CÓMO PUEDE EL ESTADO REGULAR E INTERVENIR LA INFORMACIÓN Y LOS DATOS EN INTERNET

MARÍA ISABEL JARAMILLO CANO
MARÍA CAMILA GIL MENESES

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS
FACULTAD DE DERECHO
DERECHO
MEDELLÍN
2019

CÓMO PUEDE EL ESTADO REGULAR E INTERVENIR LA INFORMACIÓN Y LOS DATOS EN INTERNET

MARÍA ISABEL JARAMILLO CANO Y MARÍA CAMILA GIL MENESES

Trabajo de grado para optar al título de Abogado.

Asesor
MIGUEL DÍEZ RUGELES
Abogado

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE DERECHO Y CIENCIAS POLÍTICAS
FACULTAD DE DERECHO
DERECHO
MEDELLÍN
2019

CONTENIDO

RESUMEN

En el artículo se hace un análisis de la intervención estatal sobre los sistemas informáticos y los continuos desarrollos tecnológicos para encontrar la utilidad de las normas que eviten el fraude, el uso del software malicioso, el acceso abusivo a dichos sistemas, entre otras muchas conductas ilícitas que se encuentran tipificadas en el Código Penal colombiano.

Y, al comparar las normas colombianas (ley 1273 de 2009) en torno a los delitos cibernéticos con la de otros países, se deduce que la ley es y ha sido insuficiente, pues no ha logrado la reducción, la prevención y la mitigación de los daños causados.

PALABRAS CLAVE: **CIBERDELICUENCIA; CIBERCRIMINALIDAD; CIBERDELITO; INTERNET; CIBERESPACIO.**

INTRODUCCIÓN

En el sistema penal colombiano, con la ley 1273 de 2009, se crea un nuevo bien jurídico denominado “de la protección de la información y de los datos”, pero se hace necesario analizar esa intervención estatal sobre los sistemas informáticos y los continuos desarrollos tecnológicos para encontrar la utilidad de las normas que eviten el fraude, el uso del software malicioso, entre otras muchas conductas ilícitas que se encuentran tipificadas en el Código Penal colombiano.

Al afirmar esto se debe proponer una manera de actualizar las normas a la par con el desarrollo de la tecnología y los avances que tienen o han tenido gran influencia en la sociedad contemporánea. Como consecuencia de lo anterior, se genera la necesidad de crear nuevos seguros que garanticen, no solo la debida protección de la información brindada en la red, sino también el pago de los daños que puedan producir quienes hacen mal uso de los datos encontrados en las redes públicas y privadas.

Por lo anterior, se tiene como objetivo general identificar, a partir de un análisis del derecho comparado, la pertinencia de las normas de prevención de los delitos informáticos. Y como objetivos específicos los siguientes:

1. Examinar la regulación de España en cuanto al control de los delitos informáticos.
2. Analizar la ley 1273 de 2009 frente a “La Protección de la Información y de los Datos”
3. Proponer una regulación acorde al derecho comparado para que complemente la ley 1237 de 2009 y pueda brindarle un apoyo en los vacíos a los que se enfrenta por la evolución constante de la sociedad en el ámbito de la tecnología.

METODOLOGÍA

Esta investigación tiene un enfoque cualitativo, basado en un proceso indagatorio, que utiliza datos recolectados sin medición numérica para resolver la pregunta de investigación.

Algunas de las fuentes de Información utilizadas para el análisis de los objetivo son la indagación en textos encontrados en la red, asesoría con profesores que tienen conocimiento en el tema y un análisis relacional de las normas en países con un contexto similar al colombiano. Esto ha planteado, obviamente, algunas dificultadas en el análisis por la enorme cantidad de información y lo difícil que resulta la síntesis de las ideas allí encontradas.

El nivel de la investigación se desarrolla a través del método hermenéutico. Esto es, se hará referencia a las cualidades, rasgos esenciales y propiedades de la normatividad respectiva a la regulación del “ciberdelito”. En consecuencia, lo que se propone es una interpretación particular de normas jurídicas prexistentes.

Las técnicas de recolección de investigación que fueron usados son:
En primer lugar, el estudio de caso, pues se hace uso de la técnica de investigación que estudia un fenómeno contemporáneo desde su contexto real, con la cual se pretende cumplir con el objetivo específico número 1.

En segundo lugar, la técnica documental para ejecutar los tres objetivos específicos, ya que buscamos adquirir conocimientos a través de información adquirida en documentos relacionados con el hecho a investigar.

Estado del Arte:

El primer antecedente jurídico en Colombia sobre delitos informáticos es el Decreto 1360 de 1989. En este se reglamenta la inscripción de software en el Registro Nacional del Derecho de Autor para regular las reclamaciones por la violación de tales derechos.

Siendo así, entendiendo el software como un elemento informático, las conductas delictivas consagradas en los Artículos 51 y 52, capitulo De las Sanciones, de la Ley 44 de 1993 sobre Derechos de Autor, que indican: "*Incurrirá en prisión de dos (2) a cinco (5) años y multa de cinco (5) a veinte (20) salarios legales mínimos mensuales*" e "*Incurrirá en prisión de uno (1) a cuatro (4) años y multa de tres (3) a diez (10) salarios legales mínimos mensuales*", respectivamente, se tienen como las primeras normas penalmente sancionatorias de dichos derechos de autor junto con las consagradas en la Ley 1360 de 1989.

Con la Ley 599 del 2000 se expide la reforma al Código Penal Colombiano en cuyo Libro Segundo Capítulo séptimo Título III consagra los delitos contra la libertad individual y otras garantías, que trata sobre la reserva e interceptación de comunicaciones (art. 192, 193, 194, 194, 196, 197 del Código Penal).

Posteriormente, llega la Ley 671 de 2001 que constituye un Estatuto para prevenir y contrarrestar la explotación y el turismo sexual con menores de edad. Además, contiene prohibiciones para los proveedores o servidores de redes globales de información. Se trata de prohibiciones simples que le quitan eficacia a la Ley pues no trae sanciones de tipo penal, sino meramente administrativas.

Con miras a remediar lo anterior, el 21 de julio de 2009 se sanciona la ley 1336 "por medio de la cual se adiciona y robustece le Ley 671 de 2001". Le Ley 1336 en su

capítulo VI sanciona los tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil.

Finalmente llega la Ley 1273 de 2009 a complementar el Código Penal y crea un nuevo bien jurídico a través del concepto de "*protección de la información y de los datos*". A partir de este Ley se tipificaron los delitos informáticos en Colombia lo que permite, tanto a las entidades públicas como privadas, enfrentar dichas infracciones adelantado las acciones penales pertinentes en cada caso. Siendo así, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea que ratificaron el Convenio sobre Cibercriminalidad (primer tratado internacional referente a los delitos informáticos suscrito en Budapest, Hungría en el año 2001 y con vigencia desde julio de 2004).

HIPÓTESIS

La existencia de una ley (Ley 1273 de 2009) que pretende regular y evitar el ciberdelito resulta conducente y pertinente, pero no reporta la utilidad deseada. El mundo cibernético cambia tan rápidamente que resulta difícil para las entidades estatales estar presentes en cada uno de los ilícitos, perseguirlos penalmente e incluso prevenirlos. Además, los cambios sociales y las formas de contrato por vía electrónica dan lugar, no solo a nuevos tipos de daño, sino también a que los conceptos contractuales tradicionales resulten anticuados. De esta forma, las nuevas necesidades que generan los avances tecnológicos multiplican los riesgos y, por lo anterior, es espera una respuesta eficiente del Estado.

Justificación:

Es necesario hablar hoy de ciberdelito y hacerlo a partir del reconocimiento de unas nuevas formas de delitos asociados con:

- El desarrollo de la tecnología de las comunicaciones
- La globalización de las actividades económicas y productivas
- La capacidad que tienen los delincuentes para traspasar las barreras nacionales.

De esta manera, el cibercriminal se relaciona con la actividad social y empresarial, porque aquel se nutre, como lo expone Felson (2012) en la introducción al texto de Miró (2012), de las actividades legales y de la enorme estructura de la vida cotidiana.

De ahí surge, como premisa, la necesidad de comprender el ciberdelito como fundamento para su prevención. Por ello, es indispensable entender las formas como las personas interactúan dentro del ciberespacio, dónde y cómo trabajan y el conocimiento de las relaciones generadas por su uso, frecuente y permanente, con los patrones de la vida diaria. Asimismo, se debe reconocer que todo esto hace a las personas vulnerables frente a los delincuentes, por el riesgo que asumen al usar los sistemas informáticos.

El uso de los ordenadores (hoy por hoy extensible a las tabletas y teléfonos inteligentes) aumenta y multiplica los fallos de los usuarios y las limitaciones que deben afrontarse en la vida diaria. El ciberespacio (gracias al desarrollo de las redes de comunicación y de los instrumentos para su uso) ha aumentado, lo recuerda Felson (2012) en la introducción al texto de Miró (2012), el número de víctimas de distintos punibles, sin que exista, necesariamente, interacción personal. La aparición efectiva de nuevos riesgos en cuanto la sociedad actual esta caracterizada, básicamente, por un marco económico que cambia con frecuencia y por la aparición de avances tecnológicos a nivel global. El extraordinario desarrollo de la técnica ha tenido y sigue teniendo, obviamente, repercusiones directas en un

incremento del bienestar individual, como también las tienen los fenómenos económicos. Sin embargo, conviene no ignorar sus consecuencias negativas, como la configuración del *riesgo de procedencia humana como fenómeno social estructural*. Ello, por el hecho de que buena parte de las amenazas a las que los ciudadanos nos encontramos expuestos provienen precisamente de decisiones que otros conciudadanos adoptan en el manejo de los avances técnicos. Es ahí, precisamente, donde radica la importancia de normas claras que se enfoquen en estos nuevos delitos, en los que no existe una relación interpersonal entre victimarios y víctimas. Ataques criminales posibilitados por el ciberespacio y la ausencia de controles por parte de los operadores.

Como lo establece Silva (2011) el Derecho Penal es un instrumento cualificado de protección de *bienes jurídicos* especialmente importantes. Sentado esto, parece obligado tener en cuenta la posibilidad de que su expansión obedezca, al menos en parte, ya a la aparición de nuevos bienes jurídicos, de nuevos intereses o de nuevas valoraciones de intereses preexistentes, ya al aumento de valor experimentado por algunos de los que existían con anterioridad, que podría legitimar su protección a través del Derecho penal. Las causas de la probable existencia de nuevos bienes jurídico penales son, seguramente, distintas. Por un lado, cabe considerar la conformación o generalización de *nuevas realidades* que antes no existían o no con la misma incidencia, y en cuyo contexto ha de vivir la persona, que se ve influida por una alteración de las instituciones económicas del crédito o de la inversión. Por otro lado, debe aludirse al deterioro de *realidades tradicionalmente abundantes* y que en nuestros días empiezan a manifestarse como *«bienes escasos»* (Silva Sanchez, 2001, p. 26)

Si es preciso reconocer que ha habido avance en las legislaciones para proteger a los clientes de software malicioso o de cara a los virus que destruyen y roban información, también es cierto que las normas que los defienden son obsoletas

porque no se adecúan tan rápidamente a los avances tecnológicos como si lo hace el delito.

Urgen, desde esta perspectiva, normas que puedan actualizarse a la par con la aparición de nuevas maneras de delito en concordancia con los desarrollos de la tecnología de las comunicaciones, lo que justifica un estudio que proponga una actualización permanente (casi “en línea”) de las normas como respuesta a las nuevas modalidades de delito y que prevean la facilidad de comparar las normas internacionales con las leyes internas, entendiendo y comprendiendo que ello posibilita la prevención y el juicio apropiado y oportuno para esta nueva forma de delincuencia.

MARCO TEÓRICO

Los neologismos cibercriminales (derivado del término inglés cybercrime), ciberdelito, ciberdelincuencia y cibercriminalidad se acuñan para referirse al fenómeno de la criminalidad asociada con el uso de las tecnologías de la información y la comunicación (TIC), tal como lo expone Miró (2012) que hoy sigue vigente y en parte incomprendida dada su peculiaridad, sus desarrollos y las estrategias que se han propuesto para hacerle frente. El ciberdelito hace parte del mundo contemporáneo y está en permanente expansión, asociado al desarrollo y a la revolución traída por la evolución de las TIC para el manejo de la información, su intercambio y la comunicación dentro de la sociedad actual.

Con la introducción del bien jurídico de la protección de la información y de los datos, se pretenden castigar aquellos delitos “que lesionan o ponen en peligro efectivo la confiabilidad, confidencialidad, la integridad y la disponibilidad de los datos, los

sistemas y las infraestructuras informáticas necesarias para el adecuado funcionamiento social" (Ricardo Posada Maya, 2017, p. 74).

Se trata, entonces, de conductas punibles que pueden tener ocurrencia en un lugar que no es físicamente tangible como lo es la Web, y que, como consecuencia de lo anterior, fortalecen nuevos riesgos, los cuales no son comunes a los delitos físicos tradicionales, y que, adicionalmente, se reproducen en una sociedad vulnerable por su incapacidad y pocos conocimientos digitales. De estas consideraciones surge la necesidad y la importancia de proteger la seguridad de la información como un bien jurídico de naturaleza intermedia, que permita tutelar al mismo tiempo otros derechos constitucionales y bienes jurídicos como el patrimonio económico, la intimidad personal y la autodeterminación informática.

Cuando se habla de cibercrimen en sentido amplio, se hace referencia a la comisión de delitos tradicionales, muchas veces a través de internet, como la extorsión, la difusión de pornografía infantil u otros delitos patrimoniales. Estas formas delictivas se encuentran reguladas, de manera general, en el artículo 58 numeral 17 del código penal por medio del cual se agrava la pena de los delitos que en principio no son informáticos, pero que se realizan empleando medios informáticos.

En sentido estricto, el cibercrimen alude a comportamientos delictivos que inciden, directamente, en un sistema informático tales como el sabotaje o espionaje informático, es decir, se busca castigar el comportamiento que lesiona o pone en peligro, de manera ilícita, la seguridad de la funciones informaticas; sin que esto implique, como requisito indispensable, la lesión o puesta en peligro de otros bienes jurídicos. Desde este concepto, no se habla de delitos tradicionales o comunes, sino de tipologías especiales realizadas a través de procedimientos informáticos, que cambian los esquemas teóricos y probatorias propias de los delitos comunes.

Innegablemente, los cambios sociales que vive la sociedad de hoy, como consecuencia de los avances tecnológicos, tienen un reflejo en la criminalidad como fenómeno social, apunta Miró (2012). Y por eso, para reprochar este accionar doloso o culposo, se obliga a probar la actuación como maliciosa o negligente dentro de los parámetros incardinados al interior del Código Penal, como lo afirma la jurisprudencia del Consejo general del Poder Judicial de España (2015). Esto es, representan un desafío al Derecho Penal, pues su estudio y aplicación no se satisface con la teoría del "delito analógico" y trae como consecuencia una incertidumbre dogmática por las nuevas versiones de los delitos tradicionales, pues tales avances tecnológicos hacen cada vez más compleja la delimitación de las categorías dogmáticas de la conducta punible. De ahí la importancia de definir su tipología dentro del contexto del Código Penal colombiano y la pertinencia de entender el desarrollo de estas nuevas formas delincuenciales.

Las nuevas tecnologías, aunque novedosas siempre, no son nuevas en el contexto del análisis jurídico, porque ellas han traído, como lo anota Cárdenas (2008), nuevos retos a las ciencias jurídicas y conllevan nuevas dificultades teóricas y prácticas. La autora define el término ciberdelito como todo delito que para su comisión requiere, necesariamente, de una red de ordenadores (Internet), lo que hace muy amplio el ámbito delictivo pues conlleva la emisión, la transferencia o intercambio de información, atentados contra la calidad de los datos o la manipulación dolosa de los mismos.

Este concepto obliga, como una primera dificultad, la aplicación del derecho penal de un nuevo espacio territorial, esto es, aquel espacio en donde se ha cometido el delito. Ese espacio ha de entenderse, como lo afirma Cárdenas (2008), como una nueva jurisdicción del Estado que fundamentaría la persecución del ilícito a través de la Internet en todo el mundo. Aparecen en esta afirmación los conceptos de "delitos a distancia", donde la conducta delictual no inicia o tiene principio en el mismo Estado en donde se consuma o de "delitos de tránsito" donde conducta y

consumación ocurren en el extranjero y el Estado es solo lugar de tránsito (la información pasa por un servidor ubicado en este). De ahí surge la problemática en la persecución del delito y en establecer la autoridad competente, por ello la necesidad de precisar cuáles Estados pueden ejercer jurisdicción y aplicación del derecho penal frente al caso concreto que se quiere procesar.

La globalización, proceso de integración cultural, económica y social a nivel mundial, ha desbordado los límites de la imaginación, arrastrando un sinnúmero de logros y de desavenencias, pero ha tenido, indudablemente, la capacidad de homogenizar, de unificar mercados, culturas, sociedades…, como lo anota Díaz (2010). Han ido cambiando, de la mano de los desarrollos tecnológicos, las maneras de los hombres para relacionarse con el mundo y con los otros. De esta forma, no hay fronteras reales, por lo que el lugar físico pasa a un segundo plano y aparece la dificultad de identificar una autoridad real que controle todo lo que ocurre en el ciberespacio. Ese cúmulo de posibilidades que otorga la expansión de las redes, de la virtualidad, también entrega oportunidades sin límites para infringir las leyes, con el agravante de la ausencia de fronteras reales en la comisión del delito. Esto hace que el ciberdelito generalmente vaya un paso más adelante que la autoridad legal para su persecución. Además, parecer ser que este tipo de delincuencia se multiplica cada día.

Entendemos entonces, que las acciones digitales o ciberinteracciones son conductas *deslocalizadas* o *desubicadas físicamente*, pues el ciberespacio como realidad virtual es precisamente un ámbito de interacción lógica. Esto no significa que el autor o usuario conectado, que domina objetiva y positivamente el sistema informático y, por consiguiente, el hecho virtual como tratamiento de información, no se encuentre en un lugar determinado o que siempre se desconozca el lugar en donde tienen origen las instrucciones informáticas. De hecho, la deslocalización ha tenido importantes repercusiones para definir la competencia de los jueces penales de conocimiento que decidirían la responsabilidad penal sobre esta clase de

comportamientos criminales. Así, usualmente tendría aplicación el artículo 43 del Código de Procedimiento Penal que literalmente señala que: "*Cuando no fuere posible determinar el lugar de ocurrencia del hecho, éste se hubiere realizado en varios lugares, en uno incierto o en el extranjero, la competencia del juez de conocimiento se fija por el lugar donde se formule acusación por parte de la Fiscalía General de la Nación, lo cual hará donde se encuentren los elementos fudamentales de la acusación"* (Ricardo Posada Maya, 2017, p. 86).

Como afirma Díaz (2010) cualquier intervención, cualquier política criminal, debe reconocer el terreno de su actuación ("dónde está Internet") y esa es una primera dificultad para la tipificación del delito, así como para la determinación de la competencia y jurisdicción de los Estados. Todo ello lleva a la posibilidad de afirmar que el delito informático (estafas informáticas, creación de programas destructores, envío de virus, saboteo de programas informáticos…) puede realizarse con facilidad, porque los recursos que requiere el delincuente son pocos (un computador y una red) y puede ocurrir en cualquier lugar del planeta. Lo anterior pone de manifiesto la dimensión de estos nuevos delitos, su simplicidad y la multiplicidad de las jurisdicciones para la aplicación de la norma legal, de la ley penal.

Un ejemplo de esta dificultad frente a la ocurrencia de los Ciberdelitos, es el caso Yahoo citado por Díaz (2010):

…en aplicación del principio de territorialidad, el Tribunal de Gran Instancia de París condenó a la empresa Yahoo por la venta en territorio francés de artículos de orientación nacionalsocialista (art. 645.1 CP francés). El alto Tribunal impuso a la mencionada empresa la obligación de destrucción de todos los datos, el bloqueo a los usuarios franceses a la página web y la prohibición de venta de los susodichos artículos. Hasta aquí no existe objeción alguna; el problema era que la empresa Yahoo tenía (y tiene) su sede en territorio estadounidense, y alegó que la orden era imposible de cumplir. Ello porque en EEUU la venta de productos relacionados con

*el nacionalsocialismo no es delito alguno, y los servidores de la empresa se hallaban en dicho país. Igualmente, también se consigue demostrar la dificultad para identificar con seguridad los usuarios franceses que accedían a la página Web en cuestión. Ésta constituye una demostración palpable de los problemas aludidos, incluso plantea la cuestión respecto de que un país tenga o no el derecho de imponer sus leyes a compañías de otro país (principio del mínimo común denominador).(*Pág. 176)

En cuanto a la detección de estos delitos existe una complejidad adicional toda vez que la acción cibercriminal puede ser programada y flexible en distintos planos, esto es, realizada por los sistemas informáticos en la forma, tiempo, repetición y ocasión dispuestos por las instrucciones designadas por el hacker/cracker. En el contexto de un ataque informático, las amenazas generalmente cumplen etapas que van desde la búsqueda de vulnerabilidades de los sistemas y los equipos, hasta actos delictivos concretos, utilizando el sistema contra los datos y la información allí registrada. (Ricardo Posada Maya, 2017, p. 87)

Este tipo de acciones también ha promovido nuevas dinámicas criminales que se traducen en la instrumentalización de cadenas de víctimas inconscientes para la realización del delito, mediante el uso de sus sistemas informáticos. Se trata, técnicamente, de *ataques* distribuidos, mediante los cuales se utilizan automáticamente redes de computadores infectados, sin conocimiento o de sus usuarios titulares lo cual, desde la perspectiva del desvalor de acción objetivo, comporta una forma particular de ejecutar los delitos que facilita su comisión y la producción de sus efectos frente a la comunidad titular de los derechos a la disposición, el acceso y el tratamiento de información confiable e integral. Así ocurre, por ejemplo, en la suplantación de sitios web para capturar datos personales. Es evidente que la conducta humana, como base de la conducta en el cibercrimen ha cambiado como objeto que se desvalora en las distintas categorías del delito, por lo que sus características deben ser objeto de una precisa

caracterización dogmática por parte de la doctrina nacional, que permita combatir y estudiar adecuadamente estas fenomenologías criminales. (Ricardo Posada Maya, 2017, p. 88)

Se entiende entonces que, en algunos tipos penales, además de verificar la presencia del autor físico que produce un peligro o causa un resultado, es imprescindible que dicho autor realice la conducta en calidad de usuario de un sistema informático o en calidad de ciberautor que se denominaría cibernauta, o sea, un usuario es aquel sujeto funcional que utiliza su identidad digital y la de sus dispositivos, mediante una conexión virtual a los sistemas que le otorgan privilegios informáticos y jurídicos, para interactuar en el ciberespacio con el fin de tratar información u obtener servicios para llevar a cabo determinadas finalidades, que en este caso desencadena en actos delictivos dolosos. cuando se habla de un sujeto idóneo o capaz para la realización de cibercrímenes, no solo se está haciendo referencia a conocimientos especiales informáticos, sino que realmente esté conectado virtualmente al sistema y pueda dominar lógicamente el tratamiento de información con fines ilícitos. (Ricardo Posada Maya, 2017, p. 89)

Regulación de España en cuanto al control de los delitos informáticos.

A pesar de que en España los delitos informáticos se encuentran tipificados en el Código Penal, debido al enorme incremento de casos y al desarrollo de diferentes formas de delinquir, las autoridades se han visto obligadas a actualizar constantemente la norma.

En dicha normativa española podemos identificar artículos como:

- **Artículo 197** que hace referencia a los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

- Los **artículos 248 y 249** versan sobre estafas. Más específicamente, el **artículo 248.2** contempla las estafas realizadas a través de maniobras informáticas.

- **Artículo 189** corresponde a las medidas que serán impuestas a aquellos que se valgan de menores de edad o incapaces para cometer actos delictivos tales como exhibicionismos o pornografía.

- El **Artículo 270** profiere la penalidad a la que serán sometidas las personas que reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad, de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros.

Estos artículos son una pequeña porción de lo que regula el Código Penal español en cuanto al ciberdelito que ha tenido cifras altísimas en los últimos años. El motivo fundamental del acrecentamiento del ciberdelito es que *"cada vez existen más usuarios conectados a las redes sociales y, debido al abaratamiento de las conexiones, tienen un mayor acceso a Internet"* (Aldama, C.).

Por lo anterior, existen otras normas que hacen referencia a las conductas que constituyen ciberlincuencia, tales como:

- Ley Orgánica de Protección de Datos de Carácter Personal.
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.
- Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- Ley General de Telecomunicaciones.
- Ley de Propiedad Intelectual.

- Ley de Firma Electrónica.

La última actualización que realizó la legislación informática española fue con el Acuerdo GOV/143/2018 de 27 de noviembre del mismo año. Allí se promueve el programa “Internet Segura” para concientizar a la ciudadanía sobre el manejo adecuado y seguro de las redes y, además, se crea la Comisión de Coordinación Interdepartamental del Programa Internet Segura que se encuentra adscrito al Departamento de Políticas Digitales y Administración Pública.

Es un hecho que los métodos, las técnicas y las herramientas que disponen hoy los ciberdelincuentes son tan amplias y de tan fácil acceso que el delito parece multiplicarse en tantas formas que una legislación debería estar permanentemente adecuándose para combatirlos y para cuidar el patrimonio de la sociedad. Cada vez es más fácil el hurto (sin que medie algún tipo de arma o violencia), la suplantación de identidad, la estafa, los ataques contra el buen nombre y la reputación… una lista creciente de nuevas formas de crimen que atentan contra la confidencialidad, la integridad y la disponibilidad de la información, activo principal de la sociedad moderna.

Resulta claro, entonces, que la legislación colombiana adolezca de una normatividad con efectividad continua y actualizada que abarque todos los ámbitos de la seguridad informática y que facilite la sanción oportuna de este tipo de incidentes y de los daños que se causan al desarrollo y crecimiento de la nación. Pero la ley 1273 de 2009 es un acercamiento, por la tipificación de los delitos (aunque con el desarrollo de la tecnología y el crecimiento y diversidad de los delitos resulta hoy pobre e insuficiente) y por la inclusión de nuevas modalidades de estos, como la interceptación ilícita, el fraude informático, la pornografía infantil (que la distingue de otras normas expedidas en países cercanos como Chile, Venezuela y Argentina, tal como lo analiza Castillo (2017)). Pero se queda corta en sanciones referidas a algunos aspectos que hoy son de gran cotidianidad e importancia en la sociedad.

Para Castillo (2017) la ley 1273 resulta desactualizada y urgen acuerdos para que las normas vayan a la par con las realidades del delito en la sociedad moderna, para que se constituya en un bien jurídico y aporte herramientas acordes a las necesidades de enfrentar el cibercrimen. Además de requerirse autoridades competentes (con conocimientos especificos en informatica y estudios teconologicos) para la tipificación de las denuncias y el manejo de estas, porque, como se ha expresado suficientemente, hay una enorme dificultad en la investigación y el castigo dada la ocurrencia de delitos en lugares más allá de las fronteras o en lugares distintos a donde se hace la denuncia.

La ley 1273 de 2009 frente a "La Protección de la Información y de los Datos"

El delito informático apunta, en esencia, a la seguridad de la información. Entendiendo que esta es vital en la vida de las empresas modernas y para todos los ciudadanos. Hacerle frente a esta nueva modalidad de delito obliga al diseño e implementación de políticas de seguridad, con estándares internacionales, que mitiguen los daños que estos causan y que ayuden a prevenirlos.

Políticas que van de la mano de normas y leyes dentro de los códigos penales de cada país y donde las sanciones, penales y/o económicas, resarzan los daños causados y desestimulen la comisión de nuevas formas de delitos cibernético que se traducen en altos costos para las empresas y en deterioro o perdida de la información necesaria para la realización de actividades vitales para la economía de las naciones.

La Ley 1273 de 2009 enfocada, como lo enuncia su título, en la protección de la información y de los datos es un intento para insertar en la legislación colombiana modelos y normas, a la par con lo que ocurre internacionalmente, que faciliten la lucha contra el delito informático y su penalización, mirando su evolución y su

incidencia dentro de un marco siempre cambiante y en continuo desarrollo a la par con la tecnología de las comunicaciones.

La Ley 1273 tuvo antecedentes en el decreto 2360 de 1989, como lo recuerda Sánchez (2017), que reglamentaba la inscripción de software en el Registro Nacional de Derechos de Autor. Primer paso para proteger las violaciones al derecho de propiedad intelectual en las soluciones relacionadas con la informática y las nuevas tecnologías. Luego, con la Ley 599 del 2000 se expide la reforma al Código Penal Colombiano el cuyo Libro Segundo Capítulo séptimo Título III consagra los delitos contra la libertad individual y otras garantías, que trata sobre la reserva e interceptación de comunicaciones (art. 192, 193, 194, 194, 196, 197 del Código Penal).

Lo cierto es que poco a poco se fue volviendo más importante la información, porque en ella se incluían datos personales y datos vitales para la seguridad de las naciones y las personas. El delito pasó de la simple copia o uso de software a ataques contra la integridad de la información, base de cualquier toma de decisiones políticas o económicas, a todos los niveles de la vida cotidiana de la sociedad moderna. El delito se ha ido adaptado a las tendencias del mercado tecnológico. Inicialmente, en los albores de la expansión de la comunicación computacional, eran el espionaje, el sabotaje, la manipulación y el fraude, ataques a la propiedad intelectual, o de autor, los delitos castigados y tipificados por los códigos penales. Hoy tienen una nueva tipología, que va de los delitos de pornografía infantil, acceso a información reservada o privada, ataques a la seguridad de las personas, a su privacidad, software malicioso, usurpación de identidad, robo de cuentas bancarias… Razón por la cual las legislaciones han debido clasificarlos y darles un tratamiento de acuerdo con sus características, su forma de materializarse y a enumerar unas sanciones acordes con la comisión de los delitos.

En Colombia, afirma Sánchez (2017), la Ley 1273 de 2009 tipificó y clasificó, en un primer momento, los delitos informáticos más comunes para el mundo moderno en donde los sistemas tecnológicos determinan el desarrollo de las actividades productivas, económicas y sociales de la comunidad.

Se hace referencia entonces, al acceso abusivo a sistemas informáticos (art. 269A), cuando hay intromisión a ellos violando la seguridad del administrador que busca proteger su almacenamiento y su procesamiento. Esto es, se ingresa en un sistema informático o "red de datos" sin autorización del prestador del servicio, poniendo en riesgo la calidad de la información almacenada, vital para el sistema mismo, para las organizaciones o a las empresas.

Por otra parte, la obstaculización al funcionamiento o acceso normal al sistema informático, a los datos o a una red de comunicaciones (art. 269B), con el objetivo de robar o borrar información, realizar daños en escala en los servicios de la red (acto normal a quienes implantan software malicioso o a quienes "hackean" los sistemas). Será delictiva, además, la interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático (art. 269C), sin orden judicial, para copiar información confidencial, así como los daños informáticos, cuando sin autorización se destruyen, dañan, borran, deterioran, alteran o suprimen datos informáticos (art. 269D).

También se castiga, de cara a la legislación actual, el uso de software malicioso u otros programas dañinos, con la pretensión de dañar información (art. 269E). La violación de datos personales, a su vez, se tipifica en los siguientes términos: (art. 269F) "…*quien, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes*…"

El artículo 269G de la Ley 1273 habla de la suplantación de sitios web cuando describe actividades que se realizan con un objetivo ilícito y sin que se esté facultado para el diseño, desarrollo, trafico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventas emergentes… Es lo que se llama en el argot Phishing,(técnica de ingeniería social para obtener información confidencial, como nombres de usuarios, claves, contraseñas, detalles de tarjetas de crédito) que hace parte de los ataques a redes sociales o a la generación de fallos humanos o errores en beneficio propio.

Igualmente, los hurtos mediante el uso de recursos informáticos o similares (art. 269I). Se amplía en éste concepto el ámbito del hurto cibernético, ya contemplado en el Código Penal y penas establecidas en el artículo 240, cuando dice: "*El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecido*s."

El artículo 269J habla de la transferencia no consentida de fondos, delito en el que el delincuente usa herramientas y medios electrónicos para afectar el patrimonio de personas o empresas.

Esta tipificación de delitos, aunque a la vista de hoy parece corta, manifiesta las múltiples formas de delito electrónico facilitadas por el auge de la informática y las telecomunicaciones. De ahí que surja como necesidad la protección del acceso a la información y al buen uso de esta.

Proponer una regulación acorde al derecho comparado para la ley 1273 de 2009.

Como se dijo previamente, al estudiar la legislación española referida a los delitos informáticos, es preciso una metodología que facilite una permanente actualización de las normas, porque el incremento y la variedad de los delitos informáticos y el enorme desarrollo de los medios virtuales así lo obligan.

No basta entonces una enumeración sumaria de los delitos tipificados, porque esta queda corta frente al desarrollo de la virtualidad y la penetración de la tecnología en la vida contemporánea. De ahí que resulte primordial la creación de jurisprudencia, que apunte a cada una de las posibilidades dentro del marco legal, ya regulado. Y tampoco son suficientes, como instrumento de disuasión, unas penas que resultan irrisorias por la falta de atención al detalle en cuanto su identificación, detección, defensa y sanción de cara a la violencia siempre creciente, que el delito informático produce en las víctimas, toda vez que, el articulo 58 menciona estos delitos de forma general y superficial, facilitando el ataque pero encontrando dificultades en la defensa y persecusión del delito para su efectiva sanción.

Es, en primer lugar, primordial la protección de la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos. Y su protección debe realizarse con el apoyo de la comunidad internacional, pues los delitos ocurren sin mediar territorialidad. Es urgente, en consecuencia, obligar a las empresas prestadoras de servicios en Internet a aceptar su responsabilidad frente al mal uso de sus recursos. Esta pelea se está dando, pero no ha sido suficientemente apoyada por todos los países, que solamente lo hacen cuando sus intereses políticos y estratégicos están en juego. De ahí que la confidencialidad, la integridad y la confianza sean presupuestos para el ejercicio de la libertad en un mundo globalizado.

Pero, ¿cómo definir confidencialidad en un mundo completamente abierto? Es acá en donde surge la necesidad de una legislación abierta al cambio, en continuo proceso de revisión. Porque la tipificación de los delitos entra rápidamente en obsolescencia y los delitos informáticos cada vez son más difíciles de prever. Porque, como se citaba anteriormente (Aldama, C.), cada vez hay más usuarios conectados y con mayor acceso a las redes lo que facilita la comisión de los delitos.

Es necesario, entonces, una continua revisión de la legislación informática, para que tanto el operador judicial como el usuario encuentren puntos de convergencia frente a las realidades delincuenciales. Además, se requiere de una política pública para generar condiciones sociales y culturales en pro de una Internet segura. Para ello deben proponerse unas comisiones que coordinen la actualización de las normas y la propuesta de actividades educativas, desde la escuela, para proteger la vida, honra y bienes de todos los ciudadanos. En especial, estas políticas deben concentrarse en los sujetos más vulnerables: los niños.

Se reitera que la Ley 1273 de 2009 es un enorme acercamiento al problema del ciberdelito, pero ha quedado en el tiempo corta frente al crecimiento y la diversidad de los delitos facilitados por el uso de las redes y la tecnología de la comunicación, pues se entiende como un mecanismo de reacción, pero no de prevención. La tipificación hecha de los delitos ha quedado corta frente impresionante cantidad de nuevas modalidades delictivas que se realizan en el día a día, como la interceptación ilícita, el fraude informático, la pornografía, la violación de la intimidad de las personas, el hurto de propiedad y haberes, el ciberbullying Además, las sanciones propuestas en ella parecen irrisorias ante la gravedad y multiplicidad de los delitos, algunos de ellos rechazados por la sociedad entera como lo son la pornografía infantil con el uso de dispositivos informáticos.

Hay pues la necesidad de acuerdos para actualizar las normas de acuerdo con las realidades que plantean los delitos informáticos en la sociedad actual, para que, de

esta manera, ellas se conviertan en herramientas útiles frente a la necesidad de combatir el cibercrimen.

CONCLUSIONES

El cambio social ha determinado el surgimiento de nuevos riesgos que se materializan en nuevas fenomenologías criminales. Los cibercrímenes representan, justamente, el nacimiento de comportamientos que, en su sentido puro, como delitos informáticos en sentido estricto, tienen lugar en realidades virtuales o simuladas como el ciberespacio. Por ello, las legislaciones de hoy protegen objetos inmateriales como los datos y la información y tutelan nuevos bienes jurídicos intermedios. Si a ello se suma el hecho de que estos delitos son realizados mediante técnicas particulares (que en muchos casos consisten en la manipulación de energía o *bytes* basados en sistemas binarios, que pueden ser traducidos a los humanos mediante infraestructuras informáticas o Hardware), se aprecian delitos que distan mucho de ser asimilables a los delitos tradicionales.

La protección de las funciones informáticas como sustrato material del bien jurídico seguridad de la información, marcan una diferencia esencial. En efecto, se trata de proteger un bien jurídico dinámico que exige cambios o mejoras en las estructuras formales y materiales de la tipicidad 'analógica', es decir, en los requisitos objetivos y subjetivos que debe cumplir una acción física que usualmente tiene lugar y causa efectos en el mundo exterior. El primer cambio perceptible es el fortalecimiento de la ciberacción (o más bien de la interactuación virtual en el ciberespacio, como ámbito deslocalizado y desregulado que dificulta la determinación del tiempo y lugar de los delitos), entendida como aquella acción virtual, interactiva/reactiva, automática, programable, masiva, anónima, etcétera, que involucra la introducción de instrucciones lógicas por parte de un autor - usuario a un sistema informático o telemático con el fin de tratar información. Cuando se transforma la naturaleza de la acción se define de manera distinta la percepción del delito y su propia dinámica de ejecución. (Ricardo Posada Maya, 2017, p. 106)

Al comparar las normas colombianas (ley 1273 de 2009), en torno a los delitos cibernéticos con la de otros países, se deduce que la ley es y ha sido insuficiente, porque no ha logrado la reducción, la prevención y la mitigación de los daños causados, tanto porque la ley misma no alcanzó a incluir todos los aspectos relacionados con el cibercrimen como porque no facilitó la adaptación de las normas al desarrollo de las nuevas modalidades del delito informático.

La ley no incluye por ejemplo, como lo identifica Castillo (2017), una clara definición de la amplia gama de los delitos informáticos que sirvan de referencia y consulta a la autoridad competente en el momento en que tengan procesos en donde haya elementos probatorios de hechos cometidos por delitos informáticos. Esto es, urge ampliar el contexto de la ley para adecuarla al momento de la sociedad actual, porque para el delincuente se han facilitado los medios para atentar contra el bien ajeno y para la sociedad, apoyada en sus autoridades y sus normas, es más lento el proceso, más difícil la investigación por la carencia de leyes que identifiquen y sancionen daños a bienes muchas veces intangibles.

No obstante, al mirar y analizar la Ley 1273 de 2009 es fácil deducir cómo Colombia, en la normatividad propuesta, prevé maneras para enfrentar un delito que, hoy por hoy, es de una enorme vigencia. Además que actualiza la normatividad, respondiendo a los cambios en los delitos, a las nuevas tipologías, de acuerdo con lo que ocurre en los países más desarrollados en el uso de la tecnología para los juegos de azar y para la realización de muchas actividades económicas.

Sin embargo, es claro que en nuestro país falta todavía una normatividad que sea capaz de comprender todos los ámbitos de protección y seguridad en la red, para así poder sancionar de forma adecuada las infracciones que se cometan, pues la presente Ley deja por fuera algunos aspectos en tanto la sociedad y la realidad se van transformando y avanzando.

De ahí que urge una propuesta en pro de mejorar la capacidad de intervención de los operadores judiciales. Sin una preparación de estos es imposible que las normas

se constituyan en verdaderas herramientas para combatir la delincuencia con el uso de las redes y la tecnología de las comunicaciones.

La mejor manera de prevenir y mitigar algunos de los daños causados por el mal uso de la tecnología de las comunicaciones es la educación. Aquella que se enfoca en educar para proteger la intimidad, para construir sociedades incluyentes y socialmente responsables.

Porque las normas solo serán útiles cuando la autoridad sea competente en la tipificación de las denuncias, en la capacidad para la investigación y en la posibilidad de castigar el delito, sin importar donde haya ocurrido. Pero, al mismo tiempo, la efectividad de las normas dependerá de la capacidad que desarrollen los ciudadanos, a través de la educación, para proteger su información.

Resulta necesario que las autoridades permitentes realicen un análisis a la Ley 1273 de 2009 para considerar la posibilidad de reformas, tanto modificación como adición de artículos, para una adecuada protección del bien jurídico, acorde con las necesidades que vienen emparejadas con las nuevas modalidades de ciberdelicuencia.

Es urgente que Colombia se ponga a la vanguardia de los avances tecnológicos y las respectivas normatividades a nivel mundial para enfrentar el delito, pues si bien cada país es diferente, la ciberdelicuencia ha tomado ventaja en todo el mundo y es deber apoyarse mutuamente para combatirla de forma adecuada. La normatividad colombiana debe analizarse desde el derecho comparado, ya que, a través de otras regulaciones, podemos dar cuenta de qué nos hace falta para disminuir esta forma de delinquir.

De acuerdo con esta visión hay cuatro aspectos que ameritan considerarse:

- La conformación de grupos interdisciplinarios que faciliten la adecuación de las normas de acurdo con la evolución de los ciberdelitos, la comparación con otras normatividades y la formulación de estrategias para combatir el delito informático.

- Una permanente formación a los operadores judiciales que les facilite la tipificación de los delitos, su investigación y su castigo.

- Educar, desde la escuela, a los jóvenes para el uso responsable de los medios de comunicación. Para que esta herramienta se convierta en medio de integración y de construcción de sociedades libres e igualitarias.

- Y, establecer vía legislativo la urgencia de una revisión máximo cada dos años de la misma ley para adecuarla a los nuevos tipos delincuenciales, de acuerdo con la dinámica del cibercrimen en la sociedad actual.

- Finalmente, es necesario complementar las categorías tradicionales del delito en la tipicidad, con una perspectiva digital que, por cierto, ya no es la excepción a la regla sino que comienza a ser la regla general en la criminalidad moderna. Esto incluso en ámbitos hasta ahora reservados a la criminalidad física, como la criminalidad organizada y transnacional, que comienza a actuar mediante organizaciones virtuales transnacionales (OVT) que dificultan aún más combatir este tipo de delincuencia sin fronteras.

BIBLIOGRAFÍA

Miró Llinares, F. (2012). El Cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Recuperado de: https://s3.amazonaws.com/academia.edu.documents/34357240/el_ciberespacio_fenomenologia.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1553978942&Signature=wqPlcf1NlsWhMr3%2FkvuZQ4TwrNA%3D&response-content-disposition=inline%3B%20filename%3DEl_Cibercrimen._Fenomenologia_y_crimin ol.pdf

Cárdena Aravena, C. (2008). El lugar de comisión de los denominados ciberdelitos. Recuperado de: http://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf?sequence=1&isAllowed=y

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest. Descargado de: https://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf

Castillo, z. n. (2017). Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en colombia. obtenido de universidad nacional abierta y a distancia —unadǁ escuela de ciencias basicas e ingenieria:

https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11943/1/1053323761.pdf

Informáticos, A. d. (2012). Legislación sobre delitos informáticos en españa. Obtenido de delitosinformaticos.com: https://delitosinformaticos.com/legislacion/espana.shtml

HISCOX. (s.f.). Obtenido de hiscox.es: https://www.hiscox.es/tipos-delitos-informaticos-espana

Arteaga, S. (11 de septiembre de 2015). Los diez delitos informáticos más comunes en España. Obtenido de Computer hoy: https://computerhoy.com/noticias/software/diez-delitos-informaticos-mas-comunes-espana-34061

Legislación Informática de España. Delitos Informáticos. (noviembre de 2018). Obtenido de informaticajuridica.com: http://www.informatica-juridica.com/legislacion/espana/delitos-informaticos/

Consolidada, L. (2015). BOE. Obtenido de boe.es: https://www.boe.es/buscar/pdf/2015/BOE-A-2015-3439-consolidado.pdf

Informático, D. d. (2019). delitos informaticos . Obtenido de http://www.delitosinformaticos.info/delitos_informaticos/legislacion.html

Cuervo, J. (junio de 2015). Código Penal Español. Obtenido de informaticajuridica.com: http://www.informatica-juridica.com/codigo/codigo-penal-espanol/

cuervo, J. (1 de enero de 2014). LEY ORGÁNICA 10/1995, DE 23 DE NOVIEMBRE, DEL CÓDIGO PENAL. Obtenido de http://www.informatica-juridica.com/ley/ley-organica-10-1995-de-23-de-noviembre-del-codigo-penal-2/

Cuervo, J. (29 de octubre de 1992). LORTAD Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. (BOE. 262 del 31 octubre 1992). Obtenido de informaticajuridica.com: http://www.informatica-juridica.com/ley/lortad/

Cuervo, J. (1 de enero de 2014). obtenidos a partir del ADN. Legislacion Informatica de España. Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN. Obtenido de informaticajuridica.com: http://www.informatica-juridica.com/anexos/legislacion-informatica-de-espana-ley-organica-10-2007-de-8-de-octubre-reguladora-de-la-base-de-datos-policial-sobre-identificadores-obtenidos-a-partir-del-adn/

Cuervo, J. (1 de enero de 2014). Ley Orgánica 5/2010, de 22 de junio de 2010, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Obtenido de informaticajuridica.com: http://www.informatica-

juridica.com/anexos/ley-organica-5-2010-de-22-de-junio-de-2010-por-la-que-se-modifica-la-ley-organica-10-1995-de-23-de-noviembre-del-codigo-penal/(s.f.).

Sánchez Castillo, Z. N. (2017). Análisis de la ley 1273 de 2009 y evolución de la ley con relación a los delitos informáticos en Colombia. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11943/1/1053323761.pdf

Ojeda-Pérez, J., Rincón-Rodríguez, F., Arias-Flórez, M., & Daza-Martínez, L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos De Contabilidad, 11(28). Recuperado a partir de https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176

Congreso de Colombia. (2009). Ley 1273 de 2009. Recuperado de: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Gandini, I., Isaza, A., Delgado, A. (2009). Ley de Delitos Informáticos en Colombia. Recuperado de: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Martínez, J. J. (2012). Colombia, el primer país que penaliza los delitos informáticos. Recuperado de: http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980

Montañez Parraga, A. C. (2017). Analisis de los delitos informáticos en el actual sistema penal colombiano. Recuperado de: https://repository.unilibre.edu.co/bitstream/handle/10901/11041/AN%C3%81LISIS%20DE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20EL%20ACTUAL%20SISTEMA%20PENAL%20COLOMBIANO%20revisado%20NHJ%20OK.pdf?sequence=3&isAllowed=y

Rengifo Aguirre, J., Flórez, D., Bedoya López, I. Y., Duque, S. (2013). Delitos informáticos Ley 1273 de 2009. Recuperado de: https://prezi.com/w_jgdngwtqi8/delitos-informaticos-ley-1273-de-2009/

Posada, R. (2017). Nuevo Foro penal No 88: El cibercrimen y sus efectos en la teoria de la tipicidad: de una realidad fisica a una realidad virtual

Sanchez, S. (2001). La expanción del Derecho Penal aspectos de la politica criminal en las sociedades post industuales