Depósito legal ppi 201502ZU4662
Esta publicación científica en formato
digital es continuidad de la revista impresa
Depósito Legal: pp 197402ZU789
● ISSN: 1315-9518 ● ISSN-E: 2477-9431

RCS
Revista de Ciencias Sociales

Universidad del Zulia. Revista de la Facultad de Ciencias Económicas y Sociales
Vol. XXIX No. 2 abril-junio 2023

Revista de Ciencias Sociales

Esta publicación científica en formato
digital es continuidad de la revista impresa
Depósito Legal: pp 197402ZU789
ISSN: 1315-9518

Revista de Ciencias Sociales (RCS)
Vol. XXIX, No. 2, Abril - Junio 2023. pp. 356-372
FCES - LUZ ● ISSN: 1315-9518 ● ISSN-E: 2477-9431

Como citar: Mejía-Lobo, M., Hurtado-Gil, S. V., y Grisales-Aguirre, A. M. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo. *Revista De Ciencias Sociales*, *XXIX*(2), 356-372.

Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones: Estudio comparativo

Mejía-Lobo, Mauricio[*]
Hurtado-Gil, Sandra Victoria[**]
Grisales-Aguirre, Andrés Mauricio[***]

Resumen

La investigación se centró en realizar un derecho comparado entre la ley de delitos informáticos vigente en Colombia, y los punibles de tal naturaleza tipificados en las legislaciones nacionales de Perú, Chile, Alemania y España. Lo anterior, teniendo como guía las disposiciones contenidas en el Convenio de Budapest sobre delitos cibernéticos. A partir de un enfoque cualitativo de corte descriptivo se presenta, en primer lugar, un recuento sobre el contenido y alcance del referido instrumento de derecho internacional; luego, se procede a relacionar la clasificación y composición de las conductas advertidas en la ley 1273 de 2009 de Colombia, por medio de la cual se crea un nuevo bien jurídico tutelado denominado de la protección de la información y datos, adicionalmente la Ley 1928 de 2018, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia. Finalmente, se manifiesta la contextualización de derecho comparado entre la reglamentación nacional y la foránea, según los países elegidos. El desarrollo permitió encontrar diferentes maneras en las cuales los ciberpunibles han sido entendidos y consagrados en las legislaciones de estudio, así como las fortalezas y debilidades que emanan de la tipificación, a efectos de investigar, enjuiciar y sancionar las conductas delictivas virtuales.

Palabras clave: Ley de delitos informáticos; convenio de Budapest; desarrollo legislativo; cibercriminalidad; ciberdelitos.

[*] Magister en Gestión y Diseño de Proyectos. Docente-Investigador en la Universidad Católica Luis Amigó, Manizales, Colombia. E-mail: mauricio.mejialo@amigo.edu.co ORCID: https://orcid.org/0000-0001-9184-0563

[**] Magister en Ingeniería de Sistemas y Computación. Docente en la Universidad de Caldas, Manizales, Colombia. E-mail: sandra.hurtado@ucaldas.edu.co ORCID: https://orcid.org/0000-0003-0788-5086

[***] Magister en Ciencias. Docente-Investigador en la Universidad Católica Luis Amigó, Manizales, Colombia. E-mail: andres.grisalesag@amigo.edu.co ORCID: https://orcid.org/0000-0002-4385-4474

Recibido: 2022-11-02 · **Aceptado:** 2023-01-20

Colombian cybercrime law, the Budapest convention and other legislations: A comparative study

Abstract

The investigation focused on carrying out a comparative law between the current computer crime law in Colombia, and the punishable offenses of this nature typified in the national legislations of Peru, Chile, Germany and Spain. The foregoing, taking as a guide the provisions contained in the Budapest Convention on cybercrimes. From a descriptive qualitative approach, first, an account of the content and scope of the aforementioned instrument of international law is presented; Then, we proceed to relate the classification and composition of the behaviors warned in Law 1273 of 2009 of Colombia, by means of which a new protected legal right called the protection of information and data is created, additionally Law 1928 of 2018, through which the Convention on Cybercrime is approved. Finally, the contextualization of comparative law between national and foreign regulations is manifested, according to the chosen countries. The development allowed to find different ways in which cyberpunishables have been understood and enshrined in the study legislation, as well as the strengths and weaknesses that emanate from the classification, in order to investigate, prosecute and punish virtual criminal behaviors.

Keywords: Computer crimes law; Budapest convention; legislative development; cybercrime; cibercrimes.

Introducción

La transición de medios analógicos a digitales, el acceso continuo a *internet*, la progresiva alfabetización informática y la masificación del consumo de dispositivos electrónicos vinculados a la red, representan algunos sucesos que desde finales del siglo XX han contribuido a reconfigurar, entre otras cuestiones, la forma en la cual los seres humanos interactúan entre sí, y las conductas que cada individuo estima conveniente desarrollar en el contexto de la virtualidad, de acuerdo con sus intereses o plan de vida particular (Hernández, 2012).

Las disciplinas jurídicas, denominación planteada por Coloma (2016), quien afirma que: "Prefiero hablar de disciplinas jurídicas, pues comunica directamente el rol clave que en ellas juega la comunidad de sujetos que la conforma" (p.254) han sido utilizadas con el fin de fomentar el imperio de la Ley en torno a los comportamientos que cada persona, sea esta natural o jurídica, efectúa en el ámbito de las Tecnologías de la Información y la Comunicación (TIC) (Rodríguez, 2015; Centeno et al., 2022). En tal prospecto, la globalización, en su sentido amplio (Grajales y Osorno, 2019), ha contribuido a que diversos gobiernos y órganos multilaterales propendan por la creación y aplicación de instrumentos legales coercitivos, tanto en los ordenamientos jurídicos domésticos, como en las redes globales con acceso a *internet*, con el fin de hacer frente, entre otras cosas, al fenómeno de la ciberdelincuencia (Punín, 2022).

De acuerdo con Fontestad y Jiménez (2021), la referida circunstancia representa una de las formas de más rápido crecimiento de la delincuencia transnacional, la cual se beneficia en el hecho que *internet* se ha convertido en un medio casi indispensable de comunicación

diaria e intercambio de información en todo el planeta. Sin duda, los cinco mil millones de usuarios de *internet* en todo el mundo (según datos de TyN Magazine, 2022) crean el ambiente perfecto para el crimen, máxime cuando se entiende que la *web* es un lugar donde es posible actuar de forma anónima y acceder a cualquier información personal que, voluntariamente o no, sea puesta en línea.

Una muestra fundamental de las tendencias normativas enfocadas a disuadir y combatir los comportamientos que se consideran perjudiciales en la red, se encuentra contenida en el denominado: Convenio de Budapest sobre Ciberdelincuencia (en adelante CBC), el cual, es un:

> Tratado internacional creado en el año 2001 e impulsado por el Consejo de Europa, con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones con el objetivo de hacer frente a los delitos informáticos. (Derechos Digitales, 2022, párr.1)

Tal instrumento se presenta como la respuesta legal del siglo XXI ante la presencia y auge de las conductas criminales, que se sirven de las Tecnologías de la Información y la Comunicación (TIC) para consumar un daño o lesión, ya sea a los sistemas informáticos, o bien a los intereses de individuos y/o corporaciones que ejecutan un significativo número de actividades en los entornos digitales mediante el uso de dispositivos electrónicos (González, 2017). Dicha norma ha favorecido igualmente el surgimiento de una amplia reflexión y debate sobre las ventajas, así como los riesgos que aparejan las telecomunicaciones y el *internet* en una sociedad del conocimiento, globalizada e hiperconectada.

La Convención se proyectó a partir de las consideraciones del Consejo de Europa (CoE), sobre la necesidad de establecer una política criminal ante los delitos cibernéticos, de modo que se procurara la protección de los intereses, prerrogativas y derechos tanto de las personas, sean estas naturales o jurídicas, como de los estados y entes a su cargo (Gascón, 2014). En tal sentido, la posición de esta política criminal prioriza la convergencia y la globalización de las redes informáticas como elementos que han dado lugar a la aparición de actos delictivos, así como la urgencia de cooperación internacional entre países e industrias privadas para el aval del uso, desarrollo y protección de las TIC bajo un interés lícito.

A partir de su promulgación, la referida disposición de derecho ha sido acogida en diferentes ordenamientos jurídicos, tanto por vía de adaptación de los contenidos de la norma a los regímenes domésticos, como por suscripción y adhesión directa al convenio (Benítez, 2021). En tales sendas, no obstante, se ha puesto de presente como criterio primigenio la cooperación internacional para hacer frente a la ciberdelincuencia y a sus múltiples manifestaciones, máxime cuando las mismas atentan de forma multidimensional a los intereses y bienes jurídicamente protegidos de individuos físicos o morales, ya sea por el propio uso que estos realizan de las TIC, o por la forma lesiva en que los ciberdelincuentes emplean estas para tomar provecho de aquellos.

La elección de los países para este estudio se realizó observando dos criterios esenciales: (i) Tomar ordenamientos que fueran parte del CoE y de Suramérica, este último por ser el lugar en el cual se ubica geográficamente Colombia; y, (ii) según los desarrollos normativos relevantes que los Estados seleccionados han dado al CBC, ya sea por vía de adhesión, suscripción o creación de nuevos tipos penales que desarrollan los fines del convenio. Esto, teniendo en cuenta la precisión indicada por Martins (2022), respecto a ser un marco generalmente aceptado a nivel internacional; y a lo desarrollado por Herrera (2018), respecto a la importancia de la actualización legislativa en países latinoamericanos. Según la Organización Derechos Digitales (2022), en la región se encuentra el siguiente diagnóstico:

> Argentina, Chile, Costa Rica, Colombia, Panamá, Paraguay, Perú y República Dominicana son los países latinoamericanos que han suscrito el convenio, mientras que Ecuador, Guatemala, México y Brasil son observadores. Recientemente se presentó el segundo protocolo adicional

> al convenio y actualmente distintos países latinoamericanos están considerando su adhesión. (párr.2)

1. Metodología

La metodología utilizada fue deductiva, exploratoria, utilizando un enfoque cualitativo de carácter descriptivo, donde se presenta inicialmente una referencia sobre el contenido y alcance del CBC, utilizando para tal efecto un recuento sobre su despliegue; luego, se relacionan los ciberdelitos considerados en las Leyes 1273 de 2009 y 1928 de 2018 -por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia; y, por último, se procede a contextualizar el derecho comparado entre la reglamentación nacional y la foránea en los países latinoamericanos de Chile y Perú y en los países europeos de España y Alemania.

Se analizó la estructura y composición del CBC, destacando las 5 clasificaciones que hace de los ciberdelitos, para luego comparar con la estructura y contenido de cada una de las normativas enunciadas; a partir de esto, se identificaron los elementos que llevaron a encontrar las coincidencias y diferencias en cada uno de los elementos tratados y así concluir sobre cada una de ellas, sus fortalezas, debilidades y diferenciales.

2. Resultados y discusión

2.1. El convenio de Budapest y la cibercriminalidad

El auge del *internet* y de los dispositivos digitales trajo consigo nuevas preocupaciones en torno a las acciones consideradas ilícitas en el ciberespacio, así como las debilidades de los sistemas informáticos y de los regímenes sancionatorios para enfrentar la comisión de punibles en tal lugar virtual. Bajo tales circunstancias, como lo explican D'Avila y Dos Santos (2016), la política criminal se tornó insuficiente, y dio lugar a la urgencia de considerar perspectivas con cierto grado de innovación ante categorías circunstanciales del *ius puniendi* que se consideraban pétreas.

Ante tales circunstancias, en su momento el Comité Europeo de Asuntos Penales convocó en 1996 a la conformación del Comité de Expertos en Delitos Cibernéticos para así desplegar la redacción de la Convención sobre Delitos Cibernéticos. La publicación del borrador inicial de la propuesta se hizo en noviembre de 2000, y fue puesta al público a través de *internet* para su discusión. En la quincuagésima reunión del mencionado comité, celebrada en junio de 2001, se sometió a la aprobación del borrador final del Convenio sobre Delitos Cibernéticos, contentivo de cuatro capítulos: El primero, sobre la terminología; el segundo, en torno a diversas acciones materiales de derecho penal y derecho procesal a nivel nacional para los países miembros del CoE; un tercer acápite, sobre la cooperación internacional; y, un cuarto capítulo, que contiene disposiciones de cierre (Rayón y Gómez, 2014).

Como resultado final, en Budapest (Hungría) se instauró el Convenio sobre Ciberdelincuencia (CBC), con fecha de implementación de 23 de noviembre de 2001. Tal instrumento tiene como objetivo producir herramientas legales que se ocupen de los delitos cibernéticos y cooperación internacional para abordar los ciberpunibles.

En esta convención, el ciberdelito se incluye como una forma de criminalizar el comportamiento, el cual comienza, generalmente, con el acceso ilegal y la interferencia con los datos y los sistemas informáticos para fines ilícitos, tal como lo había propuesto Aguilar (2015). Los delitos relacionados incluyen el acceso a computadoras sin autorización, envío y transmisión de información a través de computadoras, y uso indebido de equipos informáticos. De otro lado, la falsificación y el fraude con el uso de computadoras, así como la pornografía infantil, también se incluyen como delitos cibernéticos en esta convención, al igual que las vulneraciones de los derechos de autor y su protección como bien jurídico, determinada en Colombia, como lo presentan

Mondragón et al. (2022).

Las condiciones referidas han dado pie a que, en términos generales, se considere el ciberdelito como toda conducta típica, antijurídica y culpable que, por regla general, requiere como componente del punible la concurrencia del espacio virtual y/o de dispositivos en red para su consumación. En tal sentido, los prenotados crímenes pueden involucrar acciones de variada índole, por ejemplo: Ataques directos a equipos de cómputo u otros dispositivos para desactivarlos, uso de computadoras para difundir códigos maliciosos, obtención de información ilegal por medio de acceso a redes, robo de datos personales con fines de fraude (Garriga, 2016).

Según el CBC (incluyendo sus protocolos adicionales), los tipos de ciberdelincuencia se agrupan en cinco grupos. El primero, incluye todos los delitos informáticos dirigidos contra datos y sistemas informáticos (por ejemplo, acceso ilegal, interferencia con datos o sistemas en general). El segundo, está formado por actos ilícitos relacionados con el uso de la tecnología (falsificación, extracción, bloqueo o modificación de datos, entre otros). Las infracciones del tercer grupo, están relacionadas con el contenido de los datos o información. De otro lado, la violación de los derechos de autor y derechos conexos, pertenecen al cuarto grupo; mientras que el ciberterrorismo y la utilización del espacio virtual para cometer actos de violencia, así como otros actos que atenten contra la seguridad pública, se incluyen en el quinto grupo de ciberdelitos.

Los tipos de ciberdelitos a su vez se encuentran asociados con los métodos más comunes que utilizan los delincuentes virtuales, esto es, (i) el uso de programas maliciosos que se basan en el mal uso de las computadoras y las redes; (ii) ataques digitales, con el fin de crear una gran cantidad de solicitudes a un servidor o servicio para deshabilitar el objetivo; (iii) combinación de ingeniería social y código malicioso, donde la víctima se ve obligada a realizar ciertas acciones (hacer *clic* en un enlace en un correo electrónico, visitar un sitio *web*, entre otros), lo que posteriormente conduce a la infección del sistema utilizando el primer método; y, (iv) actividades ilegales que son violentas o potencialmente violentas: Acoso, distribución de contenidos ilegales, grooming, entre otros.

También, en las conductas referidas, los atacantes o ciberdelincuentes ocultan sus huellas a través de perfiles anónimos, mensajes cifrados y otras tecnologías similares (Anguita, 2018).

Una persona es llamada un *hacker* ético, cuando no destruye la seguridad en los sistemas, tiene cuidado con la seguridad y salvaguarda el sistema, pero lo analiza desde el punto de vista de un posible atacante o *hacker*. "Evalúa la seguridad e identifica vulnerabilidades en sistemas, redes o infraestructura de sistemas, esto incluye encontrar y explotar algunas vulnerabilidades para determinar cuándo hay acceso sin autorización u otras actividades maliciosas" (Sánchez, 2019, p.1).

Se ha estimado que lo propuesto en el CBC sobre armonización de las leyes cibernéticas deviene en una criminalización excesiva que afecta a quienes desarrollan actividades en clave de *hacking* ético y similares, pese a la ausencia de un elemento volitivo delictual. Adicionalmente, al tratarse de un instrumento de derecho que es jurisdiccional en el mundo físico, pero abierto en el ciberespacio, genera serias críticas desde las lecturas de soberanía y autodeterminación de los Estados y gobiernos (Di Piero, 2013).

En cualquier caso, la promulgación del CBC, así como su suscripción por parte de países integrantes del CoE y aquellos otros externos a tal organización, ha puesto de presente, entre otras cuestiones, la relevancia de (i) la libertad de expresión, información, reunión y asociación en relación con *internet* como herramienta para promover los derechos humanos y la democracia en todo el mundo; (ii) la infracción de los derechos de propiedad intelectual en el campo de las tecnologías digitales y los usos justos en el marco de la cooperación internacional, incluso con el sector privado; (iii) la transferencia lícita de datos, su protección y privacidad en *internet*

como criterio esencial para la confianza de los usuarios; y, (iv) las actividades permitidas a los proveedores de servicios que almacenan y procesan los datos, así como la interferencia de los gobiernos y los entes reguladores.

De todas maneras, sigue siendo motivo de preocupación la posibilidad de que *internet* se utilice para fines incompatibles con el mantenimiento de los derechos y garantías en el orden democrático y la seguridad internacional. Los gobiernos, en colaboración con todas las demás partes interesadas, deben desarrollar códigos de conducta en el ciberespacio y enfoques comunes para su uso. Esto implica también apoyar el modelo de gobernanza de *internet* con la participación de una amplia gama de usuarios y bajo la idea de flexibilidad y apertura para adaptarse al vertiginoso desarrollo y expansión de las TIC (Fernández y Martínez, 2020). En torno a lo que ya se ha realizado al respecto, la siguiente sección presenta aspectos esenciales del desarrollo del CBC en Colombia por vía de las Leyes 1273 de 2009 y 1928 de 2018.

2.2. La protección de la información y de los datos como bien jurídico tutelado

Siguiendo a Agustina (2021), se encuentra, por una parte, que el espacio de comunicación moderno es un fenómeno complejo y multidimensional. Por otro lado, la información está sujeta no sólo a la lógica del desarrollo tecnológico, sino también a las leyes del progreso social. En sentido amplio sobre las TIC, tales cuestiones hacen parte de un sistema de ideas, objetivos, actitudes, métodos y medios, por los cuales el Estado y sus asociados regulan las relaciones entre sí, de modo que la gestión de los recursos de información es pasible de circulación legal, lo cual es de fundamental importancia para la economía moderna, el sistema constitucional y las instituciones democráticas, y teniendo en cuenta, además, el alza en los delitos informáticos, los efectos generados por la pandemia ocasionada por el Covid-19 y sus efectos en la economía (Hernández, 2022).

Considerando el soporte de la política estatal en el campo concerniente a la sociedad de la información (Polo, 2020), el enfoque previamente relatado no solo aspira a la mejora de la legislación y la aplicación de la ley en la esfera de la información, sino que también determina las medidas prioritarias de tal categoría, entendida esta como derecho, deber y bien jurídico tutelado que es objeto de un entendimiento legal especializado.

En este último aspecto, el Estado, al regular las relaciones de información, implementa una dirección en clave de seguridad de la información, la cual otorga una visión holística de los patrones de conductas en red y su relevancia en el campo de la realidad jurídica. *Grosso* modo, bajo esta concepción "la cual *mutatis mutandi* refleja los grupos uno y dos de los ciberdelitos agrupados en CBC" se consideró el régimen doméstico, las conductas que según la Ley 1273 de 2009, se constituyen como ciberdelitos, con especial atención al componente de los datos y sistema informáticos, así como se puede apreciar en el Cuadro 1.

Cuadro 1
Ciberdelitos contenidos en la Ley 1273 de 2009

Clasificación de la protección	Delitos	Composición del punible según verbo rector y modalidad
Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	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.
	Obstaculización ilegítima de sistema informático o red de telecomunicaciones.	El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.
	Interceptación de datos informáticos.	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.
	Daño informático	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
	Uso de *software* malicioso	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
	Violación de datos personales	El que, 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.
	Suplantación de sitios *web* para capturar datos personales	El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes / El que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
De los atentados informáticos y otras infracciones	Hurto por medios informáticos y semejantes	El que, superando medidas de seguridad informáticas, realice la conducta [hurto] 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 establecidos.
	Transferencia no consentida de activos	El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

Fuente: Elaboración propia, 2022, con base en la normatividad sobre delitos informáticos de la Policía Nacional de Colombia.

Tomando en consideración la caracterización general de los delitos que contiene la norma, Pons (2017) expone cuatro características específicas: Que se cometen fácilmente; no requieren muchos recursos versus su beneficio; se cometen sin presencialidad; y, se benefician de lagunas de punibilidad por las regulaciones.

De hecho, el interés nacional en la promulgación de la Ley 1273 de 2009 refleja un tanto más el desarrollo de la denominada sociedad de la información "en lo que atañe a tal concepto", junto con la seguridad en red y el cuidado de datos de carácter personal (Riascos, 2012; Rojas, 2014; Recio, 2016; Castro, 2017). No obstante, estas relaciones difieren de otras en su objeto específico: Solo se puede percibir la vulneración de los datos y la información como resultado de un procesamiento especial de la conducta, teniendo en cuenta un medio físico (dispositivo) que de un modo u otro utiliza redes informáticas (medio virtual).

En tal vía, la relación jurídica de información y de los datos concurren como un medio que intenta traducir las disposiciones generales de las normas jurídicas en derechos y obligaciones específicos (subjetivos) de los participantes, máxime en la esfera de protección penal, según las prescripciones relativas a una variedad de materias que se encuentran dentro del ámbito de la norma informativo-jurídica. La especificidad de estas relaciones jurídicas está determinada por tal tipo de actividad, teniendo en cuenta la recolección, búsqueda, acumulación, procesamiento, almacenamiento, provisión, distribución, y protección de los recursos TIC, así como las actuaciones de los particulares y el Estado, para satisfacer las necesidades de información en cumplimiento de la ley, e incluso los procesos pospenales y su proceso de resocialización (Vargas y García, 2021).

En este contexto, se incorporó en Colombia el CBC mediante la Ley 1928 de 2018, con el propósito de esclarecer armoniosamente los delitos cometidos en la red informática mundial y los mecanismos de investigación penal. Y por medio de la Sentencia C-224 de 2019, la Corte se refirió sobre la constitucionalidad de dicha norma supranacional. Además de establecer que el CBC se ajusta a los fines constitucionales en términos de política criminal y soberanía.

Sin embargo, valga mencionar que desde la perspectiva sobre la eficacia de la lucha contra la delincuencia en el ámbito de los delitos cibernéticos y de los datos personales, se encuentra que el derecho penal se muestra incapaz de combatir la nueva realidad fáctica que se disipa en el mundo digital. En este entorno se añade, además, que existe una gran cantidad de información errónea, no solo por el uso de las TIC, sino por las formas en las cuales las normas tipifican los comportamientos típicos, antijurídicos y culpables, como el caso presentado por Cabrera, Lara y Ruiz (2019), sobre el uso de la información y la libre expresión. En tal perspectiva, conviene echar mano al derecho comparado, el cual facilita la observación de las normas y su alcance respectivo.

2.3. Derecho comparado en torno al desarrollo legislativo del Convenio de Budapest

Es importante resaltar que uno de los problemas de los ciberdelitos proviene del bien jurídico al que el derecho penal pretende proteger, mucho más cuando se asume que son objetos de salvaguarda que no son convencionales, dado su carácter inusual con relación a otro tipo de infracciones ya codificadas. Tal cuestión es expresada por Martins (2022), que expone el impactado en como los ciberpunibles son entendidos en las legislaciones que se han apropiado para efecto del comparativo.

De otro lado, la respuesta ante los ciberdelitos va de la mano con el sistema procesal penal y sus detalles, esto a efectos de entender la persecución y enjuiciamiento de las formas en que se cometen las conductas, mucho más cuando se considera la investigación preliminar de cara a su prevención positiva: Una acción persuasiva que actuará incluso antes de la *notitia criminis* a partir de la creación de medios que puedan controlar el delito en *internet* (Pastorini, 2020).

En todo caso, aunque se permite la configuración de la norma sustantiva y adjetiva penal, la peculiaridad de los ciberdelitos va más allá de la previsibilidad de las leyes, y acaban impidiendo una persecución penal efectiva, así

como la aplicación de medidas irrazonables por la falta de medidas específicas. También, debe indicarse que aún no existe una preparación técnica de la policía judicial para enfrentar los delitos de la era virtual, aun cuando muchos de ellos son de bajo grado de complejidad.

Teniendo en cuenta lo descrito, se reflejan las siguientes conductas punibles por vía del comparativo con relación al CBC, comenzando para tal efecto entre las observaciones entre el régimen de Perú, Chile y Colombia (ver Cuadro 2), y una vez superado el análisis sudamericano se procede con el paragón de los países europeos elegidos, partiendo del entendimiento de que estos últimos son suscriptores directos del convenio por pertenecer al CoE.

Cuadro 2
Comparación entre el componente normativo entre Perú, Colombia y Chile

Ítem de comparación	Perú	Colombia	Chile
Adhesión al CBC	Aprobado mediante Resolución Legislativa No. 30913, del 12 de febrero de 2019; y ratificado a través del decreto Supremo No. 010-2019-RE, del 9 de marzo de 2019. Entra en vigor el 1 de diciembre de 2019.	Ley 1928 de 2018 Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", Convenio y ley aprobatoria declarados EXEQUIBLES por la Corte Constitucional mediante Sentencia C-224-19 de 22 de mayo de 2019. En vigor pleno desde junio de 2020	Decreto 83 de 2017: Promulga el Convenio sobre la Ciberdelincuencia.
Existencia de normas internas que regulan ciberdelitos	Si: 30096 de 2013 (modificada y complementada) la cual reúne ampliamente los ciberpunibles más allá de la consideración del bien jurídico sobre la información y los datos, de modo que logra vincular otros punibles en los cuales se emplean los dispositivos	Si: Ley 1273 de 2009 (sin modificación), norma que en esencia reúne la protección al bien jurídico tutelado de información y datos, sin que la misma vincule directamente otros punibles en los cuales se utilizan dispositivos (Posada, 2018)	Sí: Ley 21459, que establece normas sobre delitos informáticos, deroga la Ley 19913 y modifica otros cuerpos legales, con el objeto de adecuarlos a las exigencias del Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como "Convenio de Budapest", del cual Chile es parte.
Reconocimiento de los diversos tipos de ciberdelitos referidos o contenidos en el CBC	Sí: la Ley 30171 de 2014 incorpora ampliamente la definición y tipificación de delitos (Ordoñez, 2017). "En todos los casos en los que el Convenio de Budapest ha hecho propuestas de tipificación, se han creado o modificado normas en el país relacionadas con el mismo objetivo. En la mayoría de los casos, las normas peruanas tienen una redacción similar" (Guerrero, 2018, p.12)	No. Si bien la norma 1273 hace un importante avance en materia de protección de datos personales e información, aún no se codifica en debida manera las propuestas de tipificación del CBC. En contraste, Perú, incluso mucho antes de adherirse al convenio ya había trabajado un tanto más en la tipificación de los delitos, y en mecanismos de persecución procesal penal (Chaparro, 2014; Castro, 2017)	No. Similar al caso colombiano, la norma nacional chilena que regula los ciberdelitos se enfoca un tanto más en los preceptos que atañen a los datos, los sistemas y la información. Resta atención a los alcances de la legislación peruana sobre otras conductas.
Observaciones	El desarrollo legislativo que Perú le ha dado a los delitos informáticos se caracteriza por ser progresivo y coherente desde que fueron codificados en 1991 en el artículo 207 del Código Penal. Eventualmente, La promulgación de la ley 30096 y las modificaciones realizadas a esta por vía de la ley 30171, así como la suscripción del CBC, han permitido que dicho país cuente, por lo menos desde el orden normativo, con una legislación ordenada y codificada de los tipos de ciberpunibles considerados en el convenio de Budapest.	El desarrollo legislativo de los delitos informáticos en Colombia no ha sido progresivo y rápido como sí ha ocurrido en Perú. Las leyes 1273 y 1928 son apenas un avance en la materia, pero las mismas no aparejan el mismo alcance de la legislación peruana, la cual supera la codificación de punibles sobre la información y los datos. En tal sentido, el régimen colombiano bien puede tomar como ejemplo los avances peruanos en materia de persecución de delitos del espacio virtual que reflejan actos de violencia o de amenaza de violencia sobre las personas.	El desarrollo legislativo de los delitos informáticos en Chile representa un salto importante que reconfigura la vigencia y entendimiento del CBC. Empero, su codificación actual de los ciberdelitos es intermedia entre los avances de la legislación colombiana con la ley 1275 y el régimen peruano, de modo que crece de otros componentes ajenos a los datos, la información y los sistemas (Mayer y Vera, 2022).

Fuente: Elaboración propia, 2022.

Sin duda alguna, el régimen peruano instaurado para investigar, perseguir y sancionar los ciberdelitos es de notable composición. Como explica Guerrero (2018), el mencionado país adoptó desde finales del siglo XX, normas de carácter sancionador con el fin de combatir los ciberdelitos, sin que inicialmente se revistiera un análisis de fondo. Empero, como señala el autor referido, en el 2000, se aprobó la Ley No. 27309 con dos delitos al Código Penal: El intrusismo informático y el *cracking*. Entre 2004 y 2010, se aprobaron modificaciones sobre los delitos de explotación sexual, pornografía infantil y propiedad intelectual, relacionados al uso de la TIC. En el año 2013 se aprobó la Ley No. 30096 que introdujo modificaciones al Código Penal e incorporó un los delitos informáticos y medidas procesales. Finalmente, en 2014 se aprobó la Ley No. 30171 que modificó a esta última y es la ley vigente.

Se percibe entonces que el legislador peruano no solo tomó inspiración del CBC, sino que además innovó en lo que atañe a elementos subjetivos y objetivos que se adaptaran para efectos de la eficacia en términos sancionatorios, y consideró la inclusión de otros punibles que en la actualidad son materia de amplia preocupación, como el *grooming*. Pese a todo, "ninguna de estas modificaciones fue ajena a la controversia (…) en su momento organizaciones de la sociedad civil protestaron no solo por los textos propuestos sino por la poca transparencia en el debate para su aprobación" (Guerrero, 2018, p.6). Aun así, el Estado en mención ha volcado sus intereses a la creación de entes que apoyen al órgano acusador e investigador para efecto de combatir adecuadamente la cibercriminalidad.

Por el contrario, Colombia y Chile han centrado sus esfuerzos legislativos en clave de sancionar los delitos dirigidos contra datos y sistemas informáticos, así como los ilícitos relacionados con el uso de la tecnología e infracciones sobre el contenido de los datos o información. Si bien tal consideración permite a tales países tomar la senda del enjuiciamiento criminal de los ciberpunibles, queda restando la labor en torno a los delitos que son conexos o conculcan otros bienes jurídicamente protegidos por conductas lesivas que dependen del ciberespacio y los dispositivos con acceso a la red (Pavón et al., 2022).

Ahora bien, en lo que concierne al desarrollo de los delitos plurimencionados, los casos europeos que a ejemplo de comparación se han dispuesto para este artículo parten de una nota aclaratoria: El Reglamento de Ciberseguridad de la Unión Europea (UE), introduce un esquema de certificación en toda la UE, así como un mandato nuevo y reforzado para la Agencia Europea de Ciberseguridad. En diciembre de 2020, se propone una revisión de la directiva y en mayo de 2022, el Consejo del Parlamento Europeo establece un acuerdo interino que propone dos objetivos clave: (i) Asegurar una mejor gestión y cooperación en riesgos e incidentes digitales; y, (ii) ampliación del ámbito de aplicación de las normas. Partiendo de esta nota explicativa, se ilustra lo siguiente en el Cuadro 3.

Cuadro 3
Comparación entre el componente normativo entre Alemania y España

Ítem de comparación	Alemania	España
Reconocimiento de los diversos tipos de ciberdelitos referidos o contenidos en el CBC	Los delitos informáticos en sentido amplio incluyen punibles en los que se utiliza las TIC para la planificación, preparación o ejecución. De otro lado, se toma atención a las diferentes áreas de delincuencia en las que Internet se utiliza como medio delictivo. El CBC se presenta en un esquema de armonización y apoyo para la investigación y sanción del crimen transnacional.	El Código de Derecho de la Ciberseguridad (Instituto Nacional de Ciberseguridad y Boletín Oficial del Estado [INCIBE y BOE], 2022) reúne las normas que tienen relevancia sobre el ciberespacio, la interacción entre individuos e internet, y la manifestación de ciberdelitos. Sobre estos últimos, la ley refiere desde la afectación a los datos, los sistemas y la información, hasta conductas que dependen de las TIC para su materialización. El CBC de nuevo es instrumento de armonización.

Cont... Cuadro 3

Observaciones sobre los delitos tipificados	La normativa (Código Penal Alemán), en sentido estricto, estima otros fraudes informáticos (§ 263a Párr. 1 y 2 StGB, así como acciones preparatorias según § 263a párr. 3 StGB; López, 1999), a menos que estén incluidos en los siguientes tipos de fraude o uso indebido de los servicios de telecomunicaciones: Espiar e interceptar datos , incluidas las acciones preparatorias y la recepción de datos (§§ 202a, 202b, 202c, 202d StGB) incluye el robo y la recepción de identidades digitales, tarjetas de crédito, comercio electrónico o datos de cuentas (p. ej., *phishing*), falsificación de datos relevantes para pruebas o engaño en transacciones legales (§§ 269, 270 StGB), manipulación de datos / sabotaje informático, uso indebido de los servicios de telecomunicaciones (§ 263a StGB). Sin embargo, en la interpretación en sentido amplio se considera la relación usuario-TIC según las características de la planificación, preparación o ejecución de los delitos.	El desarrollo legislativo de los delitos informáticos reúne un amplio catálogo. Al respecto se encuentran: "Contacto a través de las TIC con un menor con fin de concertar un encuentro para cometer abuso sexual o la producción de pornografía". Art. 183 ter CP / Uso de menores o incapaces con especial protección para fines pornográficos. Art. 189 CP / Descubrimiento de secretos o vulneración de la intimidad por particular, acceso o facilitación a otro para acceder a un sistema de información sin estar debidamente autorizado; facilitar a terceros la comisión de delitos; delitos cometidos en el seno de una organización criminal; responsabilidad penal de las personas jurídicas en los delitos de descubrimiento de y revelación de secretos. arts. 197, 197 bis y ter CP. Además, revelación y divulgación de secretos ajenos; y descubrimiento, revelación o cesión de datos. Arts. 197 ter, quater, quinquies, 199 y 200 CP. /Calumnias e injurias cometidas a través de la tecnología. Arts. 211 CP / Estafas informáticas. Arts. 248 y 249 CP / Uso de cualquier equipo terminal de telecomunicación sin consentimiento de su titular. Art. 256 CP/ Daños informáticos o cracking. Arts. 264 y 264 bis CP. / Delitos informáticos contra la propiedad industrial. Arts. 273 y 274 CP. /Delitos informáticos contra la propiedad intelectual. Art. 270 CP. / Falsedades informáticas y espionaje empresarial. Arts. 278 y 279 CP. / Falsedades documentales informáticas. Arts. 390.1, 2 y 3; 392; 395 y 400 CP / Delitos de ciberterrorismo. Arts. 573.2; 197 bis y ter y del 264 al 264 quater CP / Otros delitos cometidos a través de los sistemas informáticos cuando su utilización fuera determinante».

Fuente: Elaboración propia, 2022.

En el caso de Alemania, país integrante del CoE, y por tanto suscriptor original del CBC y de los eventuales protocolos adicionales de tal instrumento, se consideran los ciberdelitos en sentido estricto y en sentido intermedio (Aboso et al., 2022). En aquella consideración se entiende, por ejemplo, que el fraude informático (en los términos del artículo 263a del Código Penal alemán, abreviado como StGB) puede desglosarse en (i) adquisición fraudulenta de vehículos de motor; (ii) otros tipos de fraude crediticio; (iii) fraude utilizando datos obtenidos ilegalmente de tarjetas de pago; y, (iv) fraude utilizando otros medios de pago distintos del efectivo obtenidos ilegalmente.

De otra parte, en Alemania, los delitos informáticos en sentido amplio, incluyen todos los delitos en los que se utiliza las TIC para la planificación, preparación o ejecución. Mientras tanto, éstos se extienden a casi todas las áreas de delincuencia en las que *internet* se utiliza como medio delictivo. Por ejemplo: Formas de chantaje digital, infracción de derechos de autor y marcas registradas, organización no autorizada de un juego de azar, la distribución de sustancias prohibidas, el intercambio de pornografía infantil o propaganda que glorifica la violencia; o la violación de la esfera más personal de la vida (intimidad y buen nombre), y el *grooming*, entre otros.

Tal y como se observa, la legislación alemana bien se acerca a los delitos informáticos del CBC tanto por vía de la protección de datos, información y sistemas, como por sentido de los punibles donde la tecnología de la información y la comunicación se utiliza para planificar, preparar y ejecutar conductas punibles previamente codificadas, como el fraude, la pornografía infantil y el ciberacoso (Mayer y Vera 2022). En todo caso, los actos de ciberdelincuencia en Alemania extienden la responsabilidad penal en algunos casos a los actos preparatorios, como la producción o adquisición de programas de ordenador, cuyo

objeto es cometer fraude informático.

En lo que atañe a España, es necesario en primer lugar remitirse al Código de Derecho de la Ciberseguridad, marco que compila toda una serie de normas que tienen relevancia sobre el ciberespacio, la interacción entre individuos e *internet*, y la manifestación de ciberdelitos. En tal compendio se resumen las disposiciones que sobre los mentados punibles existe en tal legislación. De acuerdo con Fernández y Martínez (2020), los crímenes de tal naturaleza se encuentran dispuestos en varios apartes de Código Penal, y con la reforma vigente a tal estatuto, según las recomendaciones de la comunidad europea, se consideran diversos delitos que van desde la afectación a los datos, los sistemas y la información, hasta conductas que dependen de las TIC para su materialización, tal y como se observa en la tabla dispuesta.

Para efectos del propósito, Gamba (2019) ilustra que en la doctrina española los delitos informáticos se clasifican en dos grupos: El primero, que atenta contra la intimidad de las personas; y el segundo, que se compone de aquellos que atentan contra el patrimonio económico. Analizada la legislación de España en torno al ciberdelito y su comparación con el caso colombiano, hay similitudes frente al derecho penal y su aplicación punitiva en cuanto al delito informático, especialmente en consideración a la transferencia no consentida de activos, contemplado en la Ley 599 de 2000.

Así las cosas, se encuentra que las legislaciones de los países europeos descritos cuentan con una amplia cobertura en torno a las consideraciones sobre los ciberdelitos, tanto por las recomendaciones originadas en los órganos de gobierno europeo, cuyo objeto se enfoca en desarrollar los fines del CBC y sus disposiciones complementarias, como por la normativa interna que cada uno de los gobiernos comentados ha instituido en su régimen sancionatorio. No obstante, se destaca que la codificación de los ciberdelitos se encuentra diseminada en diferentes apartados de la ley penal, tal y como se considera para el momento en el caso colombiano.

Conclusiones

En la actualidad son múltiples las actividades que las personas naturales y/o jurídicas realizan con amplia dependencia de las redes de *internet* y los servicios que proporciona. Esto hace que los ciberdelitos cobren mayor relevancia social, institucional y patrimonial. Y, a diferencia de otros tipos de actividades ilegales, el delito cibernético no se limita al espacio físico, y mucho menos a jurisdicción específica.

Ahora bien, de la comparación tendida se derivan las siguientes cuestiones: La normativa vigente en el contexto colombiano considera unas conductas que, según la Ley 1273 de 2009, se constituyen como ciberdelitos, los cuales, tal y como se describió en el Cuadro 1, tienen especial enfoque al bien protegido de la información y de los datos, así como las infracciones a los sistemas informáticos. Este criterio es primigenio para entender el contraste con los demás regímenes elegidos por cuanto determina la balanza de expectativas, recomendaciones y observaciones.

Al comparar entonces la protección que ofrece el sistema sancionatorio colombiano con lo dispuesto en los casos de Perú y Chile surgen diferencias, tanto de orden histórico, como de carácter legal en torno a la tipificación del ciberdelito. En efecto, la legislación peruana se destaca por su anticipación al CBC, y por la manera en cómo aborda en un primer momento las conductas que se consideraban lesivas en el contexto pluriofensivo que se deriva del uso de las TIC. Y, desde su adhesión al instrumento de derecho, su normatividad ha avanzado con miras a fortalecer las cuestiones sustantivas y adjetivas de la persecución y sanción de los ciberdelitos.

Por otra parte, Chile se presenta en un estado intermedio entre Colombia y Perú. Sus avances en la materia se han derivado a partir de la protección de datos y sistemas informáticos, y se encuentra por el momento en la articulación de ciberdelitos que superan tal bien jurídico, toda vez de la existencia de crímenes que lesionan otros intereses cuya

realización o planeación dependen en buena medida de las TIC.

En tales apreciaciones entonces se percibe que la normativa colombiana aún tiene un camino abierto y que debe reconocer las falencias para realmente instituir los ciberdelitos según sus modalidades pluriofensivas y sus manifestaciones de orden particular. No basta con tener una adhesión al CBC para efecto de lucha transnacional contra el cibercrimen, antes bien, deben proveerse los mecanismos y herramientas legales para que la persecución de los precitados punibles tenga el sentido que aquel instrumento busca. Y como ejemplo para ello, bien puede tomarse el trasegar jurídico de Perú.

En cuanto a las legislaciones española y alemana, se encuentra que estas también han superado la lectura del bien jurídico sobre la información y los datos, así como la protección de sistemas informáticos. Aquella ha implementado una serie de disposiciones legales en variados cuerpos normativos unificados bajo un código que orienta las perspectivas entre la relación hombre-TIC, y la última ha enfocado su labor punitiva a tener en cuenta ciberdelitos tanto en su formas restrictivas y amplias según los parámetros de interpretación y los bienes jurídicos que se protegen según la forma en cómo se cometen los crímenes. A su vez, los regímenes europeos en comento van de la mano con las recomendaciones que en su comunidad supranacional se expiden para orientar una mejor prevención, sanción y enjuiciamiento de los ciberdelitos.

Visto lo anterior, se indica que es necesario armonizar las normas jurídicas internacionales y unificar las legislaciones nacionales de los Estados que determinan la composición de los delitos en el ámbito de *internet*, desarrollar un enfoque unificado para establecer la jurisdicción y desarrollar las disposiciones pertinentes del Convenio de Budapest. También resolver el problema de facultar a los organismos encargados de hacer cumplir la ley.

Referencias bibliográficas

Aboso, G. E., Agüero, J. L., Álvarez, J. T., Arocena, G. A., Buompadre, J. E., Figari, R. E., Gonella, C., Linares, M. B., Portillo, V. H., Riquert, M. A., Salt, M., y Sueiro, C. C. (2022). *Ciberdelitos: Análisis doctrinario y jurisprudencial*. ElDialLibro.

Aguilar, M. M. (2015). Cibercrimen y cibervictimización en Europa: Instituciones involucradas en la prevención del ciberdelito en el Reino Unido. *Revista Criminalidad, 57*(1), 121-135.

Agustina, J. R. (2021). Nuevos retos dogmáticos ante la cibercriminalidad: ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma? *Estudios Penales y Criminológicos*, *41*, 705-777. https://doi.org/10.15304/epc.41.7433

Anguita, J. E. (2018). Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea. *RESI: Revista de Estudios en Seguridad Internacional*, *4*(1), 107-126. http://dx.doi.org/10.18847/1.7.7

Benítez, I. F. (2021). Ciberdelitos: La implementación en el ordenamiento interno de los acuerdos internacionales en materia de ciberdelincuencia. En M. J. Cruz e I. Lledó (Coords.), *La Robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0: Los desafíos jurídicos, éticos y tecnológicos de los robots inteligentes* (pp. 79-128). Dykinson.

Cabrera, J. P., Lara, A., y Ruiz, K. M. (2019). Vulneración a la libertad de expresión: Caso los jinetes del apocalipsis. *Revista de Ciencias Sociales (Ve), XXV*(1), 102-110.

Castro, G. (2017). Contexto y certeza de los límites aplicativos de la vigilancia estatal y del habeas data en el derecho colombiano. En C. N. Güechá-Medina, M. Torres-Guarnizo y M. Ibler (Eds.), Tensiones entre libertad y seguridad (pp. 175-190). Grupo Editorial Ibáñez.

Centeno, E., Mondragón, S. L., Ospina, E. F., y Franco, L. M. (2022). Resocialización de la pena: Retos desde las nuevas tecnologías de la información y la comunicación. *Revista de Ciencias Sociales (Ve), XXVIII*(4), 303-314. https://doi.org/10.31876/rcs.v28i4.39132

Chaparro, M. F. (2014). Legislación informática y protección de datos en Colombia, comparada con otros países. *INVENTUM*, *9*(17), 32-37. https://doi.org/10.26620/uniminuto.inventum.9.17.2014.32-37

Coloma, R. (2016). Las disciplinas jurídicas y su reinvención. *Ius et Praxis*, *22*(2), 253-298. https://dx.doi.org/10.4067/S0718-00122016000200009

Corte Constitucional de la República de Colombia. Sentencia C-224 de 2019. M.P. Cristina Pardo Schlesinger. 22 de mayo de 2019.

D'Avila, F. R., y Dos Santos, D. L. (2016). Derecho Penal y ciberdelitos. Breves aproximaciones dogmáticas. *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/doctrina/44615-derecho-penal-y-ciberdelitos-breves-aproximaciones-dogmaticas

Decreto 83 de 2017. Promulga el Convenio sobre la Ciberdelincuencia. 28 de agosto de 2017.

Decreto Supremo No. 010 de 2019-RE. Ratifica el "Convenio sobre la Ciberdelinciuencia". 9 de marzo de 2019.

Derechos Digitales (16 de mayo de 2022). Convenio de Budapest sobre la Ciberdelincuencia en América Latina. *Derechos Digitales*. https://www.derechosdigitales.org/18451/convenio-de-budapest-sobre-la-ciberdelincuencia-en-america-latina/

Di Piero, C. (2013). Recensión a Miró Llinares, F. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. *InDret Revista para el Análisis del Derecho*. https://indret.com/wp-content/themes/indret/pdf/984.pdf

Fernández, D., y Martínez, G. (2020). *Ciberdelitos*. Ediciones Experiencia.

Fontestad, L., y Jiménez, M. D. L. N. (2021). *La transformación digital de la cooperación jurídica penal internacional*. Editorial Aranzadi.

Gamba, J. A. (2019). *El delito informático en el marco jurídico colombiano y el derecho comparado: Caso de la transferencia no consentida de activos* [Tesis de maestría, Universidad Externado de Colombia]. https://bdigital.uexternado.edu.co/entities/publication/42898030-1af8-4c38-a535-ed61412a6e62

Garriga, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Dykinson.

Gascón, A. (2014). La gobernanza de Internet y el Consejo de Europa. En A. J. Rover, F. Galindo y O. Mezzaroba (Coords.), *Direito, Governança e tecnologia: princípios, políticas e normas do Brasil e da Espanha* (pp. 115-131). Conceito Editorial.

González, M. L. (2017). La cibercriminalidad como instrumento para la expansión y empoderamiento del crimen organizado. *GESI:*

Grupo de Estudios en Seguridad Internacional, (46), 13-45. https://www.seguridadinternacional.es/?q=es/content/la-cibercriminalidad-como-instrumento-para-la-expansi%C3%B3n-y-empoderamiento-del-crimen

Grajales, J. F., y Osorno, Y. M. (2019). La globalización y la importancia de las TIC en el desarrollo social. *Reflexiones y Saberes*, (11), 2-9. http://34.231.144.216/index.php/RevistaRyS/article/view/1133

Guerrero, C. (2018). *De Budapest al Perú: Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia. Impacto en el corto, mediano y largo plazo.* Derechos Digitales América Latina. https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf

Hernández, D. (2022). COVID-19 in Colombia: Repercussions on the economy. *SUMMA. Revista Disciplinaria en Ciencias Económicas y Sociales*, *4*(1), 1-9. https://doi.org/10.47666/summa.4.1.04

Hernández, J. C. (2012). La protección de datos personales en internet y el hábeas data. *Revista Derecho y Tecnología*, (13), 61-85.

Herrera, K. V. (2018). Ecuador: La iniciativa popular normativa en el gobierno de la revolución ciudadana. *Revista de Ciencias Sociales (Ve), XXIV*(2), 68-82.

Instituto Nacional de Ciberseguridad y Boletín Oficial del Estado – INCIBE y BOE (2022). *Código de Derecho de la Ciberseguridad*. INCIBE/ BOE.

Ley 599 de 2000. *Por la cual se expide el Código Penal. 24 de julio de 2000.*

Ley 27309 de 2000. Incorpora los delitos informáticos al Código Penal. 26 de junio de 2000.

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.

Ley 30096 de 2013. Ley de Delitos Informáticos. 21 de octubre de 2013.

Ley 30171 de 2014. Ley que modifica la Ley 30096, Ley de Delitos Informáticos. 10 de marzo de 2014.

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. 50.664.

Ley 21459 de 2022. Establece normas sobre delitos informáticos, deroga la Ley 19913 y modifica otros cuerpos legales, con el objeto de adecuarlos al Convenio de Budapest. 20 de junio de 2022.

López, C. (1999). *Código Penal Alemán*. Universidad Externado de Colombia.

Martins, B. (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México*. Derechos Digitales América Latina. https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

Mayer, L., y Vera, J. (2022). La falsificación informática: ¿Un delito necesario? *Revista Chilena de Derecho y Tecnología*, *11*(1), 261-286. https://dx.doi.org/10.5354/0719-

2584.2022.65299

Mondragón, S., Caballero, S., Díaz, L., y Herrera, J. (2022). Protección jurídica de los derechos de autor en Colombia. *SUMMA. Revista Disciplinaria en Ciencias Económicas y Sociales*, *4*(1), 1-10. https://doi.org/10.47666/summa.4.1.09

Ordoñez, L. (2017). La protección de datos personales en los estados que conforman la Comunidad Andina: Estudio comparado y precisiones para un modelo interamericano de integración. *Foro: Revista de Derecho*, *1*(27), 83-114. https://revistas.uasb.edu.ec/index.php/foro/article/view/502

Pastorini, J. (2020). Prevención y persecución de ciberdelitos: ¿un nuevo terreno para la inteligencia artificial? *RIDP Libri*, (4), 92-99. http://www.maklu-online.eu/nl/tijdschrift/ridp-libri/ridp-libri/alternativas-al-sistema-de-justicia-criminal-latin/prevencion-y-persecucion-de-ciberdelitos-un-nuevo-/

Pavón, E., Guaytarilla, L. F., Cueva, C., y Durango, K. (2022). Perspectives on cybersecurity and cyberdefense in Latin America. *Athenea Revista en Ciencias de la Ingeniería*, *3*(9), 26-37. https://doi.org/10.47460/athenea.v3i9.43

Polo, A. (2020). Sociedad de la Información, Sociedad Digital, Sociedad de Control. *Inguruak. Revista Vasca de Sociología y Ciencia Política,* (68), 50-77. http://dx.doi.org/10.18543/inguruak-68-2020-art05

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Posada, R. (2018). *Los cibercrímenes: Un nuevo paradigma de criminalidad: Un estudio del título VII bis del Código Penal colombiano*. Universidad de los Andes.

Punín, P. D. (2022). Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica. *Revista Ruptura, 3*(3), 191-230. https://doi.org/10.26807/rr.v3i03.85

Rayón, M. C., y Gómez, J. A. (2014). Cibercrimen: Particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico escurialense*, (47), 209-234.

Recio, M. (2016). *Protección de datos personales e innovación: ¿(In) compatibles?* Editorial Reus.

Riascos, L. O. (2012). Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. *Derecho y Realidad*, *10*(20), 335-429. https://revistas.uptc.edu.co/index.php/derecho_realidad/article/view/4868

Rodríguez, M. (2015). Internet: ¿Hacia un nuevo concepto de lo público? *Revista Persona y Derecho*, (72), 133-148. https://doi.org/10.15581/011.72.133-148

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus*, *8*(1), 107-139. https://doi.org/10.14718/NovumJus.2014.8.1.6

Sánchez, M. A. (2019). *Hacking ético: Impacto en la sociedad* [Tesis de especialización, Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/4919

TyN Magazine (26 de abril de 2022). Cinco mil millones de personas utilizan internet en todo el mundo. *TyN Magazine*. https://tynmagazine.com/

cinco-mil-millones-de-personas-utilizan-internet-en-todo-el-mundo/

Vargas, W. C., y García, M. (2021). Resiliencia, comprensión psicosocial para los pospenados del Instituto Nacional Penitenciario y Carcelario en Colombia. *Revista de Ciencias Sociales (Ve), XXVII*(E-3), 151-167. https://doi.org/10.31876/rcs.v27i.36499