El Ciberterrorismo en la Legislación Colombiana: Un Análisis Desde la Criminologia†

Cyberterrorism in Colombian Legislation: An Analysis from Criminology

Submitted: 24 March 2023
Reviewed: 23 June 2023
Revised: 30 June 2023
Accepted: 3 July 2023

Article submitted to peer blind review

Hans Nicolaysen Sanchez*
https://orcid.org/0000-0001-5475-1668
María Paula Castellanos Peña**
https://orcid.org/0000-0002-5835-5133
Paola Alexandra Sierra-Zamora***
https://orcid.org/0000-0002-3146-7418
Manuel Bermúdez-Tapia****
https://orcid.org/0000-0003-1576-9464

DOI: https://doi.org/10.26512/lstr.v16i1.47743

† Artículo resultado del proyecto de investigación: "Macroproyecto en DD.HH., DIH y Justicia" del grupo de investigación "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA y Justicia", categorizado en A por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias) y registrado con el código COL0141423. Los puntos de vista y los resultados de este artículo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.
*Estudiante de la Facultad de Derecho de la Universidad Católica de Colombia y auxiliar de investigación del semillero de investigación "Derechos Humanos y Derecho Internacional", vinculado al Grupo de Investigación Persona, Instituciones y Exigencias de Justicia, de la Universidad Católica de Colombia. Contacto: hnicolaysen26@ucatolica.edu.co.
**Estudiante de la Facultad de Derecho de la Universidad Católica de Colombia y miembro del semillero de investigación "Derechos Humanos y Derecho Internacional", vinculado al Grupo de Investigación Persona, Instituciones y Exigencias de Justicia, de la Universidad Católica de Colombia. Contacto: mpcastellanos21@ucatolica.edu.co.
***Postdoctora internacional en nuevas tecnologías y derecho por la Mediterránea International Centre for Human Rights Research -MICHR-. PhD Internacional (cum laude) y Magister en Derechos Humanos, Democracia y Justicia Internacional, Universitat de Valéncia, España. Abogada, Universidad Católica de Colombia. Docente Ocasional del Doctorado en Estudios Estratégicos, Seguridad y Defensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Líder del Grupo de Investigación "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA y Justicia" de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Contacto: paola.sierraz@esdeg.edu.co.
****Abogado graduado con la mención de Summa Cumme Laude por la Pontificia Universidad Católica del Perú. Profesor ordinario de la Facultad de Derecho y Unidad de Postgrado de la Universidad Nacional Mayor de San Marcos. Profesor Investigador de la Universidad Privada San Juan Bautista. Master en Derechos Fundamentales por la Universidad Carlos III de España. Estudios de especialización en la Universidad de Valencia, en la Universidad de Salamanca y en Castilla La Mancha (España), Universidad de Bolonia y Pisa (Italia). Registrado en RENACYT PO140233 y en Min Ciencias en Colombia. Scopus ID 57278125300. Contacto: manuel.bermudez@upsjb.edu.pe.

Abstract

[Purpose] *The globalization of post-industrial society has generated new figures that govern traditional human relations such as social, political, economic and financial customs in the last thirty years. The development of new challenges is evaluated in the economic, political, social and legal field, in particular because the concepts and normative field are surpassed by the extraterritoriality of the phenomena that take place in the field of transnational crime. This new modality of execution of crimes represents a severe problem for national jurisdictions and sovereignties because it subjugates criminal phenomenology and affects criminal law, limiting it not only in a normative sphere but also in a theoretical and procedural perspective because its evaluation and subsequent judgment implies a series of limiting conditions for States and especially governments that may be affected by a cyberattack caused by governments or criminal groups that may cause effects that affect the administrative structure of a country or may cause an economic effect that may generate a severe weakening of Defense and National Security.*

[Methodology/Approach/Design] *For this reason, this work emphasizes the legal and dogmatic analysis of cyberterrorism in order to detail its characteristics and develop the analysis of its regulation in the Colombian legislative framework through the hypothesis: The development of technology in today's society allows the amplification of the use of new communication systems and access to information within cyberspace where various actions can be generated that can constitute serious damage to the development of the ordinary activities of a country, of a community, of a company or network of companies that negatively affects the social, democratic and governance spheres of a country, causing uncertainty in the population, exceeding the regulatory framework of national legislation.*

[Findings] *In short, it was possible to determine that within the Colombian legal regulation, specifically in its penal code, the crime of cyberterrorism is not tacitly typified. Owing to this fact, the findings achieved from this document led to a careful reflection about the impact of cyberterrorism on personal and national security, so it encourages the Colombian legislation interest to regulate and punish those criminal behaviors in cyberspace and, consequently, to provide guarantees under the constitutional principles of law for cyber victims and cyber criminals.*

Keywords*: Cyberterrorism. Globalization. Cyberspace. Criminology. Transnational Crime.*

Resumen

[Propósito] La globalización de la sociedad post-industrial ha generado en los últimos treinta años nuevas figuras que rigen las relaciones humanas tradicionales como las costumbres sociales, políticas, económicas y financieras. Se evalúa el desarrollo de nuevos desafíos en el campo económico, político, social y jurídico, en particular porque los conceptos junto con el campo normativo son superados por la extraterritorialidad de los fenómenos de los crimenes transnacionales. Esta nueva modalidad de ejecución de delitos representa un grave problema para las jurisdicciones y soberanías nacionales porque subyuga la fenomenología penal y afecta el derecho penal, limitándolo no sólo en el ámbito normativo sino también en el teórico y procesal, porque su evaluación y posterior juzgamiento implica una serie de condiciones limitantes para los Estados y, especialmente, para los gobiernos que pueden verse afectado por un ciberataque provocado por otros de su misma índole o grupos criminales idóneos para la producción de afectaciones en la estructura administrativa de un país o pueda, igualmente,

causar un efecto económico capaz de generar un severo debilitamiento de la Defensa y la Seguridad Nacional.
[Metodología/Enfoque/Diseño] El método de investigación utilizado fue cualitativo mediante la técnica que se basa en el análisis jurídico y doctrinal de carácter expositivo. De esta manera, es posible comparar mediante el exhaustivo estudio de la teoría que recubre el escenario internacional con respecto de la estructura de la misma dentro del ordenamiento jurídico colombiano. Por tal motivo, este trabajo enfatiza en el análisis jurídico y dogmático del ciberterrorismo con el fin de detallar sus características y desarrollar el análisis de su regulación en el marco legislativo colombiano a través de la hipótesis: El desarrollo de la tecnología en la sociedad actual permite la amplificación del uso de nuevos sistemas de comunicación y acceso a la información dentro del ciberespacio donde se pueden generar diversas acciones que pueden constituir, a su vez, un grave daño al desarrollo de las actividades ordinarias de un país, de una comunidad, de una empresa o red de empresas que afecte negativamente el sistema social, democrático y esferas de gobernanza de un país, provocando incertidumbre en la población, superando el marco regulatorio de la legislación nacional.
[Hallazgos] Las implicaciones para la práctica sugieren romper los paradigmas y transitar un terreno desconocido en materia de legislación cibernética, específicamente sobre el tipo penal de ciberterrorismo. Por ello, su aplicabilidad puede incurrir incluso en un plano virtual que trasciende al físico, el cual debe ser regulado por las leyes y el derecho para garantizar el orden, la seguridad nacional y los derechos humanos de los individuos. La presente investigación contribuye significativamente al discurso del ciberterrorismo dentro del contexto del marco legislativo colombiano, mediante un argumento de fácil de comprensión por cualquier lector que tenga conocimiento o no del ámbito jurídico.

Palabras Clave: Ciberterrorismo. Globalización. Ciberespacio. Criminología.

INTRODUCCIÓN

La globalización ha impactado de manera severa la manera en la que las sociedades se comunican y se interrelacionan en lo económico y comercial, en lo cultural, en lo político y en el ámbito demográfico provocando nuevas modalidades de migración debido a la mayor provisión de medios de comunicación y de acceso a medios de información (Clapham, 2002).

Como todo proceso humano, el impacto de la globalización ha provocado nuevas problemáticas sociales que deben ser abordadas desde una visión diferente al método tradicional especialmente debido al impacto que ha provocado, generándose modos de evaluación interdisciplinarios y sobre todo dinámicos porque las condiciones de análisis pueden diferir en función a la realidad evaluada, porque el mismo fenómeno puede provocar resultados diferenciados en función a las variables de estudio que pueden ser el tipo de país, las condiciones económicas y comerciales de una sociedad, el modo de evaluación de una población a nuevos retos, etc.

En estas circunstancias, se presentan nuevos paradigmas que influyen en la legislación nacional que debe adecuarse ante los requerimientos que plantean los gobiernos nacionales, cuando afectan la propia naturaleza de sus actos que inciden en situaciones de corrupción masiva (Bermúdez-Tapia, 2019, p. 277) y sobre todo las sociedades porque el riesgo a una condición negativa puede resultar incisiva en la gobernabilidad y sistema democrático en el país, sobre todo cuando se ejecutan situaciones que no han sido previstas en la legislación nacional, tal como sucede en la evaluación de los delitos transnacionales Llinares, 2012. p.57) y delitos cibernéticos.

El estudio de los ciberdelitos es fundamental para todos aquellos que se quieren especializar en la ciencia del derecho hoy en día, debido a que tendrán que enfrentarse a los cambios del nuevo mundo que se desarrolla a partir de la cuarta revolución industrial. El entender la tipificación de los ciberdelitos y el proceso penal para los ciberdelincuentes permitirá ahorrar una interesante parte del desgaste del aparato jurisdiccional. Con ello, el estudio y análisis de los ciberdelitos que aquejan a la sociedad a día de hoy podrá permitir a las naciones estar más preparadas para aquellos retos que se presenten en el futuro del derecho penal. Por tanto, partiendo del estudio del ciberterrorismo será posible comprender con una mejor perspectiva el actuar y el modus operandi de los ciberdelincuentes. Este trabajo pretende hacer una investigación socio-jurídica de cara a la criminología del ciberespacio mediante el estudio dogmático del ciberterrorismo.

La naturaleza de estos hechos implica un cambio en la perspectiva regulatoria normativa por cuanto los conceptos tradicionales de "sujetos activos del delito", "territorialidad" y "modalidad de ejecución del injusto penal" difieren de la clásica perspectiva del delito provocando la adaptación de nuevos elementos teóricos criminológicos para así poder adaptar al derecho penal a nuevas exigencias, sobre todo cuando la interacción entre gobiernos nacionales, el comercio mundial y la geopolítica inciden en la generación de nuevos escenarios (Richardson, 2011, p. 21).

En estos casos, un delito puede ser ejecutado en un país "x" y los efectos de las acciones en el ámbito cibernético o comercial o económico en otro país pueden resultar devastadores, especialmente cuando provoca una condición de inseguridad, tanto en una perspectiva local como también nacional, tal como sucedió en Irán cuando se logró determinar que el virus "Stuxnet" había provocado un error en la infraestructura digital y de producción nuclear en la planta nuclear de Natanz (Weinberger, 2011, p. 144).

Una condición que supera el tratamiento y evaluación de los fenómenos criminológicos porque estos se centran en la interacción de personas y grupos humanos, en función a la naturaleza de las causas que inciden en las conductas antisociales para proyectar un adecuado sistema de represión por parte del Estado a través de una legislación apropiada. De este modo el análisis de los comportamientos

negativos o antisociales permiten evaluar las causas que inciden en las conductas que serán reprimidas por los Estados porque de atenderse de forma eficaz los elementos que provocan estos comportamientos, la sociedad podría mejorar sus niveles de sociabilidad reduciendo significativamente toda situación que sea contraria al desarrollo de las personas y de la comunidad (Salinero, 2015, p. 27).

Sin embargo, esta perspectiva tradicional queda superada por el impacto de la globalización en el uso de la tecnología que permite una mayor interacción de las personas y gobiernos nacionales en el ciberespacio, en la mayoría de situaciones con situaciones ventajosas pero que no limitan las inseguridades y riesgos que deben ser manejados de forma maliciosa o temeraria por personas, grupos criminales o gobiernos nacionales con el fin de provocar un severo impacto en una realidad nacional determinada, provocando el cuestionamiento de los presupuestos normativos internacionales y nacionales frente a los DDHH (Gamón, 2017).

Consecuentemente, los nuevos desafíos sobre todo a la Defensa y Seguridad Nacional en el ámbito de la tecnología permiten detallar que el derecho penal debe incluir el análisis y tratamiento normativo de conductas punibles cometidas en el ciberespacio (López, 2020, p. 204), viéndose entonces desde la materialización de la virtualidad en el mundo físico que perjudica y ataca bienes jurídicamente protegidos en un ámbito multimodal, porque puede verse afectada la Defensa y Seguridad Nacional de un país, como también puede verse afectada la seguridad, el tráfico comercial y económico, y en el ámbito personal, derechos de orden económico, laboral, político al afectarse la intimidad y la dignidad (Barrio, 2015).

Delimitado el eje temático del presente trabajo, se planteó la cuestión: ¿Por qué la no existencia de una legislación que determine y sancione el ciberterrorismo de manera formal dentro del Código Penal atenta contra la seguridad y los derechos fundamentales de la población en Colombia? Por consiguiente, este trabajo pretende exponer la funcionalidad de los ciberdelitos enfocados específicamente al ciberterrorismo y cómo este se regula en el marco jurídico colombiano, para ello se realizará una contextualización sobre el origen del ciberterrorismo, continuando con un análisis sobre la regulación internacional y nacional que hay referente a este delito, después se darán unas breves conclusiones.

EL CIBERTERRORISMO

El ciberterrorismo implica la migración al ciberespacio de las modalidades y tipos de acciones habituales del terrorismo generándose una obligación en los países para establecer un control y punición de estos delitos (Girao et al, 2020, p. 4).

Desde una perspectiva doctrinaria, es posible detallar los siguientes elementos teóricos (Sánchez, 2015, p. 100), a efectos de detallar su contenido y condiciones:

- Ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos (Fernández, 2018).
- Ciberterrorismo es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas (CONPES 3858, 2016. p.88).
- Ciberterrorismo es la convergencia del ciberespacio y el terrorismo (Orta Martínez, 2005).
- Ciberterrorismo, es un acto criminal perpetrado a través de computadores que provoca situaciones de violencia, muerte y/o destrucción y crea terror en una comunidad o en un territorio con el propósito de coaccionar a un gobierno a cambiar sus políticas respecto de las pretensiones del grupo que los amenaza (Gonzáles Amado, 2007, p. 30).
- Ciberterrorismo, es la ejecución de un ataque sorpresa por parte de un grupo terrorista extranjero subnacional que tiene emplea la tecnología con fines políticos para incidir en la provisión de servicios básicos en una determinada localidad, sobre todo cuando se trata de energía nuclear, energía eléctrica, comunicaciones, sistemas financieros y bancarios o el comercio (Verton, 2004, p. 32).

Estas definiciones permiten diferenciar las consecuencias y naturaleza del ciberdelito respecto del ciberterrorismo (Pons, 2017, p. 81), pero permite detallar una correlación en función a género y especie porque ambas emplean el "ciberespacio".

Como la propia acción final puede ser evaluada sin que se identifique en forma automática al "autor", estas modalidades fueron extendiéndose en el ámbito de lo cotidiano y sus efectos no siempre son evaluados por la población por cuanto sus efectos no son inmediatos a lo cotidiano pero en la medida en la que se analiza su impacto puede provocar una condición que afecta a la propia gobernabilidad en dicho territorio porque los que han provocado esta situación son agentes vinculados al crimen organizado o agrupaciones terroristas que tienen por especial objetivo el provocar una condición de alto impacto en un país o una empresa o una actividad en especial.

Una condición que ha provocado que los países definan estos actos como parte de la doctrina del *ius ad bellum* que redefine la perspectiva del derecho penal en un país, por cuanto se generan estas condiciones:

- Respecto de la identificación de los "agentes del delito", su identificación puede no ser accesible sino hasta que el provocador anuncia sus pretensiones, porque generalmente son organizaciones que realizan sus actos bajo el anonimato.
- Una referencia que admite la posibilidad de que los gobiernos ejecuten estas acciones, sobre todo cuando procuran limitar o condiciones las acciones que puedan desarrollar otras naciones en el diseño de tecnología, el manejo del comercio y economía (Nava, 2016, p. 158) o inclusive el modo en el cual se accede a información de naturaleza política con el ánimo de afectar un proceso electoral (Sánchez et al, 2022, p. 244).
- El impacto en el *bien jurídicamente protegido*, puede tener un amplio margen de evaluación al afectarse a la Defensa y Seguridad Nacional con lo cual se convierte en un ataque directo a la soberanía de un país como también puede provocar situaciones de amenaza o de daño en el ámbito económico, social, político y de provisiones de servicios públicos.
- El análisis de la victimología también requiere ser reinterpretado especialmente porque el impacto puede provocar una condición que supere las capacidades del Estado para la provisión de medidas de atención y protección a su población, a su economía o a su propia seguridad interna y externa.

En el ámbito de la afectación a personas, estas pueden implicar situaciones de naturaleza penal respecto de la ejecución que afecten el ámbito financiero, comercial, económico o bancario y situaciones que afectan la intimidad y derechos de naturaleza privada, cuyo impacto puede provocar una condición de tratamiento criminológico vinculado a la *trata de personas*, si se afecta la intimidad de niños o niñas (Tirado et al, 2021, p. 1011).

El Ciberespacio como Herramienta para la Perpetración del Ciberterrorismo

Se ha evidenciado que el ciberterrorismo puede ser llevado a cabo de una manera prácticamente sencilla, pero esto solo se ha podido concluir debido a la influencia del ciberespacio en la sociedad. La masificación de la información, la velocidad con la que ésta es enviada y la gran recepción que recibe es el cóctel clave para que los ciberdelincuentes puedan ejecutar actos de ciberterrorismo, logrando su finalidad de infundir pánico generalizado, conllevando a la alteración del orden público y/o político.

La inmediatez y el fácil acceso al ciberespacio a través del internet permite que el ciberterrorismo emplee esta herramienta para lograr su cometido debido sobre todo a un registro de vacíos legales y jurídicos que impiden la tutela de DDHH en algunos rincones del internet, como la Deep Web o la red TOR (Carrera et al, 2020, p. 1264), que complican su persecución criminal y posterior punición (Bardavio, 2020, p. 393).

Dicho lo anterior es pertinente esclarecer que el ciberespacio es la herramienta clave y principal para que los ciberdelincuentes puedan ejecutar actos de ciberterrorismo donde la comunicación instantánea y masiva de información ayuda a la difusión del miedo generalizado en la sociedad. Un elemento que permite detallar algunas condiciones, especialmente debido a la amplitud de elementos que la componen:

- Respecto de sus componentes, el ciberespacio es un término que implica el uso de herramientas tecnológicas y digitales que emplea el internet a través de una interacción de personas y sistemas informáticos, por lo que una sola persona o un colectivo pueden emplear infraestructuras digitales, informáticas o de telecomunicación establecidos en redes o canales de recepción múltiples, de forma directa, indirecta, bajo autorización o sin autorización de una contraparte donde el uso de información puede provocar una condición negativa en el uso de herramientas digitales, tecnológicas o de servicios en una zona predeterminada por quien ejecuta un "ataque cibernético".

  En este sentido, el uso de la tecnología por parte de un gobierno en un Estado a través de sus agencias especializadas o por organizaciones ajenas a una estructura gubernamental puedan emplear los recursos digitales y tecnología

- Respecto del alcance de un ataque desde el ciberespacio, es importante tener en cuenta que no todos los países y potenciales víctimas pueden ser evaluadas en la misma dimensión respecto de las consecuencias que pueden generarse.

  En este sentido, el uso de satélites, el uso de cableado de transmisión de energía eléctrica o de datos de internet o el uso de infraestructura puede generar las condiciones propicias para que se pueda ejecutar un acto de ciberataque.

De este modo, se ha llegado a generar un *medio ambiente artificial* basado en el uso de la tecnología y de la difusión de información a través del internet que prácticamente puede tener un alcance global (Castells, 2009, p. 88).

- La evaluación del *contenido* de una "información" que puede ser difundido por un ciberataque incide en la naturaleza criminológica de los hechos evaluados y condiciona su tipificación como "ciberdelito" o como "ciberterrorismo", porque la información será calificada en función a los intereses que un determinado gobierno en función a las consecuencias económicas, políticas o internacionales que pueda provocar, tal como se puede desprender de la evaluación del caso de Wikileaks (Wegener, 2012, p. 145).

  Consecuentemente, la "información" que se pueda difundir, afectar, visualizar o modificar puede tener consecuencias en las decisiones gubernamentales que pueden afectar sus políticas de Defensa y Seguridad Nacional, sus relaciones diplomáticas, la regulación y desarrollo del comercio interno e internacional, como también sus ámbitos de regulación de telecomunicaciones, comerciales, civiles, constitucionales y penales.

  Un detalle que puede incidir en la gobernabilidad en un país, puede afectar el uso de los sistemas democráticos por parte de la población sobre todo en el ámbito de la fiscalización y control de las actividades gubernamentales (Sánchez, 2016, p. 227), y en la difusión de información concerniente a la gestión pública cuya condición puede resultar contrario a los intereses de las altas autoridades, el desarrollo de las actividades del gobierno o a la propia Defensa y Seguridad Nacional (Sánchez, 2013, p. 510).

- Finalmente, en el ámbito de una mayor difusión de información en un mundo globalizado, las acciones que generan odio y condiciones negativas entre grupos humanos por razones ideológicas, religiosas, sexuales, comerciales o políticas son el campo de cultivo de los mayores actos de ciberterrorismo (Gómez, 2018, p. 415).

  Una condición que afecta sobre manera la perspectiva y desarrollo normativo, jurisprudencial y doctrinario al superarse los ámbitos usuales de evaluación de la jurisdicción, de la aplicación de la ley en

> el espacio y en el tiempo y la naturaleza de los actos de represión porque la condena de estos actos no siempre llega a ejecutarse.
>
> Una condición que puede ser ampliamente debatido y evaluado en el contexto de las situaciones de corrupción que se generan a través del uso de la tecnología y de los sistemas digitales, sobre todo para ejecutar actos que inciden en las decisiones de gobierno en un país desde el exterior que son conocidos como los delitos transnacionales (Bermúdez-Tapia et al, 2021, p. 128).

La Tipificación del Ciberterrorismo en la Tipificación Penal en el Ámbito Internacional y Nacional

El impacto de las situaciones delictivas generadas en el ciberespacio ha provocado una reacción en el ámbito dogmático y jurisprudencial para poder abordar con eficacia situaciones que han afectado la dignidad, derechos de naturaleza sexual y bancaria-económica de personas, la ciberseguridad y la ciberdefensa (Zunzunegui, 2008). Por esta razón, cuando se trata del ciberterrorismo es fundamental hacer una exposición de cómo la norma nacional e internacional ha actuado conforme a la creación y documentación de este ciberdelito de impacto desenfrenado.

Ante esta necesidad, evaluaremos en primer término el contexto comparativo internacional para luego evaluar el alcance normativo en Colombia, más aún cuando se atraviesa por um Gobierno de turno a cargo del Presidente Gustavo Petro en desarrollo del plan de governo de la Paz total y la seguridad humana.

En el ámbito internacional, se han promulgado una serie de reglamentaciones y convenios relacionados al tratamiento de la ciberdelincuencia, cuya finalidad es atender por medio del Derecho y las leyes conductas perversas con el propósito de proteger adecuadamente el nuevo bien jurídico de la seguridad de los datos, la información y las funciones de los sistemas informáticos. (Convención de Budapest,2001 Artículo 1), (Directiva 2013/40/UE Artículo 2)

De manera puntual, para el desarrollo de este trabajo es pertinente realizar hincapié y profundizar en el siguiente ámbito normativo internacional:

- **Convenio sobre la Ciberdelincuencia, Budapest, 2001.**

  De manera específica, prevé la creación, implementación y aplicabilidad de una legislación penal con miras a perpetrar, sancionar y establecer límites o parámetros relacionados con la comisión de conductas punibles a través de internet, medios electrónicos, plataformas digitales, entre otras. Lo anterior, con una metodología basada en mejorar la eficacia de las investigaciones y procedimientos

penales relativos a delitos cometidos a través de la Red, y, por otra parte, permitir la obtención y mantención de la evidencia electrónica obtenida en estas investigaciones, con miras a su inclusión en juicio. (Novoa et al., 2020, p. 15).

Un marco normativo que permite el desarrollo de esquemas normativos y legales en los países para que pueda generarse un contexto vinculante que pueda ser eficaz (Novoa, 2020, p. 15). De este modo, se entiende al ciberespacio como un "Espacio virtual de interacción que surge directamente como un lugar relacional, es decir su existencia sólo será efectiva cuando haya intercambio de información, siendo por tanto espacio y medio" (Romero, 2002, p. 2).

- **Reglamento (UE) 2019/679 Del Parlamento Europeo y del Consejo refiriéndose en su contenido de manera principal al uso, tratamiento y protección de los datos personales.**

  El desarrollo e impacto de la tecnología a nivel socioeconómico y en la realidad mundial permite enfatizar en la relevancia de la "administración de información", tanto en el ámbito personal como en el ámbito económico-comercial, político e internacional.

  En este sentido, el tratamiento de datos personales es valorado como un Derecho Fundamental sujeto de protección por encontrarse estrechamente relacionados con aspectos íntimos y privados de un individuo. De este modo, el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) así lo regulan de forma expresa.

  Este reglamento de manera breve, abarca con claridad el reto asumido frente a la rápida evolución tecnológica y de medios electrónicos que requieren información personal, obligando a una acción objetiva y específica a las autoridades públicas respecto del control, manejo y tutela de la seguridad jurídica, conforme detalla el Reglamento (UE) 2019/679 del Parlamento y del Consejo de la Unión Europea (27 de abril de 2016).

- **Directiva 2013/40/UE Del Parlamento y del Consejo de la Unión Europea.**

Una norma que permite que los Estados y sus organismos públicos están plenamente obligados a garantizar el respeto de los derechos y las libertades fundamentales, de conformidad con las obligaciones de la Unión e internacionales existentes, conforme detalla el artículo 21.

En su contenido expresa también las políticas de prevención de los ciberdelitos, tratamiento, uso y protección de los mismos como también, aportar las garantías sobre los derechos de las personas y el uso de principios de naturaleza jurídica en la evaluación de estos hechos. Dicho lo anterior, resulta interesante destacar el análisis de información que tal directiva documenta con relación a los ciberataques, sus perjuicios, ejecución y materialización.

De este modo, se genera las condiciones criminológicas y judiciales para imponer penas y sanciones, de acuerdo a una clasificación en favor de establecer si el caso es de menor o mayor gravedad, como también puede presentarse en el marco de una organización delictiva, que soporta un sanción más severa, Dicho lo anterior, corresponden a situaciones donde se requiere la responsabilidad penal respectiva con la intervención de los Estados Miembros, quienes definen cuáles son las condiciones agravantes para cada caso en concreto.

- **Decisión Marco 2005/222/ JAI Del Consejo de la Unión Europea.**

Establece un ámbito de desarrollo de trabajos conjuntos por parte de las autoridades competentes como la policía y las autoridades judiciales con miras a arrimar la legislación penal con respecto a los ataques contra los sistemas de información.

Guiando la proyección de analizar las funciones de las presentes regulaciones internacionales, es posible establecer un grado de semejanza en cuanto al contexto de ciberataques posicionándolo en el marco de la delincuencia organizada, siendo un punto de eje importante ya que, “Los primeros escenarios de la delincuencia organizada se focalizan en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios” (Sánchez, 2012, p. 143).

Esta decisión parte de la visibilidad que tienen los ciberdelitos y lo que desencadenan, las afectaciones a la seguridad jurídica, socioeconómica y a la libertad propiamente dicha. Lo que es más relevante para esta regulación internacional se encuentra plasmado en dos aspectos, a saber:

a) Intervención de la legislación penal con relación a la comisión de conductas punibles que afecten los sistemas de información, datos personales y seguridad en la web.
b) Colaboración y cooperación policial y judicial con relación a ciberdelitos, ciberataques, delincuencia organizada y ciberterrorismo, para imponer sanciones penales efectivas.

Esto, en común acuerdo acaece en una proyección de garantizar los derechos fundamentales e inhibir prácticas que afectan la seguridad jurídica, van en contra del Derecho y no permiten un correcto tránsito o flujo de información en línea, generando caos, miedo e inseguridad por parte de los usuarios a nivel mundial.

- **Acción Común 98/733/JAI, de 21 de diciembre de 1998 cuya finalidad está orientada a imponer sanciones penales sobre quienes a través de los ciberataques vulneren los derechos e intereses esenciales de los demás. Se refiere también, a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea (Artículo 15).**

  En relación a esta regulación internacional, es debido mencionar que por medio de su contenido hace énfasis en la figura del Derecho objetivo, toda vez que, mediante la tipificación de conductas delictivas relacionadas con vulneración de derechos fundamentales como el tratamiento de datos personales y conductas punibles en el marco de la web, específicamente la tipificación en lo que a ser miembro de una organización delictiva, adopta un carácter legislativo sujeto de cumplimiento. Por lo cual es debido entender cómo y de qué manera se interpreta este delito.

  Es una asociación estructurada de más de dos personas, establecida durante un cierto período de tiempo, y que actúe de manera concertada con el fin de cometer delitos sancionables con una pena privativa de

> la libertad o medida de seguridad privativa de libertad de un máximo de al menos cuatro años como mínimo, o con una pena aún más severa, con independencia de que estos delitos constituyan un fin en sí mismos o un medio de obtener beneficios patrimoniales y, en su caso, influir de manera indebida en el funcionamiento de la autoridad pública. Acción Común 98/733/JAI, 1998 (21 de diciembre de 1998).

En cuanto a la regulación nacional se refiere debemos enfatizar que el hecho de un "ciberterrorismo" todavía no se ha tipificado. Una situación que proviene del contexto normativo nacional evaluado en forma sistemática en tanto eso, deriva o se encuentra relacionado con otros tipos penales terroristas.

De este modo, en Colombia existen figuras informáticas delictivas como la expresa el Artículo 195 de la siguiente manera: "Acceso abusivo a sistema informático protegido con medida de seguridad", inspirado en la Convención de Budapest, ya mencionada.

Así pues, por medio de ley 1273 de 2009, se creó un cuerpo jurídico de ciberdelitos consagrado en el Título VII bis (artículos 269 A y siguientes), con el fin de procurar obtener la salvaguarda de bienes jurídicos, derechos, sirviendo también como herramienta jurídica para evitar y mitigar la impunidad relacionada con delitos informáticos:

La modificación del Código Penal, creó 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 (L. 1273, 2009).

Esta Ley comprende que existe un problema frente a la protección y seguridad de los derechos fundamentales de los usuarios del ciberespacio y encuentra que hay múltiples conductas que, al ser perpetradas tiene matices de componer un acto punitivo. Por tales razones, el legislador encuentra (aunque de manera laxa) diez conductas que deben ser tipificadas en torno al cibercrimen. Estas se encuentran en los artículos:

- Respecto del "Acceso Abusivo a un Sistema Informático (Artículo 269 del Código Penal).
- La Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación (Artículo 269B del Código Penal).
- La Intercepción de Datos Informáticos (Artículo 269C del Código Penal).
- El Daño Informático (Artículo 269D del Código Penal).
- El Uso de Software Malicioso (Artículo 269E del Código Penal).
- La Violación de Datos Personales (Artículo 269F del Código Penal).

- La Suplantación de Sitios Web para Capturar Datos Personales (Artículo 269G del Código Penal).
- Las Circunstancias de Agravación Punitiva (Artículo 269H del Código Penal).
- El Hurto de Medios Informáticos y Semejantes (Artículo 269I del Código Penal).
- La Transferencia no Consentida de Activos (Artículo 269J del Código Penal).

Sin embargo, con esta regulación solamente se planteaba la regulación y protección de los derechos en torno a la seguridad y privacidad de información personal con relación al manejo de datos. Por tales razones, si bien es cierto que el marco normativo colombiano sustenta y fundamenta la existencia de conductas ocurridas en el ciberespacio que atentan contra derechos fundamentales de los ciberusuarios, es cierto también que la legislación es demasiado laxa e incluso inexistente frente a conductas que conllevan a la vulneración de muchos otros derechos, teniendo como ejemplo el ciberterrorismo.

Es necesario reconocer el esfuerzo del legislador colombiano en 'innovar' y tener en cuenta las nuevas modalidades de crimen, y por ende también se debe continuar trabajando en la adición de nuevos tipos penales en los cuales la conducta del ciberterrorismo y sus derivados sean legalmente prohibidos y sancionables con el fin de que el Estado colombiano pueda proteger, garantizar y evitar el desgaste de los derechos fundamentales de las ciber víctimas. Por ende, dando cierre a este apartado es necesario decir que Colombia es un Estado pionero en el desarrollo de la regulación de las conductas en el ciberespacio y que, esto es necesario para que el legislador colombiano no se frene en la tipificación de las nuevas modalidades de cibercrimen, haciendo hincapié en el ciberterrorismo, puesto que, como se evidenciaba anteriormente, el delito de ciberterrorismo es la fuente de múltiples conductas que deben ser sancionadas

PROPÓSITO

El propósito de esta investigación es dar a entender el panorama futuro que respecta al mundo jurídico (en particular el colombiano) frente a las conductas que vulneran DDHH y que están sucediendo en el presente, derivadas del emergente impacto del ciberespacio y las nuevas tecnologías en la actualidad. La conducta que genera mayor zozobra dentro del ciberespacio es la del ciberterrorismo. Por ende, la investigación pretende exponer de manera clara y fácil para todo el público la importancia de mitigar el daño que el ciberterrorismo puede ocasionar sobre los DDHH de los cibernautas, además, pretende exponer la dimensión actual del marco jurídico colombiano con respecto a la regulación y sanción de dichas conductas. Así

las cosas, la investigación tiene por objetivo ser pionera en cuanto propone y plantea alternativas que pueden ser implementadas en el ordenamiento jurídico colombiano y emplea un lenguaje dinámico y asertivo que permite comprender el contexto histórico que ha conllevado a la creación del ciberterrorismo y, a su vez, los impactos que ocasiona sobre los DDHH de las personas dentro del ciberespacio.

METODOLOGÍA

El método de investigación utilizado fue cualitativo mediante la técnica que se basa en el análisis jurídico y doctrinal de carácter expositivo. De esta manera, es posible comparar mediante el exhaustivo estudio de la teoría que recubre el escenario internacional con respecto de la estructura de la misma dentro del ordenamiento jurídico colombiano. Con respecto al estudio de las leyes que se sincronizan con la materia, es posible dilucidar lo que representa en parte la solución a la hipótesis inicial de la investigación, permitiendo corroborar, o no, la importancia de la regulación del ciberespacio en Colombia.

HALLAZGOS

En lo concerniente a los hallazgos encontrados, fue posible determinar que dentro de la regulación jurídica colombiana, específicamente en el código penal, el delito de ciberterrorismo, aunque adopta un carácter imperativo y necesario, no se encuentra tipificado tácitamente. toda vez que, en su contenido si bien aborda conductas punitivas en materia de vulneración a derechos fundamentales a través de la comisión de otros tipos penales terroristas, no concluye con la creación de un tipo penal que se refiera en debida forma y estricto sentido al ciberterrorismo. así pues, como punto de análisis, el resultado encontrado condujo hacia la reflexión detenida sobre el impacto del ciberterrorismo en la seguridad personal y nacional, con miras a desatar y despertar el interés para que la legislación colombiana, en relación con la formulación de políticas o proyectos de ley en cabeza del congreso de la república visibilicen, regulen y sancionen estas conductas criminales en el ciberespacio, para

Dicho lo anterior, es importante mencionar que el enfoque sobre el discurso del ciberterrorismo, y la metodología de la investigación realizada suscitó establecer a grandes rasgos nuevas funciones del marco jurídico colombiano, las cuales deben prever garantías bajo los principios constitucionales de derecho para ciber víctimas y ciber delincuentes.

IMPLICACIONES PRÁCTICAS

Esta investigación adopta un carácter influyente dentro de la sociedad por el público lector a quien se dirige, ya que abarca el interés por la protección de la

seguridad de cada individuo que figura como usuario dentro del ciberespacio. además, por el interés encaminado a garantizar la seguridad nacional; así, se tiene la expectativa de que al visibilizar y ejecutar conductas para que los delitos que atentan contra los derechos de las personas en el ciberespacio, trascienden a un plano físico, en el cual puedan ser objeto de sanción y la impunidad se reduzca considerablemente.

Las implicaciones para la práctica sugieren romper los paradigmas y transitar un terreno desconocido en materia de legislación cibernética, específicamente sobre el tipo penal de ciberterrorismo. El impacto generará transiciones a nivel socioeconómico ya que el ciberespacio y las operaciones en él, están estrechamente relacionadas con la globalización y la manera en que las sociedades se comunican e interconectan. como característica principal, es debido mencionar el propósito de garantizar los derechos humanos.

A su vez, pretende educar e informar a la población sobre este fenómeno con originalidad puesto que esta investigación posee un factor atrayente para quienes consideran que en la amplitud del derecho y las leyes habita un carácter extenso y gratamente interesante, objeto de estudio e investigación. Por ello, su aplicabilidad puede incurrir incluso en un plano virtual que trasciende al físico, el cual debe ser regulado por las leyes y el derecho para garantizar el orden, la seguridad nacional y los derechos humanos de los individuos.

La presente investigación contribuye significativamente al discurso del ciberterrorismo dentro del contexto del marco legislativo colombiano. está escrito con la firme intención de que su argumento sea claro y fácil de comprender por cualquier lector tenga conocimiento, o no, en el ámbito jurídico. Así mismo, la metodología condujo hacia un exhaustivo análisis jurídico y dogmático que soporta y brinda solidez al contenido del mismo.

CONCLUSIONES

Teniendo en cuenta la pregunta planteada, los resultados de la investigación demuestran que la creación y ampliación sobre la tipificación del delito informático de ciberterrorismo por parte del legislador en el Código Penal colombiano son requeridas, puesto que con esto se permitirá la imposición de sanciones pertinentes que mitiguen dichas conductas que afectan la seguridad y la privacidad personal y nacional. Así las cosas, se entiende que el desarrollo normativo colombiano frente a la tipificación penal de los ciberdelitos, pues, si bien está estructuralismo, sigue teniendo un punto de partida vastamente generalizado, lo que impide que la materialización de la conducta delictiva pueda ser punible y elevada a la repercusión legal.

Por consiguiente se encuentra que trabajar en torno a la creación de un marco normativo punitivo de las conductas ciber delictivas es imperativo para garantizar el

cumplimiento de los derechos fundamentales y la seguridad de la población colombiana, debido a que se logró exponer la manera en la que el cibercrimen funciona alrededor del mundo, además de las formas en las que las ciber víctimas no son retribuidas por la perpetración del crimen y la alta impunidad que se deriva de la escasez normativa frente a estas conductas.

Los fenómenos informáticos que han traído la evolución consigo, y las nuevas tecnologías de la información con fines económicos, financieros, culturales, académicos, recreativos y de comunicación significan un reto para el Derecho visto desde varias perspectivas, como la regulación y normatividad a aplicar; dicho lo anterior lo que resulta pertinente es atender a su desarrollo y emplear los recursos existentes con fines positivos y de innovación para la sociedad.

Una alternativa para inhibir los índices de impunidad está dada en la regulación de delitos como el ciberterrorismo, para que los datos y la información personal, por medio de los límites de la ley procure siempre estar destinada a ser un bien jurídico que deba ser protegido.

Ante la existencia de diversa normatividad internacional sobre las sanciones, el manejo y la protección de la información personal, es posible que la legislación Colombiana tome lo previamente mencionado como referente y amplíe el bagaje normativo para que conductas ciber delictivas como el ciberterrorismo no sean excluidas, evitando el sesgo proporcionado a la sociedad por su no tipificación, ya que se puede sucumbir a pensar que "como no está prohibido, está bien, ó lo puedo hacer" siendo claramente una afirmación errada.

Ya hecho el recorrido normativo e histórico sobre el ciberterrorismo, es pertinente dar respuesta al interrogante planteado como eje de este trabajo: ¿Por qué la no existencia de una legislación que determine y sancione el ciberterrorismo de manera formal dentro del Código Penal atenta contra la seguridad y los derechos fundamentales de la población en Colombia?

Es necesario recalcar que según lo demostrado a través del desarrollo del trabajo, la no existencia de una legislación completa y robusta en contra del ciberterrorismo atenta contra la garantía de derechos fundamentales y la seguridad de los usuarios del ciberespacio, puesto que es sabido que, el ciberterrorismo está a las puertas de la masividad y el anonimato en el ciberespacio y por tal motivo debe ser contemplado como una alarma para que el legislador penal colombiano lo entienda como un ciberdelito desenfrenado que puede ser pluriofensivo y debería ser estudiado dogmáticamente como un ciberdelito de peligro y de resultado.

Así las cosas, como próximos pasos el marco jurídico colombiano debe ampliar y fortalecer la legislación existente frente al ciberespacio y las conductas punibles que allí se cometen, esto lo debe hacer desde el estudio del nuevo paradigma de la criminología contemplado en la creación de los ciberdelitos, además de esto, debe comprender un proceso garantista para los ciberdelincuentes y las ciber

víctimas con el fin de no retroceder en el avance socio jurídico que la constitución nacional ha aportado a lo largo de los años.

REFERENCIAS

Bardavío Antón, C. (2020). Ciberdelitos: evolución hacia un derecho penal funcional incorrectamente dogmatizado. *Ciberdelitos: evolución hacia un derecho penal funcional incorrectamente dogmatizado*, (pp. 393-414), en Bustos Rubio, M., Abadías Selma, A. & del Moral García, A. (directores) *Una década de reformas penales: análisis de diez años de cambios en el Código Penal (2010-2020)*. J. M. Bosch Editor

Barrio Andrés, M. (2018). *Ciberdelitos: amenazas criminales del ciberespacio: Adaptado reforma Código Penal 2015*. Editorial Reus.

Bermúdez-Tapia, M. (2019 noviembre) Enfrentando al macrodelito desde el Estado. *Actualidad Penal.* (65), 277-288.

Bermúdez-Tapia, M. (2020). La influencia de la capacidad bélica sobre la soberanía nacional en las relaciones internacionales. *Revista Científica General José María Córdova*, *18*(30), 291-306.

Bermúdez-Tapia, M, Sierra-Zamora, P.A. & Ramírez Benítez, E. P. (2021) América Latina, el caso Lava Jato y la aversión al riesgo frente a la corrupción, (pp. 127-168), en Rey Pinto, Eva María y Rodríguez Samora, Diego (Editores.) *Crimen organizado transnacional y dimensiones culturales en América Latina.* Bogotá: Escuela Superior de Guerra "General Rafael Reyes Prieto"- Editorial Planeta. iSBN 978-958-42-9990-1.

Carrera Calderón, F. A., Cadena Sayavedra, F. H., Cepeda Luna, C. D., & Alvarado Villavicencio, M. S. (2020). Los delitos en la Deep Web y sus efectos sobre las Cibervíctimas frente a la legislación ecuatoriana. *Revista UNIANDES Episteme*, *7*(1), 1263-1275. http://45.238.216.13/ojs/index.php/EPISTEME/article/view/2301/1646.

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

Clapham, C. (2002). The challenge to the state in a globalized world. *Development and change*, *33*(5), 775-795.

CONPES 3858. (2016), Política nacional de seguridad digital, p.88.

Fernández, I. N. (2018). La letalidad del ciberterrorismo. *Revista general de marina*, *275*(1), 133-142.

Gamón, V. P. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *URVIO, Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93.

Gamón, Vicente Pons. (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.

Girao González, F., & González-García, A. (2020). Capacidades prospectivas y de defensa en la lucha contra el Ciberterrorismo. Análisis del Caso Español. *Relaciones Internacionales*, *29*(58), 1-25.

Gómez Martín, V. (2018). Odio en la red. Una revisión crítica de la reciente jurisprudencia sobre ciberterrorismo y ciberodio. *Revista de Derecho penal y Criminología*, (20), 411-449.

González Amado, I. (2007) Ciberterrorismo. Una aproximación a su tipificación como conducta delictiva. *Derecho Penal y Criminología. Revista del Instituto de ciencias Penales y Criminológicas*, 28(84), 13-46

Llinares, F. M. (2012). *El cibercrimen*. Marcial Pons Ediciones Jurídicas y Sociales.

López Gorostidi, J. L. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. *Estudios de Deusto*, *68*(1), 201-221.

Mendoza Buergo, B. (2001). Límites dogmáticos y político-criminales de los delitos de peligro abstracto, Granada Comares, 2001, pp. 152 y ss.

Miró Llinares, F. (2015). Cibercrimen y vida diaria en el mundo 2.0. *Cibercrimen y vida diaria en el mundo 2.0.*, 415-455.

Nava Garcés, A. E. (2016). Ciberterrorismo: la nueva cara de la delincuencia en el siglo XXI. La participación y fomento al delito por órganos de gobierno y empresas. *Revista Penal México*, *6*(11-12), 151-165. Recuperado a partir de https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/255.

Ota Martínez, R. (2005) Ciberterrorismo. *Revista de derecho informático*, 82. http://ceese- den-terrorismo.tripod.com/id71.html

Richardson, J. (2011). Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. *John Marshall Journal of Information Technology & Privacy Law*, (29)1, 1-28. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1697&context=jitpl.

Salinero Echeverría, S. (2015). El crimen organizado en Chile: Una aproximación criminológica al perfil del delincuente a través de un estudio a una muestra no representativa de condenados por delitos de tráfico de estupefacientes. *Política criminal*, *10*(19), 25-55.

Sánchez Barrilao, J. F. (2016). El Derecho constitucional ante la era de Ultrón: la informática y la inteligencia artificial como objeto constitucional. *Estudios de Deusto: revista de Derecho Público*, *64*(2), 225-258.

Sánchez Ferro, S. (2013). La última jurisprudencia de la Corte Costituzionale italiana en materia de secretos de Estado. *Teoría Y Realidad Constitucional*, (31), 503–528. https://doi.org/10.5944/trc.31.2013.10318.

Sánchez Medero, G. (2015) El ciberterrorismo: de la web 2.0 al internet profundo. *Revista Ábaco*, 3(85), 100-108. https://www.revistasculturales.com/xrevistas/PDF/72/1873.pdf.

Sánchez Verga, F., Martínez Guirao, J. E. & Téllez Infantes, A. (2022) La seguridad en el ciberespacio desde una perspectiva sociocultural. *Methaodos. Revista de Ciencias Sociales*, 10(2), 243-258.

Sierra-Zamora, P. A., & Bermúdez Tapia, M. (2021). La Incidencia Del Narcotráfico En Las Altas Esferas Del Gobierno Peruano. *Novum Jus*, *15*(2), 259-293. https://doi.org/10.14718/10.14718/NovumJus.2021.15.2.10.

Tirado Acero, M., & Cáceres Tovar, V. M. (2021). La política criminal frente al ciberdelito sexual contra niños, niñas y adolescentes en Colombia. *Revista Científica General José María Córdova*, *19*(36), 1011-1033.

Verton, D. (2004) *La amenaza invisible del ciberterrorismo. Black Ice.* McGraw Hill

Wegener, H. (2012). La "ciberguerra" se puede evitar. *Política exterior*, *26*(146), 140-153.

Weinberger, S. (2011). Is this the start of cyberwarfare? Last year's Stuxnet virus attack represented a New kind of threat to critical infrastructure. *Nature*, *474*(7350), 142-146.

Zunzunegui, S. (2008). El ciberterrorismo: Una perspectiva legal y judicial. *Eguzkilore*, *22*, 169-187.

LEGISLATION

Colombia

Ley 1273 de 2009. Por la cual se modifica el código penal y se añade un nuevo bien jurídico tutelado. 5 de enero de 2009. D.O. No. 47223.

Código Penal Colombiano. Ley 599 de 2000. Julio 24 del 2000.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET