustancial, lo que a todas luces era una percepción errónea del proyecto pues con la creación de nuevos tipos penales se hablaba de derecho penal de fondo y no de forma (Díaz, 2010).

Sin embargo, el proyecto logró ser tramitado por la Cámara de Representantes teniendo como ponente al Dr. Carlos Arturo Piedrahita Cárdenas de la Comisión Primera de dicha célula legislativa. Tras superar todos los debates, incluso mediante la definición del articulado por una

Comisión de Conciliación, finalmente se logró su sanción presidencial el 5 de enero de 2009 para derivar en la expedición de la denominada Ley de delitos informáticos 1273 de 2009 (Díaz, 2010)

5.2.2.2 Exposición de motivos.

El proyecto de ley en su respectiva exposición de motivos, argumentó que dicha necesidad se derivó de los contratiempos que surgieron como consecuencia del mal uso de las TICs y de sus principales herramientas (como lo son los computadores y el internet), ya que se generaron efectos lesivos tanto a personas naturales como jurídicas.

Como respuesta a esos impases, el proyecto consideró legítima la protección de tales intereses sociales a través de la creación de un nuevo bien jurídico, pues recordó que al ser elevados a "bien tutelado" por el Derecho, su vulneración acarrearía sanciones severas, las cuales ayudarían a disminuir su lesión. En consecuencia se dijo que se necesitaba de una norma que le otorgara ese carácter jurídico al mero interés social.

Además se argumentó que si bien el Derecho protegía infinidad de bienes jurídicos desde cualquiera de sus ramas, es el Derecho penal el que se debía ocupar de los más trascendentales para la convivencia en sociedad y cuya protección mediante otras herramientas o ramas del Derecho son ineficaces para prevenir su lesión, por esto ameritan una protección desde la última ratio como ocurrió con la información.

Sin lugar a dudas el tratamiento que se venía dando por el legislador resultaba insuficiente para protegerla pues no garantizaba su amparo integral y dejaba vacíos que facilitaban su vulneración.

Al ser entonces la información, un bien jurídico tan relevante, su protección no puede darse de manera indirecta por otros tipos penales, o como agravante, sino que necesita de la creación de tipos penales autónomos, donde el fin principal sea este bien y así su tutela resulte más eficaz.

En palabras de Pardini (2002):

> Retomando la noción del nuevo ámbito en el cual se mueve el hombre, posibilitado aquel por la aparición de Internet, es fácil advertir que esta nueva dimensión trae aparejada una nueva categoría de derechos a proteger. Entendiendo que existen nuevos bienes jurídicos a tutelar, se deduce que estos presentan nueva o especial vulnerabilidad. Así mismo, estos bienes, y los tradicionales, pueden ser objeto de nuevos ataques, en virtud de lo cual aparece una categoría distinta de ejecutores. (p. 64)

De ahí surge la necesidad de tipificar los delitos informáticos, pues su fin supremo es velar por la protección de la información (cuando esta es el fin de una conducta), a diferencia de lo que se denomina por la doctrina como criminalidad informática, donde si bien se utilizan herramientas generadas por las TICs, se usan con la intención de desarrollar otro tipo de conductas que vulneran bienes jurídicos distintos a la información, como podría ser la afectación del patrimonio a través "de estafas o extorsiones comunes, realizadas utilizando la internet" (Posada, 2013a, p. 6).

> Así las cosas, no cabe duda de que existe la necesidad de tipificar penalmente el acceso ilegítimo a sistemas informáticos, pues en el intento de aplicar disposiciones similares mediante el uso de la analogía se presentó un grave problema, pues, "en todos los países resultaba muy difícil aplicar los

> tradicionales tipos penales al acceso no autorizado de información", lo cual, como ya se dijo, genera impunidad de la conducta antijurídica. (Castro, 2008, p.630)

Finalmente como ya se mencionó, con este proyecto de ley se crearon nuevos tipos penales que consisten en las conductas que constituyen delitos informáticos, "con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales, como figuras autónomas frente a los tipos penales tradicionales" (Posada, 2013b, p.4) (Subrayado fuera del texto).

5.2.2.3 Artículo 269A del Código penal "acceso abusivo a un sistema informático".

LEY 1273 DE 2009

CAPÍTULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

> 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 Colombia, 2009, pr. 4). (Ley 1273 de 2009 que modifica Código Penal Colombiano)

Como respuesta a los peligros generados por el hacking, el Estado Colombiano decidió crear este delito autónomo para castigar los accesos abusivos, es decir, aquellas conductas que consisten en una intrusión a un sistema informático pues se ingresa sin autorización e incluso transgrediendo medidas de seguridad del sistema, ya que el sujeto que la realiza se atribuye su control en contra de la voluntad del legítimo titular.

En el mismo sentido doctrinantes han expuesto:

> (...) se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información. (Ojeda, et al., 2010, p.54)

Esta conducta es importante porque además de sancionar el hacking de una manera autónoma sirve de puente para cometer otros delitos, ya que en muchos casos, el acceso es la fase preparatoria para realizar otros ataques contra los sistemas informáticos, los cuales se enmarcan en diferentes tipos penales.

6. Capítulo IV: Elementos del tipo “acceso abusivo a sistema informático”

6.1. Elementos objetivos del tipo.

6.1.1 Sujeto activo.

La estructura del tipo penal analizado, consagra la expresión “El que”, por lo que se trata de un sujeto activo indeterminado, suponiendo entonces que cualquier persona puede llevar a cabo la conducta descrita, pues el tipo penal no reviste de ninguna cualidad especial a su autor. Sin embargo, es posible pensar que para acceder a un sistema informático el autor debe poseer conocimientos avanzados en el tema, de ahí que se tenga la concepción errónea de que este tipo de conductas siempre son realizadas por los llamados *Hackers* conocidos como:

> (…) sujetos que por su alto coeficiente intelectual y su gran habilidad en el manejo de sistemas informáticos, disfrutan creándose retos intelectuales para obtener el acceso a sistemas informáticos protegidos con complejos sistemas de seguridad, con la única intención de demostrar su poder o de estudiar los baches de diferentes sistemas de seguridad. (Díaz, 2012, p.153)

Por consiguiente, respecto del sujeto activo “basta que sea un “intruso” y se cumplan las exigencias jurídicas para ser calificado como autor” (Posada, 2013b, p.8).

Un ejemplo claro de que no solo los hackers son quienes cometen dicha conducta es que incluso quien presta el servicio puede acceder sin la debida autorización del titular a un sistema informático, convirtiendo no sólo su acceso en ilegítimo, sino además cambiando su papel de administrador del sistema al de autor de la conducta punible (Posada, 2013).

Así, en razón del sujeto activo[20] el código penal establece varios agravantes en su artículo 269H:

> "2. Por servidor público en ejercicio de sus funciones" (Congreso de Colombia, Ley 599 de 2000, Art. 269H).

Igualmente cuando el autor sea un funcionario público y cometa la conducta de acceso abusivo a sistema informático en abuso de las funciones que se le han otorgado en razón a su cargo, se justificará dicho aumento a la pena pues de éste se espera un comportamiento ejemplar.

> "3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este" (Congreso de Colombia, Ley 599 de 2000, Art. 269H).

Cuando este agravante enuncia "aprovechando la confianza" se entiende que en un principio el sujeto activo actúa conforme a la confianza que le fue depositada por parte del titular, pero en algún punto sobrepasa los límites en los cuales fue otorgada.

Ahora bien, en cuanto a las que tuvieran "un vínculo contractual" el acceso estaría legitimado en virtud del cumplimiento de una de las obligaciones derivadas del contrato, no obstante el autor decide desbordar el marco contractual.

El abuso de las anteriores relaciones puede darse desde el momento en el que se accede al sistema informático (se desconoce la autorización), o bien tras haber entrado de manera legítima

[20] A diferencia de Colombia, en el Código Penal Francés en el artículo 323-5 y 323-6 además de la pena principal que se le aplica al sujeto activo, se establecen penas accesorias que varían según se trate de una persona natural o jurídica, las cuales por tener una naturaleza diferente a la de los agravantes se aplican siempre que se configure la conducta por alguna de éstas personas y no porque de ellas emanen calidades especiales.

cuando decide mantenerse en el sistema por fuera de los límites otorgados (se excede la autorización).

> 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. (Congreso de Colombia, Ley 599 de 2000, Art. 269H)

Si bien esta circunstancia se plantea como agravante, se advierte de su interpretación armónica que se trata de una pena accesoria, el hecho que el autor tenga la "administración, manejo o control" del sistema informático sin importar la relación de la que se deriven éstas facultades. Sin embargo, una interpretación exegética podria concluir que el legislador considera de mayor gravedad este tipo de relación pues además de aumentar la pena, impone una inhabilidad para ejercer profesiones relacionadas con sistemas de información procesada.

Al igual que el anterior numeral, esta circunstancia se aplica en el momento en que se desconoce o se excede la autorización.

Finalmente resulta importante decir que: "Este tipo penal admite la coautoría y otras formas de autoría, y las diversas formas de participación criminal: (i) determinación y (ii) complicidad" (Posada, 2013, p.8).

6.1.2 Sujeto pasivo.

Puede ser sujeto pasivo del tipo penal, quien resulte ser titular del sistema informático al cual se accedió, ya sea persona natural o jurídica.

De cualquier modo, no hay que dejar de lado que dentro del sistema informático, existen toda una serie de datos e información que no necesariamente pertenece al titular del sistema informático sino a otras personas quienes al ser "titular(es) de los datos personales, sensibles o secretos almacenados en archivos o bases de datos, y cuya intimidad personal se pone en peligro" (Posada, 2013b, p.10) también son sujetos pasivos.

Ya que la redacción del artículo 269A no consagra la calidad de la información de la que se debe ser titular, se entiende entonces que son sujetos pasivos los titulares de cualquier tipo de información contenida en el sistema informático.

6.1.3 Bien jurídico.

La ley denominó su Título VII "de la protección de la información y de los datos" por lo que este es justamente el bien jurídico objeto de tutela. Dicho Título se compone por dos capítulos siendo el primero denominado: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", justamente el que consagró el delito de acceso abusivo a sistemas informáticos.

> Así las cosas, es necesario precisar y explicar en qué consiste el bien jurídico tutelado de la información (almacenada, tratada y transmitida a través de sistemas informáticos), en toda su amplitud, titularidad, autoría, integridad,

> disponibilidad, seguridad, transmisión, confidencialidad e intimidad, sin perjuicio de que con su vulneración, subsidiariamente y en tratándose de intereses colectivos, afecte otros bienes jurídicos (...). (Cámara de Representantes, 2007, pr.7)

¿Cuál es el bien jurídico protegido por el acceso abusivo a sistemas informáticos?

6.1.3.1 De la protección de la información y de los datos.

Del nombre que lleva el Título VII se tiene que el bien jurídico es la "protección de la información y de los datos", sin embargo, esta nominación resulta un tanto vaga, en el entendido que a pesar de evidenciar una intención de protección, no es claro en cuanto a qué aspectos de la información y los datos resultan relevantes para el Derecho Penal.

El Convenio de Budapest al consagrar la necesidad de tipificar los delitos informáticos en los ordenamientos jurídicos de los países parte, expresó: "Delitos contra la Confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos" (Consejo de Europa, 2001, p.4), precisando así el campo de protección de los datos y de la información.

A pesar de que el legislador colombiano le asignó otra nominación al bien jurídico y que el Convenio de Budapest no resulta vinculante para Colombia, la precisión que hace dicho Convenio no es ajena a nuestro ordenamiento jurídico ya que al nominar el primer capítulo de la ley 1273 de 2009 "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" se establece éste como un sub objeto del bien jurídico principal "De la protección de la información y los datos", estableciendo así el alcance de la protección de las conductas que componen dicho capítulo.

Según la doctrina, el ámbito de protección del bien jurídico se delimita por estas tres dimensiones, en el entendido que:

> Esta seguridad en la utilización de los sistemas informáticos de forma más o menos generalizada se manifiesta en la confidencialidad, integridad y la disponibilidad de los sistemas de comunicación e información, y que constituye propiamente el bien jurídico a proteger en la tipificación de conductas de acceso ilícito a sistemas informáticos. La integridad de un sistema informático alude a su utilización con las pertinentes modificaciones del contenido de la información almacenada en el sistema por parte de la/s persona/s autorizada/s. La confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a la/s persona/s autorizada/s. La disponibilidad hace referencia al control sobre la utilización de un determinado sistema por parte de la/s persona/s autorizada/s. (Rueda, 2009, p.187) (Subrayado fuera del texto)

En esta misma línea importantes doctrinantes colombianos como Posada coinciden con el pensamiento de Rueda Martin al expresar:

> Este tipo penal pluriofensivo exige, en primer lugar, la afectación o vulneración del bien jurídico intermedio, público u autónomo de la seguridad de la información y los datos informáticos, con lo cual se sanciona la lesión de la confiabilidad, integridad y la libre disponibilidad directa de los sistemas informáticos y el peligro indirecto de los datos y la información almacenada en ellos. (Posada, 2013b, p.11)

En conclusión, el bien jurídico a proteger mediante la tipificación del delito de acceso abusivo a sistemas informáticos al estar contenido en el capítulo I de la ley en mención, es "la protección de la información y los datos" concretamente en "la confidencialidad, integridad y disponibilidad de los sistemas informáticos y los datos"[21].

Sin embargo al ser un delito pluriofensivo, no se puede desconocer que con la comisión de dicha conducta sea posible vulnerar bienes jurídicos distintos al contemplado en el capítulo I de la ley 1273 de 2009.

¿Cuáles son los bienes jurídicos que pueden llegar a ser vulnerados mediante un acceso abusivo a sistema informático?

A continuación se muestra el análisis de algunos de los bienes jurídicos que pueden resultar afectados por un acceso abusivo a sistema informático.

6.1.3.2 Intimidad, autodeterminación informática y su relación con el bien jurídico tutelado.

Respecto de los bienes jurídicos que pueden verse afectados por un *acceso abusivo a sistema informático,* la doctrina ha expuesto:

> En segundo lugar, el tipo penal exige también la puesta en peligro del bien jurídico personalísimo de la intimidad personal en su modalidad de la intimidad y la autodeterminación informáticas —igualmente considerado como un derecho fundamental de cuarta generación (Anarte Borallo, p. 236)—, para

[21] A diferencia de Colombia, en España no se creó un bien jurídico autónomo sino el código penal consagra el delito de acceso abusivo a sistemas informáticos como aquellos que atentan contra el bien jurídico intimidad, así en el artículo 197 Bis "intrusión informática" el bien jurídico a proteger es la intimidad personal concretamente la privacidad en el ámbito de la informática, así mismo en el acceso del artículo 197.2 sobre "los abusos informáticos sobre datos automatizados relativos a la intimidad" el bien jurídico sigue siendo la intimidad solo que en su dimensión de libertad informática o habeas data.

> evitar potenciales lesiones a los datos de naturaleza privada o semiprivada (Picotti, 2006, pp. 181 y ss.) y a la información informatizada almacenada en el sistema objeto de ataque, mediante acciones ulteriores o manipulaciones informáticas que, más allá, puedan configurar un delito autónomo de interceptación o violación de datos personales (CP, arts. 269 C y F, respectivamente). Por esto, se trata de un bien jurídico colectivo-individual. (Posada, 2013b, p.11)

> Otros han dicho, que este es uno de los delitos que viola el concretamente llamado por los franceses, domicilio informático, de manera que tales acciones violan o van en contra de la intimidad personal, ya que se entrometen en un "lugar" así sea virtual, donde se almacena la información que se pretende proteger. (Márquez, 2002, p.153)

Es decir, mediante la comisión del delito igualmente se puede dar una intrusión en la intimidad personal, resultando entonces útil hacer una breve exposición sobre el derecho a la intimidad, el derecho de la autodeterminación informática y el tratamiento que la Corte Constitucional les ha dado.

Para comenzar, es importante destacar que la intimidad personal se encuentra consagrada en el artículo 15 de la Constitución Política de Colombia, como Derecho fundamental, el cual dispone que: "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar" (República de Colombia, Constitución Política de Colombia, 1991, p.18), planteando "(…) diferentes esferas o ámbitos, como son el personal, familiar, social y gremial, (…), y que están manifestadas concretamente: (...) (vi)

comunicaciones personales; (vii) espacios para la utilización de datos a nivel informático; (...)". (Corte Constitucional de Colombia, Sentencia C-881 de 2014. M.P. Jorge Ignacio Pretel, 2014, p.3).

Así mismo la Corte Constitucional de Colombia (1996) en reiteradas ocasiones se ha referido al derecho en mención, una de estas en la sentencia T-696 de 1996:

> La intimidad, el espacio exclusivo de cada uno, es aquella órbita reservada para cada persona y de que toda persona debe gozar, que busca el aislamiento o inmunidad del individuo frente a la necesaria injerencia de los demás, dada la sociabilidad del ser humano. Es el área restringida inherente a toda persona o familia, que solamente puede ser penetrada por extraños con el consentimiento de su titular o mediante orden dictada por autoridad competente, en ejercicio de sus funciones y de conformidad con la Constitución y la ley. (Corte Constitucional de Colombia, Sentencia T-696 de 1996, M.P. Fabio Morón Díaz, 1996, p.1)

Más adelante, la Corte Constitucional (2008) se pronunció en la misma línea:

> El núcleo esencial del derecho a la intimidad supone la existencia y goce de una órbita reservada para cada persona, exenta del poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural. (Corte Constitucional de Colombia, Sentencia T158A de 2008, M.P. Rodrigo Escobar Gil, 2008, p.8)

De los dos pronunciamientos de la Corte Constitucional se encuentra en común el término "órbita reservada", es decir, que hace parte de la intimidad aquel espacio que se considera privado, en consecuencia toda la información enmarcada por una persona en dicho espacio, también lo será y por su naturaleza estará fuera del dominio público.

De ahí que la Corte Constitucional ha realizado todo un desarrollo jurisprudencial clasificando la información:

> Desde un punto de vista cualitativo en función de su publicidad y la posibilidad legal de obtener acceso a la misma. En este sentido la Sala encuentra cuatro grandes tipos: la información pública o de dominio público, la información semi-privada, la información privada y la información reservada o secreta (Corte Constitucional de Colombia, Sentencia. T-729 de 2002, M.P. Eduardo Montealegre Lynett, 2002, p.15) (Subrayado fuera del texto).

La Corte retomó las anteriores clasificaciones en Sentencia T-559 de 2007, dando las siguientes definiciones:

> (i) pública o de dominio público que puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal; (ii) semi-privada, que por versar sobre información personal o impersonal tiene limitación para su acceso, de tal forma que sólo puede ser obtenida por orden de autoridad administrativa en el cumplimiento de sus funciones; (iii) privada, aquella que por versar sobre información personal o no, y que por encontrarse

> en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones; y finalmente (iv) la información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. (Corte Constitucional de Colombia, Sentencia T-559-07. M.P. Dr. Jaime Araujo Rentería, 2007, pp.3-4)

Se evidencia que dependiendo de la clase de información de que se trate varía la expectativa de intimidad y por lo tanto el tratamiento en términos de protección que el Estado debería darle, es así que sobre la información pública por su naturaleza, como lo dijo la Corte, no existe ninguna clase de reserva, pues es de dominio general y en consecuencia cuando hay una intromisión frente a ésta no se vulnera la intimidad.

Una de las características que reviste a este derecho fundamental es precisamente su disponibilidad, pues es la misma persona al delimitar su órbita reservada quien decide qué hace parte de su intimidad, es así como cierta persona puede volver pública información que otra persona pondría en su dominio privado (Corte Constitucional de Colombia, Sentencia T-552/97. M.P. Dr. Vladimiro Naranja Mesa, 1997).

Dicha característica de la intimidad también permea el campo de las tecnologías y la informática, de esta manera en:

> El daño a la intimidad en el contexto de la informática conviene precisar que el daño que nos ocupa, no es el consistente en el mero procesamiento deficiente de

> la información por la computadora, sino, el que puede derivar de la utilización de la información, por el operador o por cualquier tercero. (González, s.f., p.75)

Vale recordar que la intimidad personal tiene varias clasificaciones, siendo la intimidad informática la que resulta protegida de una manera directa por el acceso abusivo a sistema informático, así la Corte expresa en sentencia C-881 de 2014:

> El derecho a la intimidad plantea diferentes esferas o ámbitos, como son el personal, familiar, social y gremial, todos ellos comprendidos en el artículo 15 Superior, y que están manifestadas concretamente: (...) (vi) comunicaciones personales; (vii) espacios para la utilización de datos a nivel informático; (...) (Corte Constitucional, Sentencia C-881 de 2014, M.P. Jorge Ignacio Pretel, 2014, p.3) (Subrayado fuera del texto)

Finalmente en cuanto a la intimidad informática se habla de la "disponibilidad exclusiva del espacio informático" (Posada, 2013b, p.11) y en consecuencia la expectativa de intimidad que tiene el titular de los datos que allí se consignan.

Todas estas aclaraciones conceptuales se hacen necesarias ya que en el ámbito de lo privado y lo público en la intimidad se encuentra conexidad con la autonomía y el derecho de autodeterminación, los cuales han evolucionado de la mano con la sociedad de la información para llegar a hablar de autodeterminación informática.

Así las cosas:

> La intimidad se encuentra íntimamente ligada a la autonomía. Lo afirmamos, puesto que el hombre goza del derecho a autodeterminarse, derecho previo a cualquier otro derecho dentro de una democracia liberal, permitiendo al hombre determinar cuán grande es su esfera de actos privados y cuán grande es su esfera de actos públicos, pues como se ve, es el hombre el que revelando o limitando la información que aparece de él en bases de datos y demás sistemas informáticos, pueden en teoría establecer cuál será el perfil de su vida que es parte del dominio público y cual es parte de su dominio privado. Solo a partir de la autonomía que su condición humana le concede, el hombre puede o no ampliar su privacidad. (Márquez, 2002, p.104)

Esta misma autonomía que posee cada persona para decidir acerca de qué es público y qué es privado en su vida, se refleja también en la posibilidad de decidir quién, cómo y cuándo tiene acceso a su información. Es de allí de donde nace entonces el derecho a la autodeterminación informática o informativa.

> El derecho de autodeterminación informativa consiste en la posibilidad que tiene el titular de los datos personales de controlar quiénes serán destinatarios de éstos y qué uso les darán, y se ejercita genéricamente a través de los derechos de acceso, rectificación y cancelación. Además, ofrece una textura que resulta acorde con los modernos desafíos informáticos, puesto que, abandonando el concepto de intimidad como libertad negativa, permite avanzar hacia una fase activa del proceso de circulación de la información personal brindando protagonismo al interesado al posibilitarle el ejercicio de un

> adecuado control sobre la misma. (Bazan, 2005, p.11) (Subrayado fuera del texto)

Bajo el mismo análisis, la posición de la Corte Constitucional T-552/97 varió al determinar como autónomo el derecho a la autodeterminación informática cuando expresó:

> No obstante, y a pesar de que en determinadas circunstancias el derecho a la intimidad no es absoluto, las personas conservan la facultad de exigir la veracidad de la información que hacen pública y del manejo correcto y honesto de la misma. Este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad, que se ha denominado como el derecho a la "autodeterminación informativa. (Corte Constitucional de Colombia, Sentencia T-552/97. M.P. Dr. Vladimiro Naranja Mesa, 1997, p.5)

Este derecho implica tanto tener conocimiento acerca de los datos como el derecho a la transparencia en su procesamiento, el cual se refleja no solo en su almacenamiento -independientemente de su forma, sea manual o electrónica-, sino en su obtención y demás etapas del tratamiento de datos (Bazán, 2005).

No obstante en la Jurisprudencia colombiana al hablarse de autodeterminación informática la Corte lo asocia "al derecho de Hábeas Data", en sentencia SU 082/95 señaló el alto tribunal:

> ¿Cuál es el núcleo esencial del habeas data? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica.

> La autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales.
>
> Y se habla de la libertad económica, en especial, porque ésta podría ser vulnerada al restringirse indebidamente en virtud de la circulación de datos que no sean veraces, o que no haya sido autorizada por la persona concernida o por la ley. (Corte Constitucional de Colombia, Sentencia SU 082/95. M.P. Jorge Arango Mejía, 1995, p.8)

Por lo tanto si bien la Corte ha asociado estos conceptos, mantiene la autodeterminación informática como una de las dimensiones del Habeas Data, entonces no se puede hablar de una excluyendo la otra. Se hace necesario poner de presente que el derecho de Hábeas Data está consagrado en la Constitución Política como derecho fundamental y la Corte en Sentencia T-552/97 se refirió a éste en los siguientes términos:

> El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de "*conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*". (Corte Constitucional de Colombia, Sentencia T-552/97. M.P. Dr. Vladimiro Naranja Mesa, 1997, p. 7) (Subrayado fuera del texto)

Frente a este mismo tema Bazán ha mencionado:

> Es conveniente independizar conceptualmente el derecho de autodeterminación informativa, como bien jurídico protegido por el hábeas data, de derechos personalísimos tales como el de intimidad, al honor o a la imagen, y aun a la identidad, sin desconocer que tienen puntos de confluencia en tanto el de autodeterminación informativa, más allá de su dimensión sustancial, ofrece una valiosa vertiente instrumental –interalia– de aquel conjunto de derechos. (Bazán, 2005, pp.110-111)

En cuanto a las precisiones que hacen tanto la Corte como el autor Bazán, se encuentra que coinciden respecto que no se puede confundir el derecho de autodeterminación informativa con el derecho a la intimidad a pesar de que tengan puntos de convergencia, por otro lado mientras la Corte establece que el derecho de autodeterminación integra el núcleo esencial del Habeas Data, para Bazan es un bien jurídico protegido por este último.

Finalmente la Corte ha precisado que el Habeas Data se da respecto de los "datos personales", es decir, aquella información concreta que se puede vincular a una persona natural o jurídica, contenidos en las bases de datos. En Sentencia T-729 de 2002 afirmó:

> El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales. (Corte Constitucional, Sentencia. T-729 de 2002, M.P. Eduardo Montealegre Lynett, 2002, p.8)

Es decir, el Habeas Data tiene por objeto regular y controlar la relación entre el titular de los datos y los encargados de la administración de las bases en las que se depositan.

Cabe destacar que en ocasiones anteriores, la Corte Constitucional expresó que las personas jurídicas gozan de Hábeas data al exponer que también gozan del derecho de autodeterminación informática pues:

> **Sujeto activo** del derecho a la autodeterminación informática es toda persona, física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado. El **sujeto pasivo** es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales. (…). (Corte Constitucional de Colombia, Sentencia SU 082/95. M.P. Jorge Arango Mejía, 1995, p.8)

A partir del análisis realizado podemos concluir que el bien jurídico que se tutela con los delitos informáticos, y en este caso con el acceso abusivo a sistemas informáticos, es "la confiabilidad, integridad y la libre disponibilidad directa de los sistemas informáticos y el peligro indirecto de los datos y la información almacenada en ellos". (Posada, 2013b, p.10). (Subrayado fuera del texto).

Lo anterior armonizando lo expuesto en el Convenio de Budapest, los aportes que la doctrina ha hecho al respecto y la legislación colombiana, ya que estos son los aspectos a proteger de la información y los datos.

Sin embargo, como se pudo observar en este estudio, dicho bien jurídico tiene naturaleza de intermedio, de ahí que en algunas ocasiones su tutela trae como consecuencia la protección

indirecta de otros bienes jurídico-penales como la intimidad y la autodeterminación informática (cuando el sistema informático al que se accede o en el que se mantiene contiene datos de carácter personal, y como consecuencia de ese acceso se da la efectiva puesta en peligro de dichos bienes jurídicos), pero no por esto asumen la categoría de bien jurídico principal tutelado por el acceso abusivo a sistemas informáticos, el cual fue creado con la finalidad de proteger de forma autónoma los riesgos generados por la sociedad de la información.

Sobre este mismo punto Márquez (2002) señala:

> Además el acceso abusivo a sistemas informáticos no afecta la intimidad sino en contados casos, como por ejemplo cuando se introduce en un sistema de información en el que se almacena la hoja clínica o historia clínica de los pacientes, o cuando se accede al sistema informático o computador personal que tiene una persona para su uso personal, su redacción de cartas, etc. (p.153)

Por lo tanto, en concordancia con lo consagrado en el artículo 269A se exige la lesión o puesta en peligro de la confidencialidad, disponibilidad e integridad de los datos y el sistema informático.

6.1.4 Objeto sobre el que recae la conducta.

Se trata del objeto material sobre el cual se concreta la acción que el tipo penal enmarca, es así como en el caso del acceso abusivo a un sistema informático cuando en su tipificación se consagra "(...) acceda en todo o en parte a un sistema informático protegido o no con una medida

de seguridad" (Subrayado fuera del texto), se pone de presente que el objeto material es el sistema informático[22].

Teniendo en cuenta lo anterior, resulta conveniente traer nuevamente a colación el concepto de sistema informático, desde un ámbito técnico como lo es la propia ciencia informática, expuesto en el Diccionario de Informática e Internet de Microsoft (como se citó en Castro, 2011):

> La configuración que incluye todos los componentes funcionales de una computadora y su hardware asociado. Un sistema microinformático básico incluye una consola o unidad del sistema con una o más unidades de disco, un monitor y un teclado. Otros elementos hardware adicionales, denominados periféricos, pueden incluir dispositivos tales como una impresora, un módem y un ratón. El software no se suele considerar parte de un sistema informático, aunque el sistema operativo que se ejecuta sobre el hardware se denomina software del sistema. (p. 632)

Sin embargo, para efectos del delito objeto de estudio, los instrumentos internacionales y la doctrina lo han definido en los siguientes términos:

El Convenio de Budapest lo definió como, "se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa" (Council of Europe, 2011, p.4).

[22] A diferencia de la consagración que realiza España, en el artículo 1972 de su código penal, el tipo penal Colombiano no incluye los sistemas telemáticos.

Posada (2013b) en su texto el delito de acceso abusivo a sistemas informáticos, lo concibe así, "entendido como un dispositivo o un grupo de dispositivos informáticos individuales interconectados entre sí que realizan acciones de tratamiento, procesamiento y almacenamiento automático de datos" (p.13).

En cuanto al objeto sobre el cual recae la conducta del acceso, la Ley 1273 de 2009 no establece que comprende un sistema informático o que se debe entender por éste ni tampoco el ordenamiento lo hace, en este sentido no existe unidad respecto de dicho concepto. Razón por la cual el legislador debe estandarizar estas definiciones y determinar para efectos del delito que se entiende por un sistema informático con el fin de evitar lagunas, analogías o interpretaciones erróneas ya que siendo éste el objeto sobre el que recae la conducta de acceso o mantenimiento, debe ser preciso para que el operador judicial pueda determinar cuándo se configura el delito.

Sin embargo, la doctrina ha hecho ciertas precisiones, una de ellas la de Posada (2013b) quien advierte que el objeto inmaterial determinable es el sistema informático en un sentido general, y además incluye en un sentido concreto el software (tanto el sistema operativo como aplicativos), ya que es el que permite procesar las instrucciones para que opere el sistema y así mismo procesa su contenido, como los datos que se encuentran en ficheros o archivos.

De esta manera se protege principalmente el sistema informático[23] y de forma indirecta todo lo que éste contenga.

[23] A diferencia del ordenamiento colombiano, El código penal italiano, en su artículo 615-ter establece como objeto sobre el cual recae la conducta no sólo los sistemas informáticos sino también los telemáticos.

Así mismo cuando el delito expone “en todo o en parte a un sistema informático” dispone que basta con el acceso a alguna fracción de éste, ya sea a alguna aplicación, archivo, o base de datos, de las muchas por las cuales esté conformado.

En cuanto a este mismo tema Márquez (2002), se refiere al objeto material como:

> La conducta va dirigida a la protección de los datos de los sistemas informáticos. Pero una visión más estricta del problema advierte que la protección que se hace no es del sistema informático en general, sino de una parte de dicho sistema, es decir, los mecanismos de seguridad que permiten o restringen el acceso a tal sistema. es en este momento cuando la conducta se tipifica, ya que el objetivo no es proteger al sistema en sí, el objetivo es proteger los mecanismos que permiten o restringen el acceso al sistema. (p.164) (Subrayado fuera del texto)

Entendiendo que la parte sobre la que en realidad recae la acción descrita en el tipo penal son los mecanismos de seguridad del sistema informático, porque son estos los que resultan vulnerados por el hacker al acceder al sistema; se debe aclarar que Márquez hizo este aporte en vigencia del artículo 195 del Código penal derogado por la ley 1273 de 2009 y que hoy el delito contempla la posibilidad de que el acceso sea a un sistema con o sin medida de seguridad, en consecuencia el objeto se amplía a todo el sistema informático.

En cuanto a las medidas de seguridad concebidas como:

> (…) los mecanismo utilizados para proteger los datos y la información que se encuentra previamente almacenada y de acuerdo a los parámetros legales es de

> uso exclusivo del titular de la misma. Por ello, la Medida de Seguridad Informática, también conocida como barrera de seguridad es cualquier acción, objeto o sistema que se aplique para mantener la seguridad de un sistema informático (...). (Paloma, 2012, p.57)

El hecho de consagrar en la tipificación del artículo 269A de la misma ley "protegido o no con una medida de seguridad" hace que se excluya como elemento del tipo y se vuelve irrelevante si el sistema informático cuenta o no con dicha protección.

6.1.5. Verbo rector.

El tipo penal consta entonces de dos verbos rectores, los cuales se pueden observar en la tipificación de la conducta cuando se consagra "(...) acceda en todo o en parte a un sistema informático… o se mantenga dentro del mismo **en contra de la voluntad de quien tenga el legítimo derecho a excluirlo**" (Congreso de Colombia, Ley 1273 de 2009, pr.4). (Subrayado y negrilla fuera del texto).

Siendo entonces "acceda" o "mantenga" los verbos rectores que configuran la conducta, puede decirse que se trata de un tipo penal mixto ya que está compuesto por varias conductas, y alternativo pues basta con que se ejecute cualquiera de éstas para que se configure.

En palabras de Alberto J. Rey Boek y Carlos A. Núñez de León (como se citó en Castro 2011),

> De igual forma pueden clasificarse dentro de los considerados alternativos, puesto que para su comisión son posibles diferentes tipos de acciones, que actualizan los elementos del tipo penal ya sea mediante el acceso en todo o en

> parte a un sistema informático; o estando dentro de este, se mantenga en el mismo sin autorización del titular del bien jurídico o por fuera de lo acordado entre sujeto activo y pasivo de la acción típica, siendo irrelevante si el sistema informático se consagra protegido o no con una medida de seguridad. (p.623)

El verbo "acceder" consiste en "Entrar en un lugar o pasar a él" (Real Academia Española, 2017, pr. 3), para efectos del delito "no solo implica abrir y entrar sino también atravesar" (Posada, 2013b, p.14). Teniendo en cuenta que el acceso es a un sistema informático, este es virtual más no físico, entonces:

> Se realiza mediante la digitación de una serie de comandos con los cuales se ordena a un sistema informático ejecutar una determinada operación y esta, respondida en sentido positivo, le permite al sujeto solicitante utilizar en todo o en parte sus recursos. (Posada, 2013b, p.14)

De esta manera, con el acceso se concreta la vulneración del sistema y esto es lo reprochable por el Derecho penal, ya que se afecta el sistema cuando el hacker avanza hasta un nivel no permitido y llega incluso a neutralizar o controlar el sistema que está atacando (Posada, 2013b). Todo lo anterior a través de "Actividades que usualmente son clandestinas, rápidas y para las cuales se emplean sofisticados programas y técnicas de evasión y eliminación de rasgos que impidan descubrir la "trazabilidad" de la injerencia en el sistema" (Posada, 2013b, p.14).

En palabras de la doctrina:

> El delincuente (s) virtual (s) sin recibir el asentimiento necesario para poder ingresar en una red de información automatizada, o poseyendo el permiso o la

> potestad para el ingreso, pero por fuera de los parámetros que se han acordado, se introduce en él, es en este evento cuando se transgrede la normatividad penal sustantiva. (Paloma, 2012, p.72)

Así el acceso se convierte en abusivo cuando se da sin el consentimiento del sujeto pasivo, ya sea porque éste no dio su autorización o porque quien accedió lo hizo en contravía a unas condiciones previamente acordadas.

En cuanto a la otra conducta contemplada en el tipo penal, el verbo "mantener" (Real Academia Española, 2017, pr.3) se refiere a los casos en que el acceso al sistema informático en un principio se realiza de forma legítima (con autorización del respectivo titular) o aquel que se da de forma fortuita, no obstante ambos se tornan ilegítimos cuando el sujeto activo permanece en el sistema en contra de la voluntad del titular, "Permanencia que debe darse con la conciencia de que no se está autorizado y que ello constituye un abuso informático" (Posada, 2013b, p. 15).

Pues bien, si el verbo rector se traduce en mantenerse en el sistema siendo consciente de que no se tiene autorización para estar allí es de entenderse que la ejecución de esta conducta termina en el momento en el que el sujeto activo se retira del sistema, ya sea por voluntad propia o porque quién tiene el derecho a excluirlo, lo hace, en este sentido se trata de un delito de ejecución permanente.

Respecto de este supuesto a diferencia de Italia[24], Colombia en la redacción del artículo 269A no establece si el mantenimiento debe ser contra la voluntad expresa o tácita del titular, dada la forma en que está consagrado el delito en nuestro ordenamiento se trata de una manifestación que

[24] Código penal italiano artículo 615-ter, cuando consagra que el acceso o mantenimiento al sistema sea en contra de "la voluntad **expresa** o **tácita** de quien tenga el derecho a excluirlo" (Negrilla fuera del texto)

puede ser tácita, pues el hecho de que esté consagrado como prohibición o delito el no poderse mantener en un sistema informático sin autorización, significa que este tipo de conducta está proscrita y que el sujeto activo debe salir del sistema so pena de asumir la sanción penal respectiva.

Por lo anterior el delito en esta modalidad conductual, está en la acción de mantenerse de manera ilegítima, ya sea porque excedió la autorización dada o porque accedió de manera fortuita y continuo en el sistema informático sin consentimiento del titular, así no resulta lógico contemplar la hipótesis de que el sujeto pasivo advierta expresamente al sujeto activo lo que ya está diciendo la ley y el ordenamiento, que no tiene autorización para estar allí, que está excluido del acceso y del uso de dicho sistema.

Sin embargo, para no despertar dudas al respecto, el legislador podría precisar en este punto al incluir en el tipo penal el que "se mantenga dentro del mismo en contra de la voluntad ya sea expresa o tácita de quien tenga el legítimo derecho de excluirlo".

Finalmente, es importante poner de presente que sin importar cuál sea la conducta que se ejecute, ésta siempre debe ir en contra de la voluntad del titular quien tiene el derecho a decidir quién accede y quién no, de ahí que el comportamiento se predique abusivo.

6.2 Aspectos subjetivos del tipo

6.2.1 Dolo.

Al no contemplarse este tipo penal dentro de los que admiten la modalidad de culpa, se tiene entonces que este se debe dar solo de forma dolosa. El dolo entonces se configura "cuando el

agente conoce los hechos constitutivos de la infracción penal y quiere su realización" (Congreso de Colombia, Ley 599 de 2000, Art. 22, p.9) así el sujeto activo debe saber que la conducta que realiza es un acceso abusivo a un sistema informático (en cualquiera de las dos modalidades) y aun así querer su concreción.

Así mismo, el dolo también comprende "la conducta cuando la realización de la infracción penal ha sido prevista como probable y su no producción se deja librada al azar" (Congreso de Colombia, Ley 599 de 2000, Art. 22, p.9). En cuanto este tipo de dolo resulta compleja su aplicación al caso concreto, pues al tratarse de un delito de mera conducta (donde no se separa la acción del resultado con facilidad), cuando se toma la decisión de llevar a cabo la acción ya se tiene conocimiento de que el resultado será el descrito por el tipo, por lo tanto no existe la posibilidad de dejar librado al azar dicho resultado, pues éste se da por decisión autónoma frente a un acto que lleva a su concreción.

Teniendo en cuenta lo anterior, éste supuesto de hecho resulta ilusorio.

No obstante, un caso como el acceso de manera fortuita, podría en supuestos hipotéticos, dar lugar a que se invoque una actividad carente de dolo, tesis que será superada con la aplicación del dolo eventual, aunque se reitera sería un supuesto remoto.

6.2.2 ¿El tipo penal exige una finalidad especial?

El tipo penal descrito no incluye como elemento en su redacción que la conducta se despliegue con una finalidad específica, por lo tanto se evidencia que al legislador no le interesó si detrás del acceso había un ánimo especial más allá del dolo[25].

Frente a este tema se ha debatido en la doctrina si el tipo penal debería contener una finalidad especial, pues se castigan conductas que no poseen una finalidad criminal como lo es el "hacking blanco" el cual "se presenta cuando jóvenes perpetran actos de acceso no autorizados a sistemas informáticos con el propósito de demostrar la vulnerabilidad del sistema, por motivos de curiosidad o desafío intelectual" (Posada, 2013b, p.25). Sería conveniente definir una finalidad ya que de esta forma se reducen los escenarios de aplicación del tipo y se evita cobijar riesgos irrelevantes para el Derecho penal.

En el mismo sentido, frente al bien jurídico intimidad que puede resultar lesionado, la doctrina también considera se debe exigir una finalidad, pues:

> El peligro contra la reserva o intimidad de los datos no parece satisfecho con el simple acceso o ingreso del "intruso", sin que tal conducta se acompañe de una finalidad que demuestre el deseo de ejecutar conductas posteriores dentro del sistema, contra este o sobre los datos o la información sensible del titular del bien jurídico allí almacenada (como lo demuestra la mayoría de los tipos penales de lege ferenda) (Posada, 2013b, p.25).

[25] A diferencia de Colombia, el código penal de Portugal si establece como elemento del tipo una finalidad cuando consagra en su artículo 7 que el acceso se de con "(...) *la intención de obtener, para sí o para otro, un beneficio o ventaja ilegítimos".*

Sin embargo, a pesar de que el tipo no contempla como un elemento necesario alguna finalidad, se establece una circunstancia de agravación cuando el delito se da con una finalidad específica, consagrada en el numeral 6 del artículo 269H, cuando el sujeto realice la conducta de acceso o mantenimiento "con fines terroristas o generando riesgos para la seguridad o defensa nacional" (Congreso de Colombia, Ley 599 de 2000, Art. 256, p.95).

Finalmente, hecho el análisis de cada uno de los elementos del tipo, se puede concluir que el delito de acceso abusivo a sistema informático es la puerta para cometer otro tipo de conductas contempladas por diferentes tipos penales, tal como lo afirma Márquez (2002):

> Dentro de los delitos informáticos este parece ser el de mayor ocurrencia, puesto que para realizar la mayoría de las conductas mediante computadoras es necesaria la introducción abusiva a sistemas informáticos. Así, siempre concursará con otros delitos informáticos, ya que se convierte en principal elemento de modus operandi utilizado para la comisión de los demás delitos. (p. 154)

7. Capítulo V. Aspectos referidos a la antijuricidad

Debe rescatarse tras el estudio de la tipicidad, como se evidenció en la bibliografía aquí citada, que si bien Posada es uno de los mayores exponentes en Colombia sobre la materia, en sus artículos no encontramos un profundo desarrollo sobre "la antijuricidad", ya que su investigación se enfoca más en la tipicidad, la culpabilidad y los concursos que pudieren llegar a darse entre el delito de acceso abusivo informático y otros delitos.

No obstante en su investigación advierte ciertos vacíos y problemas que presenta dicha tipificación.

En este sentido, expone un punto muy interesante el cual toca el objeto de estudio de esta investigación -aunque no es un análisis tan profundo como el que se pretende hacer aquí-, al referirse al proyecto legislativo No. 263 del 2011 Senado y 195 del 2011 Cámara de Representantes, "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones" (Congreso de Colombia, Ley 1621 de 2013.pr.1) así en su artículo 40 propone la modificación del artículo 269A del C.P, en los siguientes términos (Posada, 2013b):

> "ART. 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 medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el derecho legítimo a excluirlo, incurrirá en pena de prisión de cinco (5) a ocho (8) años y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. La pena se aumentará el

> doble cuando el acceso abusivo beneficie a miembros de grupos armados al margen de la ley u organizaciones de crimen organizado, o cuando el acceso abusivo beneficie a gobiernos extranjeros" (Posada, 2013b, p. 5).

En dicho artículo cuestiona, en primer lugar, la pena que se pretende imponer ya que sobrepasa los límites sugeridos por los estándares internacionales, esto es, penas de máximo 5 años de prisión, teniendo como consecuencia una maximización punitiva (Posada, 2013b). Por otro lado en cuanto al agravante expone los problemas que en términos de antijuricidad suscitaría pues:

> Al recoger parcialmente la figura del ciberespionaje (acceso a los sistemas que almacenan datos de inteligencia y contra inteligencia), fue construida a partir de un resultado de peligro, absolutamente gaseoso (beneficie), que sin duda constituye una cláusula general que vulneraba el principio de legalidad (Posada, 2013b, pp.5-6) (Subrayado fuera del texto).

El proyecto de ley fue sancionado como la Ley 1621 de 2013 y posteriormente declarada inexequible en Sentencia C-540 del 2012 de la Corte Constitucional, por ir en contravía del artículo 158 de la Constitución Nacional, sobre el principio de unidad o relación de materia de las leyes o conexidad sustancial (Posada, 2013b). Sin embargo, esto resulta interesante pues se empieza a evidenciar la preocupación en cuanto a si la redacción de este tipo penal permite satisfacer efectivamente el principio de lesividad.

En este orden de ideas:

> "La difícil vigencia de esta figura delictiva demuestra la compleja y enorme improvisación legislativa que ha rodeado la regulación de estas modalidades criminales en Colombia, que buscan prevenir riesgos masivos y continuos que puedan afectar el funcionamiento confiable y el uso debido de los sistemas informáticos. (Posada, 2013b, pp.5-6)

De esta manera y dados los vacíos que deja la tipificación de este delito, realizamos el estudio desde la antijuricidad, pues el ejercicio legislativo además de establecer como tipos penales aquellas conductas generadoras de riesgo en la sociedad, debe velar porque dicha tipificación:

1. Cumpla con la finalidad para la cual fue creada.

2. Permita hacer un juicio en el que se concluya que existe antijuricidad no solo formal sino material en la conducta consagrada.

Con lo anterior se debe reflejar que el Derecho penal proscriba aquellas conductas que efectivamente resulten reprochables.

7.1 Antijuricidad del Acceso Abusivo a Sistema Informático.

"Una vez verificada la tipicidad de una conducta, el intérprete debe, para lograr la punibilidad de la conducta, determinar la antijuricidad de la misma para luego establecer la culpabilidad" (Arrubla, 2008, p. 329).

El ordenamiento jurídico Colombiano define la antijuricidad en el entendido que: "Para que una conducta típica sea punible se requiere que lesione o ponga efectivamente en peligro, sin justa causa, el bien jurídico tutelado por la ley penal" (Congreso de Colombia, Ley 599 de 2000,

Art. 11, p. 5). Frente a esta definición se debe precisar según la doctrina que el Código Penal colombiano contempla la existencia de la antijuricidad desde el punto de vista formal y material (Sampedro, 2008).

Dicho lo anterior, a continuación expondremos cada uno de los ámbitos que conforman la antijuricidad y su análisis en el delito de acceso abusivo a sistemas informáticos, para determinar la antijuricidad del mismo.

Respecto de la antijuricidad formal consiste en "la contrariedad entre la acción y el ordenamiento jurídico" (Arrubla, 2008, p. 329), la cual se refleja en el hecho que el autor realiza la conducta descrita por el tipo penal a pesar de que está proscrita expresamente por el ordenamiento jurídico.

Lo anterior se evidencia en el delito de acceso abusivo a sistema informático ya que está consagrada como un delito en el artículo 269A de la ley 599 de 2000 adicionado por la ley 1273 de 2009, en consecuencia quien realice las acciones descritas en el tipo penal estaría desplegando una conducta contraria a Derecho.

En cuanto a la antijuridicidad material, se entiende como "la conducta que lesiona o pone en peligro efectivamente el bien jurídico penal" (Sampedro, 2008, p.330). Entonces, no se habla de cualquier tipo de lesión o puesta en peligro, sino aquellos que tengan la virtualidad de afectar el bien jurídico protegido de manera grave (Sampedro, 2008). Es por esta razón, que:

> De trascendental importancia resulta la inclusión de la expresión "efectivamente" que califica la puesta en peligro, contenida en el artículo 11 de la Ley 599 de 2000, pues normativamente, haciendo caso a la jurisprudencia

> constitucional, se acaba con la posibilidad de presumirlo, presunción que se hace más común, a pesar de su inconstitucionalidad, en tratándose de acciones generadoras de peligros abstractos. (Sampedro, 2008, p.330)

Al hablar sobre la antijuricidad material debemos indiscutiblemente determinar si se satisface o no el principio de lesividad del bien jurídico, de ahí que para hacer un adecuado análisis resulte necesario fijar el alcance de dicho principio.

En primer lugar hemos de recordar que el principio de lesividad surgió con la intención de limitar el poder estatal, separando así definitivamente la moral del Derecho penal. Y que de su campo de protección se derivan dos garantías fundamentales para este último, como lo señala Sánchez (2013):

> En cuanto a la primera de ellas, está sustentada en la exigencia que, la construcción de conductas delictivas, es legítima siempre que el tipo penal, este sustentado sobre la tutela de bienes jurídicos relevantes para el derecho penal con lo cual se indica, que la tipificación de conductas, que no resguarden bienes jurídicos, afectan la dimensión del principio de lesividad, el cual está estrechamente vinculado, a los principios de fragmentariedad y subsidiariedad del derecho penal, que lo circunscriben a la última forma de intervención .
>
> La restante dimensión del principio de lesividad, está orientada ya al aspecto de punición, y desde este ámbito, la mera infracción normativa no supone ya la concurrencia de un injusto penal, de ahí que, no es viable imponer penas o medidas de seguridad, cuando la conducta transgresora de una norma jurídico penal, ni siquiera ha puesto en riesgo al objeto de protección, es por ello que, el

> principio de lesividad no sólo se colma con el desvalor de acción, sino que se requiere también la concurrencia del desvalor de resultado por lo menos en grado de peligro. (pp. 484-485)

Es decir, para que una conducta además de ser típica sea antijurídica desde el punto de vista material debe satisfacer el principio de lesividad, en consecuencia, debe lesionar o poner en riesgo efectivamente el bien jurídico.

Esto resulta de suma importancia ya que limita la facultad que tiene el Estado a la hora de hacer punible una conducta en el ordenamiento jurídico, evitando así la maximización del Derecho penal:

> [y] los abusos reales que el poder penal puede ocasionar, al desarrollar sus políticas de intervención, respecto de los conflictos sociales que se desarrollan en el tejido social, de ahí que, mediante el principio también denominado de objetividad se pretende encauzar el poder penal, hacia la solución exclusiva de la conflictividad social que genere unas consecuencias de dañosidad también social, con lo cual se tiende a neutralizar las distorsiones de la política penal, para hacerla derivar en aspectos meramente moralizantes o instrumentales respecto de otro tipo de políticas públicas, que pretendan impulsarse pero que no están asociadas a la defensa de bienes jurídicos (...). (Sánchez, 2013, pp.491-492)

Vista la necesidad de que las conductas contempladas como delitos deben satisfacer los criterios en mención, ponemos de presente el artículo 269A.

> 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 (...). (Congreso de Colombia, Ley 599 de 2000, Art. 269, p.94)

En este análisis es importante recordar que el bien jurídico que se tutela por este delito es la protección de los datos y la información, y específicamente la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Además aclarar que el tipo penal es considerado un delito de mera conducta[26]:

> ... un delito de mera actividad, es decir, "... aquellos en los que la realización del tipo coincide con el último acto y por lo tanto, no se produce un resultado separado de ella"; en otras palabra, no se requiere que "la acción vaya separada de la causación" de un resultado separable espacio-temporalmente de la conducta", por lo cual es claro que ya sea al momento de acceder al sistema informáticos o cuando se mantenga dentro de él, se está subsumiendo la acción en el resultado descrito en el tipo penal. (Castro, 2008, p.633)

Entonces no se exige un nexo de causalidad entre la acción realizada por el sujeto activo y el resultado obtenido, no obstante sí debe haber una relación entre las acciones que el sujeto activo le ordene al sistema que ejecute y la eficaz respuesta que se obtiene (Posada, 2013b).

[26] El código penal francés en su artículo 323-7 admite la tentativa frente al delito de acceso abusivo a sistema informático, a diferencia de Colombia ya que por no tratarse según el ordenamiento de un delito de resultado difícilmente se configurará una tentativa.

Posada (2013b) define esta relación como el "nexo de naturaleza lógica" el cual consiste en:

> Determinar la existencia de un diálogo informático entre el autor y el sistema informático, que obedezca a la interacción input-output propiciada por las instrucciones electrónicas imputadas al sistema por el sujeto activo y respondidas por la máquina conforme al tratamiento de los datos o al software correspondiente, según el propósito del autor. (p.23)

Por lo anterior, además de verificar dicho nexo, se debe constatar que el sujeto activo si tenía control sobre las instrucciones dadas al sistema (Posada, 2013b).

En consecuencia, sólo cuando se da ese nexo de naturaleza lógica, realmente se podría poner en riesgo el bien jurídico que se tutela, es decir la protección de los datos y la información a través de la afectación de la disponibilidad, la integridad y seguridad de los sistemas informáticos. Al tratarse entonces de una posibilidad, a pesar de que se verifique dicho nexo, no siempre se va a concretar en la vulneración del bien jurídico, por lo tanto este estudio se debe realizar según el caso concreto.

Por otro lado el tipo penal se encuentra cobijado dentro de los tipos penales de peligro, ya que para su comisión no necesita que efectivamente se lesione el bien jurídico sino que basta con la sola puesta en riesgo, lo cual se traduce en la disponibilidad que tiene el sujeto activo cuando accede al sistema informático, es decir, "Peligro verificable y concreto que existiría cuando el sujeto tenga "la posibilidad fáctica —al menos un instante— de obtener servicios o de disponer de la información existente y retirarla del mismo […]" (Posada, 2006, citado por Posada, 2013b, p. 24).

Es importante resaltar que dentro de los delitos de peligro se ha construido una clasificación que distingue los delitos de peligro abstracto en donde "(…)*no es necesaria la verificación del daño causado en el caso concreto*, sino que el mismo se presume" (Bernate, 2006, p. 48-49) y concreto donde la acción "(…) tiene como atributo la posibilidad efectiva de lesionar determinado bien jurídico, la cual a su vez debe determinarse desde una perspectiva *ex ante* y se convierte en la verdadera y concreta puesta en peligro de un interés tutelado." (Cita, 2010, p.16-17), así la conducta del mero acceso en sí misma no es riesgosa sino que debe ir acompañada de dicha disponibilidad para que efectivamente se tenga como resultado la puesta en riesgo del bien jurídico, por lo que no se puede considerar un delito de peligro en abstracto.

Por lo tanto:

> Teniendo en cuenta que este tipo de presunciones de iure en los tipos de peligro son esencialmente desproporcionadas y lesivas de garantías fundamentales como la ofensividad material, resulta necesario reinterpretar la figura como un delito de peligro en concreto (CP, art. 11), en el entendido de que se requiere verificar un peligro efectivo contra los bienes jurídicos protegidos por la norma penal. (Posada, 2013b, p.12)

Ahora bien, con el simple "acceso o mantenimiento" ¿se vulnera o pone en riesgo efectivamente el bien jurídico tutelado?

Al hacer un estudio somero, se encuentra que si una persona accede o se mantiene dentro de un sistema informático sin autorización del propietario de éste o de la información allí contenida, se pone en riesgo el bien jurídico protegido. Esta afirmación se ve reflejada al menos en:

La confidencialidad, ya que los datos o información están al alcance de una persona que no ha sido autorizada, o que está por fuera de los límites establecidos en un momento y de una manera distinta para la cual fue autorizada.

La integridad, pues en el momento que la persona accede o se mantiene en el sistema, deja abierta la posibilidad para que la información resulte modificada o alterada por quien accede sin dicha autorización.

Y la disponibilidad, dado que, como consecuencia de llevar a cabo los verbos rectores se puede obstruir el sistema evitando así que su legítimo titular acceda en el momento que lo desee, así mismo restringir su disponibilidad para que no se lleven a cabo las tareas ordenadas por el titular.

> De esta manera cuando un hacker penetra ilícitamente en un sistema informático ajeno, tanto si se han infringido medidas de carácter técnico como si no ha sido así, se encuentra en un espacio, el propio sistema, en el que su integridad se ha visto afectada porque la sola entrada y el consiguiente uso del sistema da lugar a modificaciones en los datos del mismo, junto con las alteraciones de tales datos para intentar borrar los rastros que pudieran identificarles. Asimismo la confidencialidad del sistema se ve afectada si se utiliza por parte de una persona que no está autorizada. Finalmente la disponibilidad del sistema se afecta cuando penetra una persona no autorizada. Se puede constatar que en estos supuestos de accesos ilícitos a un sistema informático se vulnera el bien jurídico expuesto con independencia de las

> ulteriores finalidades que haya perseguido el hacker con tales entradas. (Rueda, 2009, p.187) (Subrayado y negrilla fuera del texto)

En este punto se debe tener en cuenta, que tal como está redactado el artículo 269A del Código penal, el simple acceso o mantenimiento está exponiendo con alto potencial, la lesión del bien jurídico, por lo cual se considera como ya se dijo, un delito de peligro concreto, pues lo mínimo que exige esta clase de tipos penales es la puesta en peligro del bien jurídico tutelado. Sin embargo, se debe aclarar que en aras de satisfacer el principio de lesividad y antijuricidad material, debe tratarse de la "efectiva" puesta en peligro.

Así las cosas, en cuanto al acceso abusivo a sistema informático es importante señalar que se pone "efectivamente" en riesgo la confidencialidad, integridad y disponibilidad de los datos y del sistema informático, cuando del acceso o mantenimiento se deriva que el sujeto activo tuvo "la posibilidad fáctica —al menos un instante— de obtener servicios o de disponer de la información existente y retirarla del mismo […]" (Posada, 2013b, p.15), este resultado de peligro es el que se debe concretar para que se satisfaga el principio de lesividad y se configure la antijuricidad del delito.

A continuación se traerán a colación distintos supuestos de hecho que enmarcan un acceso abusivo a sistema informático, con el fin de hacer un estudio profundo y determinar si en estos casos se satisface el principio de lesividad y configura la antijuricidad material.

Caso No. 1.

Un estudiante que encuentra un computador en el campus de su Universidad, decide acceder a éste con el fin de saber quién es su dueño y así poder entregarlo, el computador no consta de

ninguna contraseña o medida de seguridad, por lo cual accede de manera exitosa a éste y su sistema informático, encontrando así el nombre del respectivo propietario (Posada, 2013b).

Así las cosas, si bien se accede y se verifica el nexo, no se logra lesionar el bien jurídico protegido, lo que se refleja en la ausencia de antijuricidad de la conducta.

Bajo este supuesto de hecho, si se hace un estudio desde la tipicidad y antijuricidad formal, encontramos que sí se configura el tipo penal, ya que el estudiante ejecutó uno de los verbos rectores de la conducta al acceder sin autorización del titular del sistema informático.

Respecto a la antijuricidad material, observamos que no se configura el delito ya que no se satisface el principio de lesividad, pues la conducta del estudiante no puso "efectivamente" en riesgo el bien jurídico protegido, cuando él accede lo hace con el fin de encontrar su legítimo dueño y devolver un objeto perdido. En este sentido si bien existió la posibilidad de obtener servicios o información del sistema informático (pues el sujeto podía ordenarle tareas al sistema y éste responderlas), dicha posibilidad no resulta relevante para el Derecho Penal pues en ningún momento se pone en peligro la confidencialidad, disponibilidad e integridad de los datos o el sistema informático y mucho menos cuando el computador es devuelto a su legítimo propietario, esto último evidencia la ausencia de un proceder delictivo que es lo que resultaría reprochable.

Caso No. 2.

Un análisis similar se puede hacer en el supuesto en que una niña accede a un computador que se encontraba en la biblioteca para revisar su correo electrónico y el dueño del computador la denuncia por acceder sin su autorización.

Se observa que si bien se logra configurar la tipicidad y antijuridicidad formal, el problema surge nuevamente desde el ámbito de la antijuricidad material, ya que ésta última no se configura, pues la persona si bien accedió al computador y tenía la oportunidad de utilizar el sistema, accedió sólo a su correo electrónico y por tanto a su información, en consecuencia, no puso efectivamente en riesgo la confidencialidad, disponibilidad e integridad de los datos o sistema informático del propietario del computador.

En este sentido, el principio de lesividad pugna porque se genere un efectivo riesgo a los bienes jurídicos de terceros para que el Estado pueda intervenir y sancionar dichas conductas como delitos, lo cual como se observa, no se satisface.

Caso No. 3

Para cerrar esta exposición de supuestos de hecho, traemos el ejemplo planteado por Posada (2013b) en su texto:

> Cuando se accede a un PC nuevo u otro que no tenga datos personales, salvo que el autor tenga la intención de instalar un troyano u otro programa malicioso o dañino. Por fuera de este caso, el acceso al sistema sería insignificante si el agente no tiene la posibilidad de disponer, al menos un instante, de los datos personales o la información informatizada almacenada en ellos (p.23-24) (Subrayado fuera del texto).

Tal como se evidencia, no existe un efectivo peligro del bien jurídico tutelado, pues ni siquiera se da la posibilidad de disponer de datos o información ya que no existen.

Finalmente, de los casos expuestos se puede concluir que nunca se puso efectivamente en riesgo el bien jurídico tutelado a pesar de que se configura la conducta por ser típica y antijurídica formalmente, poniendo de presente que la falta de antijuricidad material es un problema que resulta de la forma en que está consagrado el delito de acceso abusivo a sistema informático en el artículo 269A.

Dado lo anterior, se debe entonces realizar el mismo estudio desde el punto de vista de los sistemas informáticos, ¿Por el hecho de acceder a un sistema que no contenga datos, se lesiona o pone en peligro efectivo la confidencialidad, la integridad y la disponibilidad de éste?

En cuanto a la integridad y disponibilidad del sistema informático no se ve afectada si se trata de un acceso simple, pues por el solo hecho de acceder sin que se haya desplegado otro tipo de acción -como lo advierte Posada (2013b) -, tal como instalar alguna aplicación que dañe, destruya o permita controlar el sistema, no se van a ver afectados dichos aspectos, por lo tanto no se verifica el peligro en la posibilidad que tiene el sujeto activo de disponer al menos un instante de los servicios del sistema, ni mucho menos de la información contenida.

En cuanto a la confidencialidad del sistema informático, es un punto más complejo pues se debe tener presente que "la confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a las personas autorizadas" (Rueda, 2009, p.187), lo que nos lleva a preguntarnos ¿Cuándo se accede o se mantiene en el sistema informático sin autorización se lesiona o se pone de inmediato en peligro efectivo dicho aspecto del bien jurídico tutelado?

Cuando se genera un acceso simple no se pone en riesgo o se lesiona la confidencialidad del sistema informático *per se,* pues según Rueda Martin "la confidencialidad del sistema se ve afectada si se utiliza por parte de una persona que no está autorizada" (Rueda, 2009, p.187), en este

sentido no se puede equiparar el acceso por una persona no autorizada a la utilización de éste por la misma, no basta entonces con el simple acceso o mantenimiento, sino que de éstos debe derivar "la posibilidad fáctica —al menos un instante— de obtener servicios o de disponer de la información existente y retirarla del mismo […]"(Posada, 2013b, p.15) para que se pueda afirmar que hubo un peligro concreto de utilización del sistema por persona no autorizada.

Equiparar el simple acceso a la utilización del sistema por persona no autorizada sin que se concrete el peligro en esa "posibilidad fáctica", implica entonces contemplar que el simple acceso o mantenimiento es suficiente para poner en peligro o lesionar el bien jurídico protegido desde la confidencialidad, y en consecuencia, que la conducta descrita en el tipo penal por sí sola constituye un riesgo que satisface el principio de lesividad, tratando el delito como un tipo de peligro abstracto.

Como sabemos, considerar un delito de peligro abstracto es suponer que desde el principio la sola comisión de la conducta, como se encuentra descrita, al ser ejecutada lesiona o pone en peligro el bien jurídico que se busca tutelar, sin necesidad de hacer el estudio del supuesto de hecho y verificar si el bien jurídico si resulta afectado, se tiene entonces una presunción legal.

Si consideramos el delito de acceso abusivo a sistemas informáticos un delito de peligro abstracto, estaríamos entendiendo que con el "solo acceder o mantenerse sin autorización" dentro del sistema informático se estaría poniendo en peligro efectivamente "la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" se presumiría entonces, la antijuridicidad material y se configuraría el delito.

De allí que resulte importante que la afectación a la confidencialidad sea efectiva, en consecuencia, se debe entender como la posibilidad de al menos un instante que tiene la persona

que accede al sistema informático sin autorización, “de obtener los servicios o disponer de la información existente y retirarla del mismo” (Posada, 2013b, p.15).

8. Capítulo VI: Casos emblemáticos colombianos referidos al delito objeto de estudio

Como se observó, este tipo penal empezó a integrar el catálogo de delitos de la legislación penal colombiana hace muy poco, razón por la cual el desarrollo jurisprudencial ha sido escaso.

Debido a que son escasos los asuntos que los altos tribunales han conocido, que consagren los supuestos de hecho que configuran accesos abusivos a sistemas informáticos, no contamos con el suficiente material jurisprudencial.

Sin embargo, se procede a enunciar dos casos emblemáticos que se han tomado en consideración por los tribunales a través de providencias, en cuanto consideramos que existen allí pronunciamientos interesantes para el objeto de estudio.

8.1 Hacker Sepúlveda y Bajaña, 2015.

En el "acta de audiencia de verificación de preacuerdo espionaje, concierto para delinquir y otros con detenido" (Juzgado 22 Penal del Circuito de Conocimiento de Bogotá, 2015, p. 1), condenan a los hacker Andrés Fernando Sepúlveda y Daniel Agustín Bajaña por la comisión de varios delitos informáticos, entre estos el acceso abusivo a sistema informático contemplado en el artículo 269A del Código Penal colombiano.

Los hechos se configuraron tras la contratación de Andrés Sepúlveda por el director de la Campaña para la candidatura presidencial Centro Democrático Corazón Firme, con el fin de que se encargara de la seguridad informática y el manejo de las redes. Para cumplir con dichas tareas Sepulveda contrató a sus propios trabajadores, entre estos al ecuatoriano Daniel Agustín Bajaña.

Una vez la Fiscalía hizo la captura, Sepúlveda manifestó en la diligencia de allanamiento y registros que entre las conductas que había desplegado, realizó accesos abusivos a sistemas informáticos (Fiscalía General de la Nación, 2016), así en la investigación y tras la recolección de diversos elementos materiales probatorios se encontró y probó lo siguiente:

1. Que el Centro Democrático determinó al señor Sepúlveda para que ofreciera dinero a servidores públicos, entre estos un funcionario del Ejército Nacional, con el fin de que le proporcionara 10 cuentas de correos electrónicos con sus claves, pertenecientes a los jefes negociadores del proceso de paz en la Habana, así mismo para que le hicieran entrega de las bases de datos GADH (Grupo de atención humanitaria para el desmovilizado), las cuales contienen datos de carácter secreto y ultra secreto. Por otro lado a otro funcionario quien le entregó las bases de datos de la GRUTE (Grupo antiterrorismo Sijin), siendo todas bases de datos secretas (Fiscalía General de la Nación, 2016).
2. En los equipos de Sepúlveda la Fiscalía encontró las bases de datos mencionadas y entre los correos electrónicos, el de alias "Boris" quien era el jefe de seguridad y telecomunicaciones de las FARC en la mesa de la Habana (Fiscalía General de la Nación, 2016).
3. Por parte de la misma candidatura al parecer se determinó al señor ANDRÉS FERNANDO SEPÚLVEDA ARDILA, para que sin autorización accediera al correo del ex presidente FRANCISCO SANTOS, acceso que se logró en parte, ya que se accedió a los correos de las secretarías del mismo, MARÍA ANGÉLICA CUELLAR y ALEJANDRA OSPINA ESTEFAN. (Fiscalía General de la Nación, 2016, p.13) (Subrayado fuera del texto)

Cabe resaltar que el acceso al correo electrónico de Francisco Santos fue resultado del acceso al dominio de éste, es decir, al sitio web "*pachosantos.com*" y al correo "*mail.pachosantos.com*", tal como se afirmó en la imputación fáctica "(...) Sin autorización alguna accedieron al dominio del correo electrónico del grupo de trabajo del ex vicepresidente de la República Francisco Santos Calderón(…)" (Juzgado 22 Penal del Circuito de Conocimiento de Bogotá, 2015, p.2).

La anterior tarea fue solicitada a Daniel Agustín Bajaña Barragán, quien la concretó de manera exitosa, por lo cual fue condenado a 40 meses de prisión junto con Andrés Sepúlveda condenado a 10 años, por el delito de acceso abusivo a sistema informático entre otros (Fiscalía General de la Nación, 2016).

8.2 Corte Suprema de Justicia, Sala Penal, control parental.

En la Sentencia SP 9792 del 29 de julio de 2015 dictada por la Corte Suprema de Justicia, Sala de Casación Penal, se sentó un precedente importante en cuanto a la legitimidad de los accesos hechos por los padres a los correos electrónicos de sus hijos y demás sistemas de comunicación como computadores y otros dispositivos electrónicos.

Los hechos que dieron lugar al pronunciamiento de la Corte, se dan con ocasión de la solicitud de la defensa de Edwin, condenado por acceso abusivo con menor de 14 años, en la que alega como ilícitas las pruebas sobre las cuales se fundó dicho fallo, ya que consistían en mensajes contenidos en el correo electrónico de la menor que habían sido obtenidos de manera ilícita por su madre y no conforme a la ley, pues no fueron producto de una búsqueda selectiva en base de datos.

La Corte expuso:

> Toda medida que implique control de las comunicaciones tiene que respetar el principio de proporcionalidad, por tanto se debe determinar que la misma tiene como fin la protección y garantía de derechos que es adecuada al fin perseguido y que no existe otra medida que permita obtener los mismos resultados y sea menos restrictiva de derechos.
>
> En consecuencia, los padres, en ejercicio de la patria potestad, constitucional y legalmente se encuentran autorizados para asistir, orientar y controlar las comunicaciones de sus hijos menores de edad, limitados solamente por la menor afectación de otras prerrogativas y por la finalidad de protección y garantía de los derechos fundamentales de los niños, niñas y adolescentes.
>
> Resulta un verdadero contrasentido afirmar que las actividades de seguimiento, orientación, protección, que implementa una madre o un padre respecto de sus hijos menores en la intimidad de sus hogares, per se, se ofrecen ilegales, si en la interacción que ello implica requieren de la aprobación de una autoridad judicial, cuando la ley, los instrumentos internacionales, el Gobierno Nacional a través de todas las campañas de información, prevención y orientación difundidas a través de los diferentes medios de comunicación, insta y alerta para que se acompañe a los menores todo el tiempo en el que usan y permanecen en contacto con la variedad de dispositivos electrónicos de comunicación y computadores, especialmente, cuando acceden a redes sociales,

con el deber de verificar los contenidos y con quién o quiénes se comunican, para evitar que sean objeto de comportamientos y personas que vulneren o pongan en peligro el pleno ejercicio de sus derechos y les afecten su normal desarrollo físico y mental.

La Corte entiende que cuando el fin no está encaminado a los postulados de asistencia, acompañamiento, orientación, educación y protección considerados en la Constitución Política, la ley, los tratados internacionales y el ejercicio de la patria potestad, sí puede comprenderse que la intervención de los padres afecta la intimidad del menor, la que resulta ilegítima y reprochable.

Por lo tanto, desde el marco del derecho internacional, la Constitución Política y la ley, reitera la Sala que los padres en cumplimiento de la responsabilidad parental, las obligaciones de asistencia y protección, el ejercicio de los deberes de cuidado, acompañamiento y orientación de sus hijos menores, para garantizarles la plena maduración de sus capacidades física, intelectual y moral, más allá de los límites que fija el derecho a la intimidad, tienen la facultad de acceder a las comunicaciones de las plataformas tecnológicas que los niños, niñas y adolescentes reciben y abordan, pues no de otro modo, al estar bajo su amparo, pueden verificar el contenido de los mensajes y la clase de personas con las que interactúan a través de tales medios, que de ser necesario, permitan su intervención oportuna para prestarles ayuda, auxilio, apoyo y defensa, conforme su encargo les demanda. (Corte Suprema de Justicia, Sala de

> Casación Penal, SP 9792 de 2015, MP. Salazar, Patricia, p. 32) (Subrayado fuera del texto)

Así la Corte sienta las bases sobre los casos de acceso abusivo a sistema informático en los que su titular sea un menor de edad, afirmando que este se vuelve legítimo cuando se accede en cumplimiento de los deberes de control y orientación de los padres a pesar de no contar con el consentimiento del menor, por lo tanto estaríamos frente a una conducta típica pero que carece de "antijuridicidad formal", siempre y cuando los padres obren en virtud de estos deberes.

En esta misma línea, la Corte señala que el derecho a la intimidad es un derecho fundamental del cual también son titulares los niños y adolescentes, sin embargo éste no es absoluto y se puede limitar en aras de la protección especial de la cual gozan estos sujetos.

Protección especial que no solo es ejercida por el Estado sino en gran medida por quienes se encargan del cuidado de los menores, en consecuencia en las relaciones padres e hijos, tal derecho puede resultar afectado por el ejercicio del deber de protección evitando mayores conculcaciones, en este sentido la Corte Suprema de Justicia afirma:

> No se puede pasar por alto que la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales ya evocada, insiste en que en procura de la defensa de los niños, **la familia debe implementar las medidas de protección que su condición requiere**, siendo la más elemental de ellas, conocer, con quiénes interactúan en los diferentes espacios de su vida cotidiana, que incluye los accesos a las redes de internet y

> sus diferentes contenidos. (Corte Suprema de Justicia, Sentencia SP 9792 de 2015. M.P. Salazar, Patricia, 2015, p. 45)

Finalmente la Corte realizó un análisis sobre lo que se debe entender por bases de datos, y concluye que dentro de ésta categoría no se encuentran las cuentas personales de correos electrónicos, ni "las bases de datos tampoco pueden confundirse con los sistemas informáticos creados por el usuario que como particular no ejerce la actividad de recolección y organización de información de manera técnica, habitual o institucional" (Corte Suprema de Justicia, Sentencia SP 9792 de 2015. M.P. Salazar, Patricia, 2015, p.36).

En conclusión, al analizar este caso, se observa que los pronunciamientos y aclaraciones en cuanto al acceso abusivo a sistema informático se dan desde el escenario de vulneración de la intimidad y no del bien jurídico de "la confidencialidad, integridad y disponibilidad de la información y los datos". Se percibe entonces, que en esta sentencia frente al acceso abusivo a sistema informático, para el tribunal resulta de mayor relevancia proteger la intimidad como bien jurídico autónomo que los mismos datos y la información, siendo estos últimos los que tutela el tipo penal en mención.

9. Capítulo VII: Conclusiones

Una vez analizada la información anterior, la primera conclusión que se deriva de ello es que para que el acceso abusivo a sistema informático cumpla con la antijuricidad material, éste debe satisfacer el principio de lesividad. En este sentido, debería al menos consagrarse como un delito de peligro en concreto tal como se expuso en este trabajo; sin embargo, de la redacción actual del tipo penal en el artículo 269A de la Ley 599 de 2000, lo que se da a entender es que se podría configurar la conducta sin que se logre efectivamente poner en peligro el bien jurídico tutelado "la confidencialidad, integridad y disponibilidad de los datos y del sistema informático", es decir, estaríamos frente a un delito de peligro abstracto.

Al considerar este delito de peligro abstracto, se corre el riesgo de judicializar conductas que si bien pueden ser relevantes para el ordenamiento jurídico, no lo son para el Derecho penal, es decir, mediante esta figura solo se debería permitir que se sancione aquellas conductas que además de estar consagradas como delito, produzcan también un daño concreto o la puesta en peligro efectiva al bien jurídico tutelado.

Entonces ¿existe una tipificación coherente y conveniente en términos de política criminal?

De lo expresado por el tipo penal:

> 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. (Congreso de Colombia, Ley 599 de 2000, art. 269A)

Dicha tipificación tal y como se encuentra establece que en el ordenamiento jurídico colombiano, es suficiente ejecutar todos los verbos rectores de la conducta para que se configure el delito, sin que en realidad se dé la efectiva puesta en peligro o lesión del bien jurídico.

Lo anterior ha impactado en la aplicación por parte de los operadores judiciales ya que al constatar la realidad, si se denunciare un caso en el que se acceda a un sistema informático que no contenga datos, los funcionarios entran a verificar que la conducta que se desplegó fue la descrita en el tipo penal y bastaría con probar que el denunciado accedió o se mantuvo sin autorización en el sistema informático para configurar el delito, por lo cual el juez terminaría condenando y aplicando una pena sin que efectivamente se haya puesto en peligro o lesionado el bien jurídico, es decir, se estaría utilizando un tipo penal que no cumple con el principio de lesividad y antijuricidad material, contemplando así accesos que deberían ser irrelevantes para el derecho penal.

Por otro lado, en cuanto aquellos supuestos de hecho en que sí se pone en riesgo el bien jurídico tutelado, continúa la preocupación respecto de la redacción del artículo 269A, ya que en términos de punibilidad, la sanción resulta desproporcionada pues la descripción del tipo concede penas iguales a accesos que poseen una mayor relevancia frente a los que no.

Para precisar estos puntos, se exponen los siguientes supuestos de hecho:

El primer caso tiene que ver con una usuaria de Facebook que deja su computador con su cuenta abierta, por lo cual una persona con la intención de jugarle una broma decide cambiar el estado de una de sus redes (facebook), posteriormente cierra la sesión de la usuaria inicial, y deja de utilizar el computador.

En el segundo caso, un hombre nota llamadas extrañas en el celular de su novia y con el fin de averiguar qué está pasando, decide revisar su correo electrónico, en donde encuentra varios mensajes de un amigo. Lleno de celos además de reclamarle al amigo, termina teniendo una gran discusión con su novia, es así que en un ataque de ira, ella decide denunciarlo por haber invadido su espacio, sin embargo, días después lo perdona.

El tercer supuesto de hecho plantea que, una persona posee un computador viejo que no utiliza pero que contiene su información, no obstante otro sujeto al notar que nadie utiliza el computador decide hacerlo sin pedir la autorización correspondiente, debido a que el dispositivo no cuenta con ninguna medida de protección, puede entrar tranquilamente y usarlo para sus tareas; sin embargo, cuando el dueño del computador está al tanto de la situación, se exalta e inicia una pelea por los hechos y al no encontrar ninguna respuesta decide ponerle fin al problema denunciándolo.

Como se observa, en estos casos sí se pone en riesgo el bien jurídico tutelado, se satisface el principio de lesividad y se da la antijuricidad material, configurando el delito de acceso abusivo a sistema informático en su totalidad, ya que en todos éstos el acceso viene con la posibilidad concreta de obtener servicios del sistema y disponer de la información que allí se encuentra.

Pero la tarea del Derecho penal al ser un derecho de última ratio va más allá de sancionar conductas que cumplan con los requisitos para configurarse como delito, y es velar porque se sancionen solo las conductas dignas de reproche penal.

En este orden de ideas, la tipificación actual del delito supone dar el mismo tratamiento punitivo a los casos de acceso abusivo que no logran afectar el bien jurídico, a los que si bien lo

logran, dicha afectación resulta irrelevante para el derecho penal y a los que logran una afectación del bien jurídico que sí merece un reproche social y una sanción incluso penal.

Resulta entonces desproporcionado aplicar las mismas penas a un acceso donde las consecuencias no van más allá de una broma, una pelea de pareja, o un mal entendido, a un acceso a sistema informático de entidad financiera, corporativa o estatal en la que las consecuencias son la puesta en riesgo o vulneración del patrimonio, el orden económico o la seguridad nacional.

No significa que casos como los tres ejemplos que se acaban de plantear no se deban observar, ya que resultan relevantes para el Derecho penal cuando van más allá del simple acceso o mantenimiento, por ejemplo cuando se pone en peligro el ámbito personal o la esfera privada de una persona, teniendo consecuencias graves como la divulgación de la información que se encuentra en Facebook, en el correo electrónico, en su computador personal, las fotos que se encuentran en su Ipad, o incluso cuando se extorsiona al titular de la información por el simple conocimiento de ésta.

De esta manera, solo cuando el acceso trae consigo la intención de despegar otras conductas o perseguir otros fines como los mencionados anteriormente, resulta relevante activar el derecho penal siendo adecuado consagrar en este tipo de accesos el ánimo de tener un propósito o provecho.

En conclusión, la redacción del tipo penal, además de necesitar una finalidad en dichos escenarios; debe establecer *el acceso abusivo a sistema informáticos* con una pena privativa de la libertad ejemplar para aquellos supuestos de hecho que recaen sobre el sistema informático de una entidad financiera, corporativa, estatal, institucional y entidades particulares que desempeñen

funciones públicas, y de los datos que estos contienen, ya que es allí donde resulta un verdadero valor para los fines sociales por los que el Estado vela, y existiría un interés legítimo y especial de protección.

10. Capítulo VIII: Propuesta

Teniendo en cuenta las conclusiones a las que se llegó en este trabajo, se considera pertinente realizar algunos aportes específicos a la tipificación del delito que buscan evitar que su consagración no satisfaga el principio de lesividad y no cumpla con la antijuricidad material.

Para exponer nuestra propuesta comenzaremos recordando lo descrito en el artículo 269A de la Ley 1273 del 2009.

> **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 Colombia, Ley 1273 de 2009, art. 269A)

Nuestra propuesta entonces, sugiere una nueva redacción del tipo penal en los siguientes términos:

Artículo 269A: **Acceso abusivo a un sistema informático**. El que, sin autorización o por fuera de lo acordado, acceda a un sistema informático del sector estatal, financiero o corporativo, protegido con medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad expresa o tácita de quien tenga el legítimo derecho a excluirlo, teniendo la posibilidad fáctica de obtener servicios o de disponer de la información existente, incurrirá en pena de prisión de

sesenta (60) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Cuando se trate de un acceso en los términos descritos en el inciso anterior a un sector distinto a los allí referidos y con el proposito de obtener provecho, la pena será de veinticuatro (24) meses a cuarenta y ocho (48) meses y en multa de 50 a 500 salarios mínimos legales mensules vigentes.

Así las cosas, la primera propuesta se basa en que resulta de vital importancia que el legislador determine los conceptos necesarios y básicos para poder entender la conducta, tal como ya lo han hecho los instrumentos internacionales entendiendo la importancia de aclararlos, entre estos se toma como ejemplo los esfuerzos de la Comunidad europea reunidos en la Decisión Marco 222/2005 donde expresa que "Unas definiciones comunes en este ámbito, más concretamente de los sistemas de información y los datos informáticos, son importantes para garantizar la aplicación coherente de la presente Decisión marco en los Estados miembros" (Consejo de Europa, 2005, p. 1).

Es así que en el ordenamiento jurídico colombiano cuando el tipo penal expone "en todo o en parte a un sistema informático" se hace realmente necesario dar una definición precisa de lo que se debe entender por "sistema informático" en la Ley 1273 de 2009, para que así exista unidad por parte de los operadores judiciales a la hora de aplicar las disposiciones legales a los distintos supuestos de hecho.

Ahora bien, en cuanto a la tipificación específica del delito de acceso abusivo a sistema informático, la primera observación que encontramos es que al establecer "en todo o en parte", la tipificación resulta confusa, pues dado que no hay claridad sobre lo que se debe entender por tal

expresión, queda abierto al campo de la subjetividad dándose todo tipo de interpretaciones. Resultaría entonces conveniente que el legislador definiera a que se refiere y así poder encontrar el sentido de dicha redacción. No obstante cabe notar que ya sea que se acceda o mantenga en todo el sistema informático o solo en una parte, el resultado será el mismo, es decir, se estaría accediendo o manteniendo en un sistema informático, que es lo exigido por el tipo, por lo cual cuestionamos ¿si resulta realmente útil establecer "en todo o en parte"? o sí sería más eficaz y práctico establecer en la tipificación "acceda a un sistema informático" ya que independiente de que sea en todo o parte, la pena es la misma.

La segunda observación se da respecto al enunciado en el tipo penal que expresa "protegido o no con una medida de seguridad", para lo cual tomamos como referentes (ya que no son vinculantes) el Convenio de Budapest de 2011 y la Decisión Marco 222/2005.

El Convenio consagra en el acceso ilícito que "(...) Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad (...)" (Consejo de Europa, 2001, p. 4) y la Decisión Marco 222/2005 expone "(...) que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad" (Consejo de Europa, 2005, p. 3).

De la posibilidad que brindan estos instrumentos internacionales, consideramos -y así lo proponemos-, que resulta necesario establecer como elemento esencial del tipo en el ordenamiento jurídico colombiano que el sistema informático esté protegido con medidas de seguridad, así, si uno de los propósitos del Derecho penal es consagrar como delitos aquellas conductas que afectan bienes jurídicos de terceros, al no exigir al titular que construya medidas de seguridad, el Estado entra a velar por los sistemas informáticos cuya protección ni siquiera es

de interés de su titular. Y el legislador termina "alcahueteando" la negligencia y descuido del sujeto pasivo de la conducta, al no preocuparse por el debido cuidado de sus intereses, lo que resulta incoherente en términos de política criminal.

En este sentido, las medidas de seguridad (mecanismos de autoprotección) tienen como fin la conservación tanto del sistema como de su contenido y cuando no posee dichas medidas, significa que está desprotegido lo que "señala de manera inequívoca el poco interés del titular del sistema para reservar la disponibilidad, integridad y confidencialidad de los datos o de la información almacenada" (Posada, 2013b, p.17). Por ésta razón, es conveniente volver a lo descrito en la tipificación anterior del delito en el artículo 195 del código penal antes de la reforma de la ley 1273 de 2009 que dispone "(...) se introduzca a un sistema informático, protegido con medida de seguridad (...)", tal como lo establecen también los ordenamientos jurídicos de Italia (Código penal italiano, artículo 615-ter) y España (Código español, artículo 197Bis).

En la tercera observación, se pone de presente el desacuerdo con que accesos que no logran siquiera poner en riesgo el bien jurídico protegido, o aquellos que logrando hacerlo resultan irrelevantes para el Derecho penal (desde el ámbito de lo que se logra con un simple acceso), tengan la misma pena que aquellos accesos que por su naturaleza tienen mayor relevancia.

Así tomamos para nuestra propuesta nuevamente como referente la Decisión Marco 222/2005 cuando expresa:

> "Se ha comprobado la existencia de ataques contra los sistemas de información, en particular como consecuencia de la amenaza de la delincuencia organizada, y crece la inquietud ante la posibilidad de ataques terroristas contra sistemas de

> información que forman parte de las infraestructuras vitales de los Estados miembros. Esto pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia, y por tanto exige una respuesta por parte de la Unión Europea".
>
> (...)
>
> 1. Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. (Consejo de Europa, 2005, p. 3) (Subrayado fuera del texto)

En este orden de ideas, observamos que la comunidad europea con este instrumento tiene como propósito principal proteger la infraestructura de los Estados y sus instituciones, poniendo de presente que son este tipo de accesos los que han despertado preocupación[27] y por ende la necesidad de una sanción. Tanto así que en la tipificación del acceso ilegal a sistemas de información establece la posibilidad de que frente a aquellos casos que sean de menor gravedad no sea necesario establecer una infracción penal.

Así, cuando el Estado decide dejar por fuera los supuestos de hecho en los que el interés a proteger no resulta relevante, se evita consagrar tipos penales que no satisfagan el principio de lesividad y antijuridicidad material, o que cumpliendo con estos no son dignos de reproche penal.

[27] En Colombia con los casos que llegan a la fiscalía se evidencia que la preocupación y el verdadero interés está en aquellos accesos que se dan en los sistemas de la infraestructura del Estado, casos como por ejemplo el de una funcionaria quien accedía al sistema informático de transito de Barranquilla con el fin de coordinar centrales ilegales o paralelas de tránsito (Fiscalía General de la Nación, 2016, s/p), o el de el hacker Andrés Fernando Sepúlveda y Daniel Agustín Bajaña, en donde el acceso también afectó la institucionalidad del Estado, siendo este uno de los casos más importantes para el país, evidencia que son este tipo de accesos los que interesa perseguir y sancionar.

En esta línea, se considera que el tipo penal debe tener en cuenta en primer lugar accesos que se realicen a un sistema informático de una entidad estatal (no solo aquellos sistemas que manejan datos de inteligencia y contrainteligencia, pues todo lo abarca el espionaje, sino todo sistema de la entidad), corporativa, financiera y aquellas que desempeñen funciones públicas -tal como lo hace Estado Unidos en la ley de fraude y abuso informático- donde poner en riesgo o lesionar la confidencialidad, integridad y disponibilidad de los datos y el sistema significa poner en riesgo o lesionar intereses de tan alto rango como la seguridad nacional y el orden económico, de ahí que la pena deba ser proporcional a los intereses que están en riesgo.

Y en segundo lugar frente a aquellos accesos que se dan en sistemas de un sector diferente a los mencionados se debe mantener la conducta siempre y cuando se realice con un propósito ulterior, pero con una pena menor. Lo anterior dado a que el grado de afectación no es el mismo cuando se accede al sistema de una entidad institucional que cuando se accede por ejemplo al correo personal de alguien, pues las consecuencias que se podrían acarrear no son equivalentes, por lo cual se justifica que el reproche penal sea menor.

Finalmente la cuarta observación, gira en torno a que esta nueva tipificación debe estar consagrada de manera tal que de la conducta no solo resulte su tipicidad y antijuricidad formal sino también su antijuridicidad material, por lo cual el tipo penal debe considerarse un delito de peligro concreto y su tipificación lo debe evidenciar de forma manifiesta e inequívoca, exigiendo que se dé la efectiva puesta en peligro del bien jurídico tutelado y se satisfaga el principio de lesividad. Así cuando se dispone que el acceso o mantenimiento en el sistema informático exista con “la posibilidad fáctica de obtener servicios o disponer de la información contenida”, ya se está exigiendo la efectiva puesta en peligro del bien jurídico.

La tipificación que sugerimos, evita que se desgaste el aparato judicial cuando se activa por casos que no resultan relevantes y que por esta razón terminan en el proceso de investigación o a mitad del proceso penal.

Referencias Bibliográficas

Aboso, G. & Zapata, M. (2006). Cibercriminalidad y derecho penal. Buenos Aires: B de F.

Acurio, S. (2015). Derecho penal informático: Una visión general del Derecho Informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital. Recuperado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Acurio, S. (s.f.). Delitos informáticos. Recuperado de: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf delitos informáticos generalidades página 21.

Aguilera, P. (2010). Seguridad informática. Madrid: Editex.

Aránguez, C. & Alarcón, E. (2000). El código penal Francés traducido y anotado. Granada: Comares.

Baquero, J. & Gil, E. (2015). Metodología de la investigación jurídica. Quito: Universidad de Los Hemisferios.

Barreiro, A. (1995). El delito de descubrimiento y revelación de secretos en el Código Penal de 1995. Un análisis del artículo 197 del CP. Recuperado de: https://revistas.uam.es/revistajuridica/article/viewFile/6240/6703

Bazán, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. Estudios Constitucionales, 3(2), 85-139. Recuperado de: http://www.redalyc.org/articulo.oa?id=82030204

Bernate, F. (2006). Estudios de derecho penal económico. Bogotá: Grupo Editorial Ibañez.

Borghello, C. (2011). Seguridad informática: sus implicancias e implementación. Buenos Aires, Argentina: Universidad Tecnológica Nacional.

Brigard y Urrutia. (s.f.). Políticas de tratamiento de la Información. Recuperado de: http://bu.com.co/es/politicasdeprivacidad

Bustos, J. (2008). Derecho Penal Especial. Bogotá: Leyer.

Camacho, S. (2005). Partes intervinientes, formación y prueba del contrato electrónico. Madrid: Reus.

Cámara de Representantes. (2007). Exposición de motivos del proyecto de ley 123 de 2007. Bogotá: Gaceta del congreso.

Castells, M. (2002). La era de la información. Economía, sociedad y cultura. México: Siglo XXI.

Castro, C. (2008). Manual de Derecho Penal, Parte especial Tomo II Bogotá: Universidad del Rosario.

CCOO Federación de Industria Textil –Piel, Químicas y Afines. (2007). XV Convenio general de la industria química. Recuperado de: http://www.ccoo.cat/fiteqa/faurecia/informacion/LEGAL%20LABORAL/convenios/conv_indsquimicas.pdf

Cifuentes, E. (1997). El hábeas data en Colombia. Ius et Praxis, 3(1), 81-106.

Cita, R. (2010) Delitos de peligro abstracto en el derecho penal colombiano: crítica a la construcción dogmática y a la aplicación práctica. (Tesis de maestría) Universidad Nacional de Colombia, Bogotá.

Congreso de Colombia. (2000). Ley 599 de 2000. Código penal colombiano. Bogotá: Diario Oficial.

Congreso de Colombia. (2009). Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las

tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá: Diario Oficial.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Recuperado de: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

Corte Constitucional de Colombia. (1995). Sentencia SU 082/95. M.P. Jorge Arango Mejía. Bogotá: La Corte.

Corte Constitucional de Colombia. (1996). Sentencia T-696 de 1996. M.P. Fabio Morón Díaz. Bogotá: La Corte.

Corte Constitucional de Colombia. (1997). Sentencia T-552/97. M.P. Dr. Vladimiro Naranja Mesa. Bogotá: La Corte.

Corte Constitucional de Colombia. (1997). Sentencia T-552/97. M.P. Dr. Vladimiro Naranja Mesa. Bogotá: La Corte.

Corte Constitucional de Colombia. (1999). Sentencia T-307 de 1999. M.P. Eduardo Cifuentes Muñoz. Bogotá: La Corte.

Corte Constitucional de Colombia. (2002). Sentencia. T-729 de 2002. M.P. Eduardo Montealegre Lynett. Bogotá: La Corte.

Corte Constitucional de Colombia. (2007). Sentencia T-559-07. M.P. Dr. Jaime Araujo Rentería. Bogotá: La Corte.

Corte Constitucional de Colombia. (2008). Sentencia T-158A. M.P. Dr. Rodrigo Escobar Gil. Bogotá: La Corte.

Corte Constitucional de Colombia. (2010). Sentencia C-936/10. M.P. Luis Ernesto Vargas Silva. Bogotá: La Corte.

Corte Constitucional de Colombia. (2012). Sentencia CC T -260/12. M.P. Humberto Antonio Sierra Puerta. Bogotá: La Corte.

Corte Constitucional de Colombia. (2014). Sentencia C-881 de 2014, M.P. Jorge Ignacio Pretel. Bogotá: La Corte.

Corte Constitucional de Colombia. (2014). Sentencia C-881 de 2014. M.P. Jorge Ignacio Pretel. Bogotá: La Corte.

Corte Constitucional de Colombia. (2014). Sentencia T-158A de 2008. M.P. Rodrigo Escobar Gil. Bogotá: La Corte.

Corte Suprema de Justicia. (2015). SP 9792 de 2015. M.P. Suarez, Patricia. Bogotá: La Corte.

Cortes, R. (2015). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia, revista de derecho comunicaciones y nuevas tecnologías. 14, 1-17. Recuperado de: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics227.pdf

Council of Europe. (2011). Convenio de Budapest de 2011. Recuperado de: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

Diario del Derecho de España. (2015). La AP de Murcia condena a una trabajadora por delito de intrusión informática por acceder ilegítimamente al sistema informático de su empresa y a los correos corporativos durante su baja laboral. Recuperado de: http://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1144636

Díaz, A. (2010). Aniversario en Colombia del nuevo delito de violación de datos personales, primer año de vigencia de la ley delitos informáticos. Bogotá: Díaz García Alexander

Díaz, A. (2012). Derecho informático elementos de la informática jurídica. Bogotá: Leyer.

Doyle, C. & Bartlett, A. (1986). Cybercrime: an overview of the federal computer fraud and abuse statute and related federal criminal laws. New York: Novinka Books.

España, M. (2003). Servicios avanzados de telecomunicaciones. Madrid: Díaz de Santos.

Fiscalía General de la Nación. (2014). A la cárcel por usar de manera ilegal la información de las víctimas del conflicto. Recuperado de: http://www.fiscalia.gov.co/colombia/noticias/a-la-carcel-por-usar-de-manera-ilegal-la-informacion-de-las-victimas-del-conflicto/

Fiscalía General de la Nación. (2016). Mujer implicada en caso de corrupción con oficina ilegal del tránsito en Barranquilla, se entregó a la Fiscalía. Recuperado de: http://www.fiscalia.gov.co/colombia/noticias/mujer-implicada-en-caso-de-corrupcion-con-oficina-ilegal-del-transito-en-barranquilla-se-entrego-a-la-fiscalia/

Fiscalía General de la Nación. (2016). Proceso de investigación y judicialización. Orden de archivo FGN-20-F-01. Recuperado de: http://www.fiscalia.gov.co/colombia/wp-content/uploads/20170111.pdf

Fiscalía General de la Nación. (2017). Condenado por alterara el sistema web de la Universidad de Choco para hacer titulos de abogado falsos. Recuperado de : http://www.fiscalia.gov.co/colombia/noticias/condenado-por-alterar-el-sistema-web-de-la-universidad-de-choco-para-hacer-titulos-de-abogado-falsos/

Genghini, R. & Rocca, D. (2002). Il reato di accesso abusivo ad un sistema informatico otelematico: l'art. 615 ter del Codice Penale. Rubrica legale – ICT Security, 3, 1-3. Recuperado de: http://www.genghinieassociati.it/wp-

content/uploads/2007/05/Il%20reato%20di%20accesso%20abusivo%20ad%20un%20sistema%20informatico...Lu-Ago%202002.pdf

González, G. (s.f.). El derecho a la intimidad y a la informática. Recuperado de: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwi2nL2jmovTAhVLlFQKHcNwAs0QFgglMAI&url=http%3A%2F%2Frevistas.pucp.edu.pe%2Findex.php%2Fthemis%2Farticle%2Fdownload%2F11095%2F11608&usg=AFQjCNG9EinWrKu9fQVsffACSqstBFGg0g&sig2=jAiNgSFi3nQ9f660s7ewEA

Gonzales, J. (2010). Los delitos informáticos y su aplicación en la legislación colombiana. Maestría en Derecho Penal. Universidad libre de Colombia. Bogotá, Colombia.

Hoscman, H. (2013). Negocios en Internet. Buenos Aires: Astrea y Universidad del Rosario.

Jefatura de Estado de España. (2015). Código penal español. Recuperado de: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t10.html#a197t

Juzgado 22 Penal del Circuito de Conocimiento de Bogotá. (2015). Acta de Audiencia de verificación de preacuerdo espionaje, concierto para delinquir y otros con detenido, Radicado 110016000000201401031. Juez. Rosa Tulia Ramos Villalobos. Bogotá: El Juzgado.

Lefebvre, F. (s.f.). Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Recuperado de: http://content.efl.es/getFile.aspx?data=ZmlsZU5hbWU9TVBFTl8wOTg1MF8xMDAyMC5wZGYmYXJlYT1leHRyYW1lbWVudG9zJnN1YkZvbGRlcj1kb2N1bQ%3D%3D&download=0

Loiseau, V. & Canales, P. (2004). Delitos informáticos en la legislación de España, Francia, Alemania e Italia. Santiago de Chile: Biblioteca del Congreso Nacional de Chile - Departamento de Estudios, Extensión y Publicaciones.

Márquez, C. (2002). El delito informático, la información y la comunicación en la esfera penal conforme con el nuevo código penal. Bogotá: Leyer.

Miro, F. (2012). El Cibercrimen. Fenomenologìa y criminología de la delincuencia en el ciberespacio. Madrid: Marcial Pons.

Montaño, A (2008). La problemática jurídica en la regulación de los delitos informáticos. Coyoacán Ciudad de México. Recuperado de: https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi-v7vS94HVAhXCJCYKHSZvAzMQFgghMAA&url=http%3A%2F%2Fwww.ordenjuridico.gob.mx%2FPublicaciones%2FTesis2010%2F01_LDP_MONTANO.pdf&usg=AFQjCNFat0T-xM0OBj67uss2F5SlLzuJwA

Narváez, D. (2015). El delito informático y su clasificación. Revista de Ciencia, Tecnología e Innovación Uniandes Episteme, 2(2), 1-16. Recuperado de: http://186.46.158.26/ojs/index.php/EPISTEME/article/viewFile/102/91

Ojeda, J., Rincón, F., Arias, M. & Daza, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad. 11(28), 41-66. Recuperado de: http://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176 .

Palazzi, P. (2000). Delitos informáticos. Buenos Aires: Ad Hoc.

Palomá, L. (2012). Delitos informáticos (en el ciberespacio) doctrina y análisis de casos reales. Bogotá: Andrés Morales.

Pardini, A. (2002). Derecho de Internet. Capítulo II el ámbito electrónico y sus formas de comunicación. Buenos Aires: La Rocca.

Pinochet, F. (2006). El derecho de internet. Santiago de Chile: Derecho de Chile.

Policía de Estado de Italia. (1930). Código Penal Italiano. Recuperado de: http://www.wipo.int/wipolex/es/text.jsp?file_id=229521

Posada, R. (2013a). El delito de transferencia no consentida de activos. Revista de Derecho, Comunicaciones y Nuevas Tecnologías, (8), 1-27.

Posada, R. (2013b). El delito de acceso abusivo a sistema informático: A propósito del art. 269A del CP del 2000. Revista de Derecho y Comunicaciones Nuevas Tecnologías, 9, 1-31

Precedo, J. (2015). Espiar el móvil de la pareja: dos años y medio de cárcel. Diario El País. Recuperado de: http://politica.elpais.com/politica/2015/10/02/actualidad/1443804996_640011.html

Real Academia Española. (2017). Concepto de la RAE. Recuperado de: http://dle.rae.es/?id=0K1XBn0

Red Inalámbrica WiFi. (2016). Definición de WiFi. Recuperado de: https://redwifi.wordpress.com/definicion-de-wifi/

República de Colombia. (1991). Constitución política de Colombia de 1991. Bogotá: Colegio de Abogados Rosaristas.

Rueda, M. (2009). Cuestiones político-criminales sobre las conductas de hacking. Revista Internacional de Derecho Penal Contemporáneo. 28, 157-193. Recuperado de: http://mmcdesign.com/revista/wp-content/uploads/2009/09/26_7_los_ataques_contra_los_sistemas_.pdf

Rueda, M. (2010). Los ataques contra los sistemas informáticos: conductas de Hacking: Cuestiones político-criminales. Recuperado de: http://www.egov.ufsc.br/portal/sites/default/files/los_ataques_contra_los_sistemas_informaticos_conducta_de_hacking._cuestiones_politico-criminales.pdf

Sáenz, F. & De la Cuesta, J. (2005). Código penal francés. Recuperado de: http://diarium.usal.es/vito/2015/02/03/traducciones-al-espanol-del-derecho-frances-en-legifrance/

Salazar, J. (2009) Situación normativa de la sociedad de la información en Colombia. Revista Criterio Juridico, 9(1), 89-103. Recuperado de: http://portalesn2.puj.edu.co/javevirtualoj/index.php/criteriojuridico/article/viewFile/323/1162

Sampedro, C. (2008) Lecciones de Derecho Penal, parte general. Bogotá: Universidad Externado de Colombia.

Sánchez, C. (2013). Bien jurídico y principio de lesividad. Bases históricas y conceptuales sobre el objeto de protección de la norma penal. Revista Digital de Maestría en Ciencias Penales, 5. 436-497.

Sieber, U. (1998). Computer Crime and Criminal Information Law. Recuperado de: http://www.jura.uni-muenchen.de/sieber/article/mitis/ComCriCriInf.htm.

Tribunal Constitucional de España. (2013). Sentencia EDJ 2013/182887. M.P. Andrés Ollero. Madrid: El Derecho y Quantor.

Tribunal Supremo de Madrid. (2007). Sentencia STS 1807/ de 2007, sala de lo penal con Ponente Miguel Colmenero Menéndez de Luarca. Delito de descubrimiento y revelación de

secretos. Recuperado de: http://www.poderjudicial.es/search/documento/TS/531204/Dolo/20070412

Tribunal Supremo de Madrid. (2009). Sentencia 123/2009. M.P. Luciano Varela Castro. Recuperado de: http://supremo.vlex.es/vid/-57821781

Unión Europea. (2005). Decisión marco 225/JAI del Concejo: Relativas a los ataques contra los sistemas de información. Recuperado de: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF