Ciberdelincuencia: a propósito del derecho penal informático en Colombia

Cybercrime: About Computer Criminal Law in Colombia

CRISTIAN DAVID ARTEAGA GONZÁLEZ*

CIt a r Como: Arteaga González, C. D. (2021). Ciberdelincuencia: a propósito del derecho penal informático en Colombia. *Episteme. Revista de divulgación en estudios socioterritoriales*, *13*(1). https://doi.org/10.15332/27113833.8322

Recibido: 10/08/2020 Aceptado: 01/03/2022

RESUMEN En el presente artículo se realiza un análisis conceptual y propositivo sobre la ciberdelincuencia que tiene lugar en Colombia, centrándose esencialmente en tres aspectos principales, primero, establecer de forma concreta cual es el alcance de las conductas punibles desplegadas mediante el uso de las tecnologías de la información y las comunicaciones, segundo, desarrollar una aproximación conceptual a la diferencia que debe existir entre los delitos comunes materializados a través de las t ICy los delitos informáticos *stricto sensu*, y finalmente, analizar la regulación colombiana referente al tema de delitos informáticos propiamente dichos y el bien jurídico que protegen.

Palabras clave: delito, ciberdelitos, delitos informáticos.

ABSTRACT In this article, a conceptual and purposeful analysis of cybercrime that takes place in Colombia is carried out, essentially focusing on three main aspects, first, to establish concretely the scope of punishable behaviors deployed through the use of information and communication technology; second, to develop a conceptual approach to the difference that should exist between common crimes materialized through ICt s and *stricto sensu* computer crimes; and finally, analyze the Colombian regulation regarding the topic of computer crimes themselves and the legal right they protect.

Keyword: crime, cybercrimes, computer crimes.

Introducción

Con la llegada de la cuarta revolución industrial, la masificación del internet, de las redes sociales y de espacios como el denominado metaverso, surge un mundo de relaciones sociales paralelo e intangible a lo que hasta ahora se conocía como el mundo real y palpable, en dicho espacio las personas tienen la oportunidad de realizar casi todas las interacciones sociales conocidas, entiéndase hablar, enamorarse, coquetear, discutir, enseñar, celebrar contratos y ejecutarlos, entre otras tantas. Así, se materializa lo que sería una vida en sociedad digital, que rompe los límites de la distancia, gracias a la inmediatez garantizada por las tecnologías de la información y las comunicaciones (t IC).

De ahí la necesidad de crear el derecho de la informática, siendo esta la rama del derecho que tiene por objeto regular todos los ámbitos donde los sistemas informáticos estén presentes. La definición aportada no tiene discusión en la doctrina, aunque se puede afirmar que se trata de un concepto general, tanto en lo referente a sistemas informáticos, que se entienden en el sentido más amplio, es decir, se incluyen prácticamente todos los equipos que guarden relación con las nuevas tecnologías; como en la expresión referida a los ámbitos donde se encuentran presentes, que son, hoy en día, prácticamente todos.

En esa línea, además de los cambios positivos de la globalización y la instantaneidad de la información y la comunicación, también se han importado al mundo digital las conductas más graves y reprochables exhibidas por el ser humano, verbigracia, acosar, amenazar, extorsionar, divulgar pornografía infantil, calumniar, injuriar, hurtar, vulnerar la privacidad, etc. Los que antes del fenómeno informático se conocían simplemente como delitos y, ahora de forma más o menos precisa se busca denominarlos como ciberdelitos, delitos informáticos o delitos a través de las t IC, los cuales por el aumento radical en su realización se han vuelto un fenómeno de alta importancia social y de un enfoque especial en términos de política criminal de la mayoría de los estados y en especial del Estado colombiano.

Por ende, el derecho penal informático, entendido como una herramienta de control social que busca regular la vida en sociedad y garantizar la protección de bienes jurídicamente relevantes, mediante la prevención y la coacción, tiene la obligación de responder de forma certera, eficaz y oportuna a todos los cambios relevantes de la sociedad, siempre con la finalidad de mantener la paz y la estabilidad de su sistema democrático y de las garantías individuales de sus ciudadanos.

* Abogado Cum Laude de la Universidad Santo Tomás, sede Villavicencio. Auxiliar de investigación adscrito a la dirección general del Grupo de investigación en derecho procesal "Octavio Augusto Tejero Duque" capítulo Villavicencio del Instituto Colombiano de Derecho Procesal, coordinador de la sublínea especializada en Derecho Procesal Penal. Investigador de la iniciativa Primeros en f Ia DI (Federación Iberoamericana de Asociaciones de Derecho e Informática).

En ese orden de ideas, lo que se busca con la presente investigación, más allá de dar respuestas definitivas, es aportar, primero, desde una perspectiva académica al análisis de las problemáticas existentes, y segundo, desde una perspectiva propositiva, aportar a la creación de nuevas posturas, en aras de enriquecer el debate jurídico-académico.

Finalmente, es de suma importancia abordar desde el estudio de la dogmática penal los nuevos escenarios delictivos que afronta la sociedad, entendiendo el deber regulatorio del Estado, de cara a estas nuevas dinámicas. No obstante, sin desconocer, como bien lo contempló Lagares García (2013), que "la fuerte evolución de las tecnologías y su veloz instauración en nuestras vidas, como algo común e indispensable, ha puesto en evidencia la lentitud con la que la Ciencia Jurídica responde tras realizarse el cambio sociológico" (p. 40). La lentitud del Estado frente al fenómeno del internet y la ciberdelincuencia es evidente en Colombia, donde no es sino hasta el año 2009, con la Ley 1273, que se empieza a hacer un esfuerzo regulatorio interno y hasta el año 2018, cuando el país se adhiere al convenio sobre la ciberdelincuencia de Budapest.

Propuesta de concepto y clasificación

Frente a esta temática, se procurará establecer un desarrollo semántico de los conceptos y su vinculación en términos de *género y especie*. Los conceptos que se estudiarán son, principalmente, los siguientes, sin perjuicio que dentro de cada uno de ellos se desarrollen otras definiciones necesarias para su cabal entendimiento:

«Los escenarios delictivos que afronta la sociedad como la ciberdelincuencia son nuevos para el derecho penal.»

1. Delito: como género y extracto primigenio e insoslayable de análisis, se tratará de forma sumaria la noción adoptaba por el ordenamiento jurídico colombiano.
2. Delitos a través del uso, las tecnologías de la información y las comunicaciones: como subgénero, siendo la idea más amplia en la que se relaciona el concepto de delito y el fenómeno de las nuevas tecnologías.
3. Delito informático en estricto sentido: como especie, ligado a la información que reposa en los sistemas informáticos en forma de datos.
4. Delitos comunes en el ciberespacio: como especie, concepto ligado a las redes sociales y al ciberespacio, en los que se desarrollan delitos preexistentes a las nuevas tecnologías.

Del delito

El análisis sucinto de la concepción del delito es de gran importancia, pues como se puede evidenciar, es el elemento transversal a todos los conceptos que de forma posterior se relacionan con las nuevas tecnologías. Ahora bien, la doctrina internacional tiene una postura muy clara y casi homogénea en términos de la teoría del delito para su conceptualización, la cual recoge el código penal colombiano al establecer en su artículo 9 que: "para que la conducta sea punible se requiere que sea típica, antijurídica y culpable. La causalidad por sí sola no basta para la imputación jurídica del resultado" (Ley 599, 2000, art. 9)

En otras palabras, el delito es una conducta desviada, activa o pasiva, que forma parte del conjunto de relaciones sociales interpersonales, con característica negativa y conflictiva en la sociedad,

EPISTEME / ISSN: 2027-7504 / E-ISSN: 2711-3833 / VOL. 13, N.º 1 / ENERO-JUNIO 2021 / 38-47

lo que crea la necesidad estatal de prevenir y castigar su existencia. También puede ser entendido el delito como el injusto culpable[1], a partir de un juicio de desvalor de acción y de resultado.

Los elementos estructurales de la conducta punible se pueden sintetizar de la siguiente manera: en primer lugar, la tipicidad, que refiere objetivamente a que el modelo de conducta esté expresamente establecido en la ley penal como delito, si no lo está, se habla de una conducta atípica y por ende irrelevante en términos del derecho penal, es por eso que es tan importante la tipificación que se hace sobre los delitos informáticos, pues es la base para buscar su prevención, y subjetivamente refiere a la relación psicológica del autor con su conducta, en esta sede se estudian las modalidades de la conducta, dolo, culpa y preterintencional[2]. Por otro lado, está la antijuridicidad, que formalmente refiere a que el acto sea contrario a derecho, y material, es decir, que la conducta lesione o ponga en un riesgo real y efectivo un determinado bien jurídico, en el caso concreto sería el de la información contenida en datos. Finalmente, la culpabilidad deja de juzgar o valorar el acto en sí mismo y pasa a analizar a quién lo llevó a cabo, al hacer un juicio de desvalor de autor, valorar la exigibilidad de conducta y establecer si se está frente a una persona imputable.

1 Tipicidad más antijuridicidad.

2 Entendiendo las modalidades del dolo, directo, indirecto, de eventual y las modalidades de la culpa, con o sin representación.

Delito a través del uso de las TIC

Habiendo hecho una aproximación a la definición de delito, ahora resulta importante abordar qué son las t IC, con el fin de poder dar luces al respecto de lo que son los delitos a través del uso de dichas tecnologías. En esa línea, el artículo 6 de la Ley 1341 de 2009, modificado por el artículo 5 de la Ley 1978 del 2019, facilita el concepto de tecnologías de la información y las comunicaciones adoptado por Colombia:

> **ARTÍCULO 6º. Definición de TIC.** Las tecnologías de la información y las comunicaciones (t IC) son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341, 2009, art. 6)

Como se extrae de la norma, las t IC son un conjunto amplio que abarca desde cualquier sistema informático existente hasta aplicaciones y redes sociales, etc. Por esa razón, y con la finalidad de no dejar ningún tipo de avance tecnológico fuera del concepto, para los efectos de la presente investigación se opta porque sea justamente la denominación t IC el núcleo con el cual se relacionan las nuevas tecnologías existentes y las que se creen después.

Ahora bien, el autor mexicano Julio Téllez Valdez (1996) conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tiene a las computadoras como instrumento o fin" (pp. 461, 474). El concepto del maestro está sujeto a ciertas apreciaciones para los fines del presente trabajo académico:

1. En lugar de atribuirse dicha definición a la idea de *delito informático* debe atribuírsele a la de delito a través de las t IC, pues como se verá más adelante el concepto de delito informático será restringido a cierto número de conductas en concreto, con base en sus características particulares.
2. De la definición del doctor Téllez debe cambiarse el hecho de entender como eje central a los computadores, pues es una idea muy restrictiva de lo que son hoy en día las nuevas tecnologías de la información y las comunicaciones, con fenómenos como el internet de las cosas y el uso masivo de diferentes sistemas informáticos como los *smartphones* (teléfonos inteligentes). Por ende, debe adoptarse el concepto de t IC presentado con anterioridad, en sentido similar a como lo establecieron las doctoras Isabel Anayanssi y Karen Enoe (2015) al decir que "dada la existencia de cada vez más dispositivos tecnológicos incluiremos los teléfonos inteligentes así como las tabletas, independientemente de otros dispositivos producto del avance tecnológico" (p. 186).
3. Finalmente, el hecho de que las t IC sean la finalidad de la conducta o, por otro lado, meras herramientas o medio, va a diferenciar los ciberdelitos, por ejemplo, el acoso sexual mediante aplicativos como Facebook o WhatsApp de los delitos informático como un acceso abusivo a un sistema informático.

Con base en lo anterior, se puede afirmar sin miedo a equivocarse que los delitos a través del uso de las TIC terminan abarcando cualquier conducta en la que se tengan como medio o fin estas tecnologías, entiéndase sistemas informáticos, programas informáticos, aplicaciones, redes sociales, etc., tal y como lo determinó el doctor Álvaro Mendo (2015) al establecer que:

> Sí existen, sin embargo, delitos que están relacionados con las nuevas tecnologías porque, junto a la forma de comisión tradicional, también pueden ser cometidos con el uso de las mismas o porque el objeto del delito son, precisamente, equipos o elementos informáticos. (p. 207)

Con lo anterior, se erige esta idea como la más amplia y completa para hablar del fenómeno de la delincuencia en el nuevo panorama tecnológico. Entonces, dentro de un espectro tan amplio surgen dos ideas a modo de clasificación de las

«Delitos informáticos en estricto sentido, afectan los principios básicos de la información»

conductas que se pueden dar mediante el uso de las t IC, que son el concepto de ciberdelito y el de delito informático.

Delitos comunes en el ciberespacio o ciberdelitos

Para los efectos del presente trabajo, el concepto de ciberdelito se circunscribe a cuando el doctor Julio Téllez dice que se tiene a las computadoras[3] como instrumentos, es decir, es el caso en el que el individuo hace uso de las t ICcon la intención de facilitar la realización de una conducta punible, que bien podría ser realizada mediante otra vía o con otro *modus operandi*, externo a las nuevas tecnologías, pues lo que hace es atacar un bien jurídico tradicional, o nuclear, como la vida, la honra, el patrimonio etc., este tipo de conductas se desarrollan dentro del ciberespacio, en especial, dentro de las redes sociales entendidas como: "complejas estructuras de comunicación establecidas en torno a un conjunto de objetivos que garantizan, al mismo tiempo, unidad de propósitos y flexibilidad en su ejecución gracias a su capacidad para adaptarse al entorno operativo" (Castells Olivan, 2009, p. 46).

En ese orden de ideas, se puede simplificar que una red social es un entramado de relaciones de comunicación e intercambio de información entre seres humanos conectados o vinculados entre sí; el tamaño de dicha red va a ser directamente proporcional al número de seres humanos que decidan

3 En el caso de la postura adoptada en este trabajo, tecnologías de la información y las comunicaciones.

participar en ella. Por otro lado, cuando se refiere a redes sociales dentro del internet o del ciberespacio, se adecúa la definición anterior, pues lo único que varía es que la herramienta que facilita el espacio de conexión entre seres humanos es digital, entiéndase Facebook, Instagram, WhatsApp, Telegram, entre otras; dichas redes sociales digitales, nacen y mueren de acuerdo al interés que la sociedad deposite en el uso de ellas.

Dentro de dicho espacio virtual de relaciones interpersonales, crece el fenómeno del anonimato, pues es tan fácil como crear un perfil con datos falsos o directamente sin datos, lo que ayuda a los delincuentes a emprender sus actos de preparación, ejecución y consumación de la conducta punible, de manera tal que los hace sentir protegidos y fomenta la impunidad por su actuar; además, facilita la realización de delitos desde cualquier parte del mundo y que surtan sus efectos en un lugar totalmente distinto.

Puede tomarse como ejemplo la brillante postura del doctor Leandro Rezende (2015), cuando en su clasificación conceptual explica que los crímenes informatizados son: "las conductas cometidas vía sistemas informatizados para atacar bienes jurídicos ya conocidos y contemplados por el derecho penal" (p. 227), postulando con posterioridad que:

> El aspecto informático, aquí, sirve solamente a una cuestión de *modus operandi*. No es la seguridad de la información el bien jurídico violado o puesto en amenaza, pues la informática es usada como mero instrumento para la práctica del delito que, reitero, ya son figuras típicas. (p. 227)

Lo anterior ciertamente es una apreciación similar, por no decir idéntica de la postura que aborda el presente artículo, pues es cierto que lo que ocurre en este tipo de conductas no es más que el hecho de emplear como instrumento a las t IC, como un medio para la consecución de un resultado lesivo a un bien jurídico, que existía incluso previamente a la aparición de los mismos sistemas informáticos. No es diferente el caso de, por ejemplo, un homicidio, delito que protege el bien jurídico denominado vida; dicha conducta puede desarrollarse con un arma de fuego, un arma blanca, un vehículo, agentes químicos, entre infinitas posibilidades más, sin embargo, no se tiene que hacer una construcción dogmática particular para cada caso, es así que no existe un accidente-homicidio, un veneno-homicidio o clasificaciones típicas por el estilo, a lo sumo puede buscarse sancionar la excesiva gravedad de la violación al ordenamiento jurídico y tipificarse un modelo de ejecución concreto, como una agravante genérico o especial del delito autónomo.

«Las posturas indiferentes, agnósticas o el ateísmo, aparecen comprendidas en el ámbito del derecho a la libertad religiosa»

Características de los ciberdelitos

- Este tipo de conductas no requieren en el autor un conocimiento especializado en informática, razón por la cual cualquier persona de conocimiento medio, con básica preparación en internet y uso de sistemas informáticos, como los computadores o los teléfonos inteligentes, puede desarrollar alguna de estas conductas.
- Estos delitos no son otra cosa que la realización de conductas típicas preexistentes, por ejemplo: 1) acoso sexual; artículo 201 A del Código Penal Colombiano (CPC) o ciberacoso sexual;

2) extorsión, artículo 244 del CPC o ciberextorsión; 3) amenaza, artículo 347 del CPC o ciberamenaza 4) terrorismo, artículo 343 del CPC o ciberterrorismo. Por lo anterior, los bienes jurídicos tutelados en estas conductas son tan variados como delitos existentes, por ello, no se requiere un esfuerzo legislativo en la tipificación de nuevas conductas, pues como se explicó lo único que varía es la manera o el modo de realización del delito mismo.

Delito informático

Los delitos informáticos, en estricto sentido, son aquellos delitos que atacan a los principios básicos de la seguridad de la información, que explica muy bien Leonardo Rezende (2015) como:

> El principio de la *disponibilidad* implica que un determinado sistema estará siempre disponible para solicitudes, en cuanto él da *confidencialidad* garante que los datos serán asesados solo por usuarios autorizados. Ya del principio de *integridad* es la garantía de que el mensaje permanece completo y exacto al final de la transmisión. El principio de la *autenticidad, por su vez,* es lo garante que los datos son verídicos, o que el usuario es legítimo. Finalmente, el principio de *no repudio* es la garantía de que una persona no puede negar su autoría en un acto documento que así esté constando en un sistema. (p. 226)

Además, dichos principios son reunidos también en la Ley 1273 del 2009, y sintetizados en el nuevo bien jurídico tutelado por la norma, 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" (Ley 1273, 2009), con lo que se puede postular que los principios básicos de la seguridad de la información son los que nutren el nuevo bien jurídico constituido por la ley. Así pues, las conductas punibles consagradas en dicho cuerpo normativo lo son en la medida en que afectan alguno o varios de los principios que contextualizan el bien jurídico. Ejemplo de ello es el artículo 269 A de la Ley 1273 del 2009, que establece en su descripción típica que:

> 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. (Ley 1273, 2009, art 269A)

Como puede analizarse, la descripción típica caracteriza de forma taxativa la violación del principio de *confidencialidad* de la información, que garantiza solo las personas autorizadas puedan acceder a ciertos datos resguardados en la seguridad de los sistemas informáticos; de la misma forma el artículo 269B sobre la *Obstaculización ilegítima de sistema informático o red de telecomunicación*, refiere a la violación al principio de *disponibilidad*, así sucesivamente el articulado demuestra que la violación a alguno de estos principios acarrean, per se, la vulneración del nuevo bien jurídico tutelado.

«El bien jurídico tutelado que protege es la información y los datos personales, lo que las hace conductas punibles autónomas.»

Características de los delitos informáticos

- Si bien el sujeto activo en este tipo de delitos es indeterminado, se requiere

conocimiento especializado en programación e informática, para poder incurrir en las conductas descritas.

- Son delitos relativamente nuevos, ejemplo de ello es que no es sino hasta el 23 de noviembre del 2001 que se adopta el denominado convenio de Budapest sobre ciberdelincuencia, como un esfuerzo global para combatir dicho fenómeno, y Colombia lo ratificó mediante la Ley 1928 de 2018 y se adhiere formalmente desde el 16 de marzo de 2020, tal como explica la Cancillería al decir que:

> Colombia fue invitada por el Consejo de Europa para adherirse al convenio el 11 de septiembre de 2013, luego de que el Gobierno nacional adelantara las gestiones pertinentes, las cuales estaban encaminadas a contar con instrumentos jurídicos y de cooperación internacional para enfrentar la ciberdelincuencia, el Estado colombiano se adhirió formalmente el 16 de marzo de 2020, cuando depositó ante el Consejo de Europa en Estrasburgo, el instrumento de adhesión al convenio de Budapest, que es el estándar mundial en la lucha contra la ciberdelincuencia. (Cancillería de Colombia, 2020)

- El bien jurídico tutelado es el de la información y de los datos, lo que hace que sean conductas punibles autónomas, sin embargo, pueden ser realizadas como delitos medios para un delito fin. Por ejemplo, se puede interferir en el sistema informático de un auto Tesla, con la finalidad de tomar el control del vehículo y materializar un homicidio o interceptar información con la finalidad de extorsionar.

« Se requiere conocimiento especializado en programación e informática, para poder incurrir en las conductas descritas »

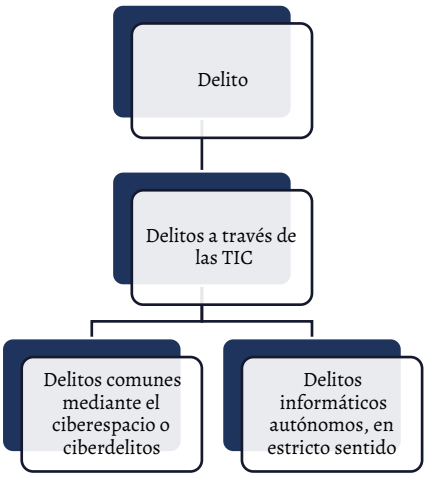
Conclusiones

En conclusión, como género se tiene el delito mediante el uso de las t IC, pues abarca cualquier conducta punible en la que se vean inmiscuidas las t IC, ya sea como medio o como fin. Ahora bien, como especie, se encuentra lo que puede llamarse ciberdelito, delito digital *lato sensu* o delitos comunes a través del ciberespacio, pues no es otra cosa que la realización de delitos previamente existentes, mediante las nuevas herramientas de comunicación, teniendo como finalidad el simple uso de las redes sociales, aplicaciones o ciberespacio para facilitar la comisión del delito.

Finalmente, se encuentran los delitos informáticos en estricto sentido, que son aquellos en los que se afectan los principios básicos de la información, y de la mano de ellos el bien jurídico de la información y de los datos, que, en otras palabras, es la información registrada en un dato. Por ende, son un grupo de delitos muy reducidos y que nace como consecuencia de la existencia misma de las nuevas tecnologías; además,

son conductas autónomas, no obstante, en muchos casos se usan como delitos medios para afectar diferentes bienes jurídicos. Por otro lado, en este espacio de la delincuencia en internet es donde se encuentran los grupos de los denominados *crackers*, especializados por la complejidad de su conocimiento en programación y alteración de *software* y sistemas informáticos.

Figura 1. Cuadro conceptual explicativo



Fuente: elaboración propia.

Referencias

Anayanssi, I y Enoe, K. (2015). Sexting y Redes Sociales: Diversas relaciones y Consecuencias Jurídicas. En F. Bueno de Mata (coord.), *Fodertics 3.0. Estudios sobre Nuevas Tecnologías y Justicia* (pp. 185-196). Comares, S.L.

Cancillería de Colombia (2020, 17 de marzo). Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia. https://shortly.cc/iLxmq

Castells Olivan, M. (2009). *Comunicación y poder.* Alianza .

Código Penal [CP]. Ley 599 de 2000. 24 de julio de 2000 (Colombia).

González Hurtado, J. A. (2013). *Delincuencia informática: Daños informáticos del artículo 264 del Código Penal y Propuesta de Reforma*. Universidad Complutense de Madrid.

Lagares García, D. (2000). *Internet y Derecho.* Carena.

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. 5 de enero de 2009. D.O No. 47223.

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. 30 de julio de 2009. D:O No. 47.426.

Ley 1928 de 2018. Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. 24 de julio de 2018. D.O. No. 50664.

Mendo, Á. (2015). El Cibercrimen en las Redes sociales. Especial Atención a la Suplantación de Identidad. En F. Bueno de Mata (coord.), *Fodertics 3.0. Estudios sobre Nuevas Tecnologías y Justicia* (pp. 205-214). Comares, S.L.

Rezende, L. (2015). Política Criminal en el Ciberespacio: Crítica al Concepto de Crimen Informático. En F. Bueno de Mata (coord.), *Fodertics 3.0. Estudios sobre Nuevas Tecnologías y Justicia* (pp. 215-230). Comares, S.L.

Téllez Valdéz, J. (1996). Los Delitos Informáticos. *Informática y Derecho: Revista iberoamericana de derecho informático*, 1(9-11), 461-474.