Estado y soberanía en el ciberespacio*

[Artículos]

Eduardo Andrés Perafán Del Campo[**]
Sebastián Polo Alvis[***]
Marco Emilio Sánchez Acevedo[****]
Catalina Miranda Aguirre[*****]

Fecha de recepción: 5 de noviembre de 2020
Fecha de aprobación: 7 de diciembre de 2020

* Este artículo es resultado del proyecto de investigación "Derecho, Estado y sociedad", adscrito a la línea "Derecho constitucional y políticas públicas", del grupo de investigación Derecho Público y TIC (G-TICCY), de la Universidad Católica de Colombia.
** Candidato a doctor en Ciencias Sociales, Dinámicas y Cambios en el Espacio y en la Sociedad de la Globalización por la Universidad de Granada, España. Magíster en Estudios Políticos e Internacionales y Politólogo de la Universidad del Rosario, Colombia. Editor académico de la revista científica *Novum Jus*. Profesor universitario e investigador del grupo de investigación en Derecho Público y TIC de la Facultad de Derecho de la Universidad Católica de Colombia. Analista y consultor en asuntos públicos e internacionales. Correo electrónico: eaperafan@ucatolica.edu.co, eduardoapdc@gmail.com; ORCID: https://orcid.org/0000-0002-9981-2679
*** Estudiante de Maestría en Economía de las Políticas Públicas de la Universidad del Rosario. Politólogo de la Universidad del Rosario. Profesor e investigador de la línea de investigación "Dinámicas y asuntos internacionales" del Grupo de Estudios Políticos Internacionales (GEPI), de la Facultad de Ciencia Política y Gobierno de la Universidad del Rosario. Correo electrónico: sebastian.polo@urosario.edu.co; ORCID: https://orcid.org/0000-0003-2950-6710
**** Doctor en Tecnologías de los Servicios de la Sociedad de la Información de la Universidad de Valencia, España. Especialista en Derecho Constitucional y en Gobierno Local Electrónico. Abogado y profesor de posgrado de la Universidad Católica de Colombia e investigador de la línea de investigación "Derecho y TIC". Correo electrónico: mesanchez@ucatolica.edu.co; ORCID: https://orcid.org/0000-0002-7745-2182
***** Internacionalista de la Universidad del Rosario, investigadora del Centro de Pensamiento Estratégico y Proyección Institucional de la Oficina de Planeación, Policía Nacional de Colombia. Asesora de la Dirección de Justicia, Seguridad y Gobierno del Departamento Nacional de Planeación. Correo electrónico: cmiranda92@hotmail.com; ORCID: https://orcid.org/0000-0002-3017-5915

Citar como:

Perafán Del Campo, E. A., Polo Alvis. S., Sánchez Acevedo, M. E. y Miranda Aguirre, C. (2021). Estado y soberanía en el ciberespacio. *Via Inveniendi Et Iudicandi*, *16*(1). https://doi.org/10.15332/19090528.6480

Resumen

El presente trabajo tiene como objetivo estudiar la transformación del concepto de soberanía estatal frente a la emergencia del ciberespacio. De esta forma, la ideas que se desarrollarán en este artículo partirán de la reconstrucción de las nociones tradicionales de soberanía estatal, la revisión de los enfoques de actuación estatal en el contexto de la gobernanza global del internet, la conceptualización de las nuevas formas de ejercicio de la soberanía estatal en el ciberespacio y el desarrollo del caso colombiano como ejemplo en materia de ciberseguridad y ciberdefensa.

Palabras clave: soberanía, Estado, ciberespacio, ciberdefensa, internet.

State and sovereignty in cyberspace

Abstract

This paper aims to study the transformation of the concept of state sovereignty regarding cyberspace's emergence. Thus, the ideas that will be developed in this article will be based on the reconstruction of the traditional notions of state sovereignty, the review of approaches related to state actions in the context of global internet governance, the conceptualization of the new forms of exercising state sovereignty in cyberspace and the development of the Colombian case as an example of cybersecurity and cyberdefense.

Keywords: sovereignty, State, cyberspace, cyber defense, internet.

Introducción

Tras los diversos cambios que se han desarrollado con la transformación de las interacciones humanas al nivel global, posibles gracias a la progresiva y acelerada modernización de los medios de comunicación, los retos sobre la vigilancia y el control de la libertad de los ciudadanos incluyen nuevos desafíos derivados de estos avances tecnológicos en la era de la virtualización. Con la consolidación de la cobertura, la velocidad de navegación y el acceso a nuevos dispositivos de tecnología para la navegación, el uso del internet ha generado nuevos cuestionamientos sobre el ejercicio de la libertad de las personas y del rol que deben asumir las instituciones, así como medio para la consecución de información, para el establecimiento de todo tipo de interacciones entre personas que trascienden el contacto humano, entre otros elementos que han permitido una dinamización total de las actividades productivas humanas.

El problema no solo reside en el establecimiento de una nueva dimensión de acción por cubrir en temas de legislación, protección y vigilancia, sino también es un reto para la especialización de funciones que permita una acción pertinente del Estado. Por lo tanto, es necesario comprender el posible nexo entre el fenómeno de la masificación del uso y acceso al internet y las responsabilidades del Estado de ejercer un control adecuado frente a este proceso, específicamente en el establecimiento de una relación causal que incide en una transformación del Estado tanto en el ejercicio de nuevas funciones para la protección de la ciudadanía, como en el surgimiento de nuevos interrogantes que pueden contribuir a la mutación de la percepción de la soberanía del Estado (Barragán y López, 2018; Rodríguez, 2020).

La relevancia que el internet ha cobrado en nuestro diario vivir es evidente. Desde la mayoría de medios y sistemas de información y comunicación a nivel internacional, pasando por el sistema financiero

mundial, hasta los protocolos de activación de misiles nucleares, todos poseen como base para su funcionamiento el internet. Esta herramienta ha evolucionado de forma tal que ha creado un nuevo espacio virtual de interacción, el cual desdibuja las fronteras territoriales e integra a quienes tienen acceso al mundo digital en una red compleja de transmisión de información: el ciberespacio (Mansell y Raboy, 2011)

Este espacio virtual de interacción ha dado paso al mejoramiento de la comunicación entre una gran diversidad de actores a nivel internacional, los cuales intercambian información a asombrosa velocidad respecto a una inconmensurable variedad de asuntos. El ciberespacio no es solo el escenario en donde se intercambia información sobre asuntos que en principio podríamos considerar como de entretenimiento para el usuario, los cuales giran alrededor de la cultura pop, el cine, la televisión y la música. En internet también se desarrollan asuntos de carácter económico, político y social que demandan una considerable proporción de la atención de dicha diversidad de actores en el ciberespacio.

La convergencia de contenidos de carácter económico, político y social en el internet, y las condiciones particulares de dicha red, han permitido que esta se transforme en una importante plataforma de activismo político. Esto se puede observar en, por ejemplo, el uso del internet como catalizador de la primavera árabe, la militancia internacional en apoyo a la liberación de Palestina y Cataluña, entre otros casos (Soengas-Pérez, 2013). El internet posibilita la producción de contenidos que pueden tener impacto en el desarrollo de la vida política en los distintos ámbitos e instancias del Estado (Silva y Pérez, 2019).

El carácter transnacional del internet, la convergencia de una gran cantidad de actores internacionales en el ciberespacio, la facilidad y aparente libertad para la producción de diversos contenidos en la red (incluidos materiales sensibles), el impacto de dicha información en la

población, la constante evolución tecnológica y los desafíos que un mundo interconectado plantea (Koerner y Perafán, 2020), son algunos aspectos alrededor de los cuales los Estados deben reflexionar a partir del surgimiento de este nuevo espacio. Uno de estos elementos es la ciberseguridad y la ciberdefensa.

Se conoce con el nombre de *ciberespacio* al espacio artificial creado por el conjunto de sistemas de la información y telecomunicaciones que utilizan las tecnologías de información y comunicación (TIC), es decir, de redes de ordenadores. Mucho más que internet, más que los mismos sistemas y equipos, el *hardware* y el *software*, e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás, ha sido creado por el hombre para su servicio (Ministerio de Defensa, 2013). En otras palabras, el ciberespacio es la dimensión generada durante el tiempo de interconexión e interoperabilidad de redes, sistemas, equipos y personal relacionados con los sistemas informáticos, cualesquiera que sean estos, y las telecomunicaciones que los vinculan (Consejo Argentino para las Relaciones Internacionales, 2013).

Ahora, para entender la ciberseguridad se debe partir de la seguridad de la información, que, según Kosutic:

> Se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, donde por confidencialidad se entiende, la propiedad que la información no sea puesta a disposición de otros sin autorización, integridad es la propiedad de mantener la exactitud y completitud de la información y disponibilidad es la propiedad de ser accesibles y utilizables ante la demanda de una entidad autorizada. (Kosutic, 2012)

En este sentido, es posible entender la *ciberseguridad* como la seguridad de la información en el ciberespacio, en otras palabras, cuando se busca *proteger* la información contenida en el *hardware*, redes, *software*,

infraestructura tecnológica o servicios, nos encontramos en el ámbito de la seguridad informática o *ciberseguridad* (Medina, 2019).

Las ideas hasta ahora presentadas se desarrollarán alrededor de dos grandes temas en este artículo. El primero recogerá las discusiones sobre la mutación del ejercicio de la soberanía por parte de los Estados en un escenario en constante trasformación: el ciberespacio. El segundo desarrollará dos elementos fundamentales a través de los cuales los Estados ejercen su soberanía: la ciberseguridad y la ciberdefensa; estos dos elementos serán abordados a partir del caso colombiano. Metodológicamente, este trabajo se desarrollará mediante disertaciones teóricas sobre los límites y retos de la organización estatal en el ejercicio de su soberanía en el ciberespacio (Gallego, 2014). A partir de lo anterior, se procederá a esbozar diversos estudios de casos para el abordaje casuístico de los postulados teóricos y, por último, se construirán reflexiones finales sobre los diversos condicionamientos del Estado para su ejercicio de control en espacios virtuales.

Soberanía, Estado, tecnología y globalización

Estado y soberanía

Preguntémonos: ¿hasta qué punto, en un espacio cuyas fronteras son difusas, el ejercicio de la libertad del ciudadano puede considerarse como contraproducente para los intereses y responsabilidades del Estado? Para ello, es necesario comprender los límites y elementos incidentes en la condición ontológica de la soberanía estatal. Antes del abordaje de esta cuestión, es necesario afirmar que la soberanía es un elemento esencial para la preservación de la seguridad de los Estados (Burgos, 2018) y que la interconectividad es un elemento transformador de las sociedades y los individuos, en el marco de un proceso de globalización acelerada (Carreño

y Sánchez, 2018), y que estos dos son conceptos que tienden a contraponerse. Esto se debe a que la soberanía busca el establecimiento de unos límites de acción que contribuyan a la implementación de un ordenamiento determinado en pro de la seguridad y el orden dentro de una autoridad establecida, mientras que la interconectividad es un proceso que pretende trascender los límites anteriormente mencionados (Blanco, 2013).

En la tradición de la ciencia política existe una amplia literatura respecto al concepto de Estado. Sin embargo, si inspeccionamos algunas de sus definiciones tanto clásicas como modernas, podemos encontrar algunas características en común. Si consideramos el trabajo de Maquiavelo (2010), Hobbes (2009), Weber (1964), Kelsen (1949), Bobbio (1989), entre otros, podríamos caracterizar al Estado como una entidad jurídico-administrativa soberana que dispone del monopolio de la fuerza legítima y que se encuentra emplazada en un territorio, la cual tiene como fin garantizar el acceso a una serie de bienes contractuales para su población. Tal vez, los bienes más importantes que provee el Estado para estos autores son la seguridad, la administración de justicia y un paquete de derechos básicos consignados en la mayoría de las constituciones nacionales (Saidiza y Carvajal, 2016).

De manera complementaría, desde la sociología, cabe anotar que la forma particular en la cual el Estado provee estos bienes responde a los marcos de referencia moral (Galán, 2017) que, de manera histórica, han sido construidos por parte de la población emplazada en los dominios del Estado (Oppenheimer, 2014). En pocas palabras, el accionar estatal responde a una construcción social que parte de los imaginarios de los diversos actores que componen el Estado (Wendt, 2003). En este sentido, tal como puede ser constatado en la realidad, cada Estado se comporta de una forma particular frente a su población, al igual que la manera en la

cual reafirma su soberanía responde igualmente a criterios socialmente construidos.

De acuerdo con Burdeau, “el signo esencial de la soberanía es precisamente la posesión del poder constituyente” (citado por Peralta, 1999). Dentro de una perspectiva liberal, frente a la creación de un nuevo orden político y jurídico de los Estados por medio del acoplamiento estructural del sistema político y el sistema de derecho en una constitución, el establecimiento de una relación de autoridad es un factor que ha determinado el desarrollo de la concepción de la soberanía bajo los preceptos de este paradigma (Ramírez y Noguera, 2017; Schwartz, 2019). Asimismo, para Burdeau, la soberanía es una “característica, atribución o facultad esencial del poder del Estado que consiste en dar órdenes definitivas, de hacerse obedecer en el orden interno del Estado y de afirmar su independencia en relación con los demás Estados” (Burdeau, 1973, p. 248). Partiendo de esta definición, es posible vislumbrar que la soberanía es un elemento constitutivo del orden interno y de la legalidad inherente al Estado.

Empero, como resultado de las diversas transformaciones políticas, económicas e ideológicas sobre las teorías del Estado, manifestadas tras la caída de la Unión Soviética como símbolo del fin de la Guerra Fría, se daría apertura a un proceso de interconectividad que trascendería los órdenes nacionales vigentes en ese entonces (Laidi, 1998). Con el avance a gran escala de las tecnologías y los medios de comunicación y transporte, que se daría simultáneamente con la apertura y expansión del libre comercio, la cooperación internacional y la integración política, el Estado se vería en un proceso de replanteamiento de funciones ante la presencia de nuevos retos y problemáticas producto del advenimiento de nuevas coyunturas y amenazas latentes.

En este sentido, con base en los avances anteriormente mencionados, iniciaría un proceso crítico de transformación sobre la percepción y naturaleza de uno de los factores transversales de la sociedad y el Estado liberal moderno: el individuo. De acuerdo con Zygmunt Bauman, la aceleración de las dinámicas de interacción humana incide directamente en un proceso de individualización de la sociedad, que se materializa como la "capacidad práctica y realista de autoafirmarse, en detrimento de un proceso colectivo de ciudadanía" (2015, p. 15). De acuerdo con Bauman (2015):

> [...] liberar a la gente puede volverla indiferente. El individuo es el enemigo número uno del ciudadano, sugería De Tocqueville. El "ciudadano" es una persona inclinada a procurar su propio bienestar a través del bienestar de su ciudad, mientras que el individuo tiende a la pasividad, el escepticismo y la desconfianza a la "causa común", el "bien común", la "sociedad buena" o la "sociedad justa". ¿Qué significa el "bien común" si no dejar que cada uno se satisfaga a sí mismo? (p. 41)

A pesar de estos procesos de individualización y de "desarraigo" del individuo dentro de un proyecto de sociedad civil, los cuales se han manifestado en actividades determinadas como la libertad económica, de locomoción y de información, la reacción del Estado se ha manifestado en un proceso de transformación orgánica y funcional en torno a estos fenómenos. El Estado ha debido replantearse frente al advenimiento de una "modernidad liquida"[1], la cual puede ejemplificarse en las características que hasta ahora le hemos otorgado en este artículo al ciberespacio, en fenómenos relacionados con la globalización que se pueden observar en el ámbito migratorio (Navas y Montoya, 2018; Polo y

[1] La modernidad líquida se concibe, dentro de los postulados de Zygmunt Bauman, como un proceso de aceleración y de transformación etérea de las relaciones sociales y de poder existentes entre los sujetos, la tecnología y las instituciones, el cual se desarrolla en un escenario político e ideológico de posmodernidad.

Serrano, 2018; Salazar, 2016), en la transformación de las relaciones laborales (Ostau y Niño, 2017; 2018), en la incursión de debates bioéticos y perspectivas alternativas en la realidad y quehacer jurídico de los Estados (Palencia et ál., 2019; Restrepo, 2018; Torres et ál., 2018; Woolcott, 2015; Woolcott y Fonseca, 2018), en el valor y protección de las ideas en una economía de mercado (Flórez et ál., 2018; Woolcott y Flórez, 2014), en los principios que orientan los sistemas de gobierno (Ruiz-Rico y Silva, 2018), entre otros.

Ahora, particularmente, dentro del caso económico, el proceso de desmontaje de los modelos keynesianos derivó en la consolidación de un modelo neoliberal de Estado, abocado a la implementación de un modelo regulador en torno a las actividades económicas de los individuos. Sin embargo, esto también incidió en una percepción del Estado como un actor que se halla en una disyuntiva en torno a su vocación funcional: ¿ser un ente garante de las libertades individuales o corresponder a un fin esencial de su existencia mediante la defensa de la soberanía y el bien común (garantía del paquete básico de derechos)? Dicha disyuntiva también depende de una condición progresiva de predominio de la ausencia de certeza política, en la que no existen principios rectores que brinden una concepción definida y clara de los roles del Estado dentro de un mundo globalizado. De acuerdo con Pardo (2009), dichas condiciones se desprenden de la siguiente situación:

> El derecho, los poderes públicos, los juristas, siguen fascinados por una ciencia que realizó descubrimientos espectaculares y que sigue deslumbrando con sus avances, pero en la que ya no se encuentran las certezas de antaño. El derecho persiste en ir a buscar en la ciencia certidumbres, cuando lo que obtiene de ella son, como mucho, probabilidades. Se cierra así un círculo envolvente que se inicia cuando la ciencia, con sus avances, plantea incertidumbres que afectan a derechos y

> valores relevantes que ella no resuelve; son las instancias políticas o jurídicas las que han de decidir; pero éstas a su vez se remiten a la ciencia en la búsqueda de unas certezas que allí con frecuencia no encuentran, con el riesgo de que sea la tecnociencia organizada la que acabe dominando espacios de decisión con el déficit de legitimidad que de ello resulta. (p. 18)

Partiendo de lo anterior, es posible afirmar que estos procesos de interconectividad, que se han desarrollado en el marco de la globalización, generan un escenario de incertidumbre política que repercute en un aparente accionar limitado de los Estados, por la consecuente indecisión que se da ante la inconclusión de los debates de la vocación y finalidad del Estado. Inclusive, podría plantearse una pérdida de poder del Estado como consecuencia de un posible accionar soberano limitado en el ciberespacio.

Sin embargo, por otra parte, recordemos los planteamientos de Michel Foucault que dieron forma al surgimiento de la teoría de la biopolítica, la cual le otorga al Estado la condición de ser una forma de poder heredera de las prácticas del poder pastoral que ejerce vigilancia y control sobre todos los espacios de la vida ciudadana, y ata la identidad y el diario transcurrir de los sujetos a los marcos de posibilidad de acción del Estado. Frente a esta concepción del Estado, a la cual Foucault llamó en su momento la más eficiente y compleja estructura de técnicas de individualización y procedimientos de totalización en la historia de la humanidad, podríamos también preguntarnos si realmente dicha forma de poder ha perdido relevancia frente al fenómeno del internet y la consolidación del ciberespacio. Para responder este cuestionamiento, es importante que más adelante indaguemos sobre la naturaleza del poder que desarrolla Foucault.

Gobernanza global de internet: ¿soberanía limitada?

La posible pérdida de relevancia por parte del Estado en el contexto del ciberespacio podría evidenciarse en el empoderamiento de otros actores a nivel internacional, los cuales podrían poseer un margen de actuación y decisión más amplio sobre el internet. Podríamos pensar que el ejercicio de la soberanía en el ciberespacio escapa del dominio exclusivamente estatal, al observar un modelo en el que la sociedad civil y la empresa privada son los protagonistas de la *global media and comunication policy* ('política de los medios de comunicación globales'). Un escenario en el cual la discusión sobre los elementos inherentes al concepto de soberanía (territorio, seguridad y legalidad) trasciende la exclusividad estatal y se crea la gobernanza global de internet.

La Commission On Global Governance (1995) definió la gobernanza global de internet en los siguientes términos:

> La suma de las muchas maneras en que los individuos e instituciones, públicas y privadas, manejan sus asuntos comunes. Es un proceso continuo a través del cual se pueden acomodar intereses conflictivos o diversos y se pueden adoptar medidas de cooperación. Incluye instituciones y regímenes oficiales facultados para hacer cumplir la ley, así como acuerdos que las personas e instituciones han concertado o perciben que son de su interés. (p. 2) (traducción propia)

En este orden de ideas podemos definir la gobernanza global de internet como el proceso de concertación y confrontación de intereses de diversos actores internacionales, mediante el cual se moldea la forma en la que se gestiona el internet a nivel mundial. En este sentido, la principal evidencia de cómo se desarrolla la gobernanza global de internet y cuáles son sus particularidades recae en los diversos escenarios internacionales de discusión respecto al internet, los acuerdos internacionales en esta materia

y la normativa que regula el desarrollo de la red a nivel internacional (Internet Society, 2016).

Si bien esta gobernanza involucra un gran número de actores que no son exclusivamente estatales, especialmente la sociedad civil y el sector privado, el protagonismo de los Estados ha sido determinante en el desarrollo de la *global media and comunication policy* (Mansell y Raboy, 2011). Tal como sostiene Chenou (2014), los representantes estatales han sido el grupo con mayor participación con relación a los demás grupos de interés en las instancias de discusión de la gobernanza global de internet. Inclusive, siendo los Estados el grupo de interés con mayor representación en dicha gobernanza, estos no poseen necesariamente posturas convergentes respecto a la gestión del internet. Por el contrario, dados los valores particulares de cada Estado y la manera diferenciada en que cada uno percibe la forma en la que debe actuar respecto a sus funciones estatales sustantivas en este ámbito, se defienden modelos diferentes para la gobernanza de internet en escenarios internacionales.

Un claro ejemplo de estas diferencias en los modelos estatales de gobernanza en internet son las posturas contrarias que defienden Estados Unidos y China. Chenou señala que las principales divergencias entre estas dos potencias se encuentran en el terreno de la seguridad informática y la libertad de expresión. Mientras que Estados Unidos promulga una política de *internet abierto* fundamentado en la autorregulación privada de los contenidos, China defiende una postura más restrictiva respecto a los contenidos disponibles en la red y al acceso de los datos privados por parte del Estado (Chenou, 2014).

Estos dos modelos generales dan cuenta de dos lógicas estatales basadas en valores culturales diferentes. Mientras que Estados Unidos es el abanderado del desarrollo pleno de las libertades individuales y de los valores democráticos a nivel mundial (Huntington, 2015), China se

caracteriza por la cohesión social y la integración de su población dentro de un proyecto normativo en el que la población debe seguir fervientemente las directrices de su Estado para posicionarse como un actor poderoso y protagónico en el sistema internacional (Callahan, 2015).

Cada uno de estos modelos posee simpatizantes y detractores en los escenarios de discusión de la gobernanza global de internet. En términos generales, los planteamientos de Chenou (2014) nos permiten observar que los Estados han votado en dichos escenarios internacionales en dos bloques: uno a favor de un enfoque amplio respecto al desarrollo del internet y otro que sostiene una postura más restrictiva.

Este conjunto de factores, en los cuales el Estado reafirma su poderío en términos de su relación con el ciberespacio, se han evidenciado en la gobernanza global de internet. En este sentido, la idea sobre una posible pérdida de poder por parte de los Estados en el ciberespacio debe ser matizada y, por el contrario, se puede observar que estos poseen un amplio margen de acción en la gobernanza global de internet respecto a aquellos elementos que tradicionalmente se han relacionado con el concepto de soberanía.

Una nueva soberanía

Es pertinente mencionar el importante abordaje del concepto de soberanía realizado por Hans Kelsen y su razón de ser en el Estado. Según este autor, en la revisión de este concepto

> [...] las dificultades comienzan en el instante en que la reflexión va más allá del orden jurídico estatal propio, es decir, más allá de aquel dominio que se considera de ordinario como orden jurídico estatal, hallándose ante objetos que aspiran al calificativo de "Derecho" con la misma razón que el orden jurídico del Estado, sin que por eso puedan considerarse como partes consecutivas de éste. (Kelsen, 1949)

Por lo tanto, dentro de las concepciones tradicionales de la soberanía, como un elemento que depende el ejercicio del Estado para la consecución de sus intereses y la preservación de su seguridad, es necesario entender las posibles transformaciones y respuestas que se han dado a esta problemática.

Ahora bien, a pesar de que no se ha aclarado teóricamente una materialización deontológica de las responsabilidades y capacidades del Estado para dar una respuesta certera a esta problemática, el Estado ha tendido a mutar simultáneamente con la aparición de estos nuevos retos para la legalidad. Con el advenimiento de los modelos neoliberales de Estado, los cuales han focalizado sus funciones en el desarrollo de un rol regulador mínimo de las actividades de la economía, se ha superado progresivamente la estructura orgánica tradicional del Estado.

Ante las crecientes necesidades del Estado para regular las diversas actividades de los ciudadanos, la delegación hacia entidades descentralizadas que propicien una acción reguladora especializada frente a una temática determinada ha sido un elemento que ha surgido durante los últimos años, animando reflexiones sobre el ejercicio y naturaleza de estas entidades, hasta incluso ser un paso de apertura al debate sobre la trascendencia del modelo de división trifinio del poder público. No obstante, este es un debate de grandes magnitudes que no compete al presente artículo, pero es necesario para resaltar que el desarrollo de las nuevas transformaciones del Estado, ante las nuevas necesidades operativas para la vigilancia y la protección de la ciudadanía, es una temática que merece ser mencionada.

Desde estos elementos previos, las experiencias como el acceso y uso del internet para la consecución de información, la comunicación y la interacción en un amplio espectro de coyunturas y asuntos determinados pueden ser una ventana de oportunidad que determina la misma

condición de individualidad del usuario. Con el surgimiento de estos recursos y su consolidación en la vida cotidiana de la humanidad, en una primera fase jamás el hombre estuvo más cerca de un estado de libertad plena, garantizada por el acceso a grandes fuentes de información, a diversas formas de comunicación, interacción y acción dentro del medio, al punto de llegar al límite de lo aceptable y legal para la sociedad. Es el caso de la *deep web*, que es un medio de acceso a información y servicios que pueden ser ilegales, como la venta de drogas o la venta pirata de elementos protegidos por derechos de autor, pasando por el acceso a información privilegiada y venta de armas, hasta servicios de naturaleza perversa, como la experimentación humana, la pornografía infantil y la oferta de violencia física y sexual.

A pesar de la seria posibilidad de que estos delitos se desarrollen mediante las facilidades operativas de dichos medios, el accionar del Estado para su prevención, neutralización y mitigación sigue siendo insuficiente y, al mismo tiempo, condicionado por el mismo medio. A pesar de que existen mecanismos de detección de acceso y uso de estos recursos ilegales, mediante la triangulación de posición por dirección IP, el rastreo de movimientos bancarios virtuales, entre otras herramientas, sigue habiendo una relativa fractura entre el avance acelerado y progresivo de nuevos *modus operandi* desde el plano virtual y las formas de enjuiciamiento y de ejercicio de la ley en el plano real. De acuerdo con Valencia, "las nuevas tecnologías permiten el acceso a espacios globales que conectan diversos territorios, grupos e individuos, sin que los Estados tengan capacidad de controlar o regular lo que sucede dentro de sus fronteras" (2015, p. 34).

A pesar de que se han redactado y concebido diversas perspectivas, escritos y ensayos sobre este tema, es claro dilucidar que, ante la incertidumbre teórica y política para la evolución orgánica y facultativa del Estado para la respuesta oportuna ante el mencionado problema, las

tendencias temáticas para la solución de este problema se han dirigido por dos vías. La primera corresponde a una perspectiva sobre la concepción de los vacíos de las capacidades y las competencias del Estado ante la presunta libertad ilimitada de los usuarios, mediante la identificación y caracterización de estos elementos como un problema mancomunado de todos los Estados. La identificación de la naturaleza de esta condición, la cual prohíja la proliferación de un sinfín de medios para la comisión de delitos que atentan contra la posible seguridad de los ciudadanos y el Estado, tienden a estar relacionados con comportamientos del delito organizado transnacional (DOT).

Ahora bien, dentro de esta categoría se ubica la consolidación de elementos vinculantes en derecho (Acosta y León, 2018) para la creación de obligaciones que correspondan a una responsabilidad institucional para la prevención y mitigación de estos medios. Dentro de esta forma de acción, se da la creación de tratados y acuerdos internacionales con el propósito de generar una acción mancomunada ante estos potenciales flagelos, puesto que la naturaleza transnacional de la interacción cibernética puede incidir en la necesidad de cristalizar una cooperación internacional que responda de forma cohesionada y coordinada. Dicha materialización de compromisos ocurre mediante el establecimiento de un régimen internacional, el cual se define, según los principios de Stephen Krasner, como "una serie de principios implícitos y explícitos, normas, reglas y procedimientos de toma de decisión, en los cuales las expectativas de los actores convergen en un tema dado de las relaciones internacionales" (1983, p. 2), el cual busca su aplicación como obligación de los Estados bajo el principio de *pacta sunt servanda*.

De acuerdo con Valencia (2015):

> Los riesgos tecnológicos, que no respetan las fronteras de los Estados, obligan a que los Estados deban colaborar y cooperar cada vez más entre ellos para garantizar un mínimo de efectividad en la solución de los problemas globales que afectan a los ciudadanos de diversos Estados, de múltiples formas. (p. 34)

Sin embargo, no solo los mecanismos de cooperación internacional mancomunada para la detección de delitos cibernéticos y los elementos vinculantes en el marco del derecho internacional siguen siendo relativamente incipientes; también es necesario resaltar que los delitos cibernéticos pueden estar ligados a otras formas de actividades ilícitas en los ámbitos nacional e internacional, como el secuestro, la extorsión, la tortura, el asesinato, el fraude, el robo, la prostitución y trata de personas, el tráfico ilícito de migrantes, entre otros asuntos de seria importancia para la seguridad de la ciudadanía y de los Estados. Lo anterior ha conducido, por ejemplo, a pensar desde una perspectiva crítica, condicionada a las realidades regionales, los retos en materia de criminología. Sobre este asunto es pertinente revisar el caso latinoamericano tanto desde la perspectiva criminológica como desde la construcción de referentes regionales particulares para asumir los retos de un mundo globalizado y cambiante (Silva et ál., 2018).

Por otra parte, la segunda vía, a diferencia de la primera, busca el desarrollo de una estrategia a un nivel particular frente a la mencionada problemática. A pesar de que este mecanismo tiende a estar articulado a los elementos que permiten una cooperación global en la materia, el desarrollo de esta estrategia se basa en un ejercicio de vigilancia sistemática a potenciales infractores y delincuentes. Esto se ejerce mediante el principio de vigilancia de panóptico de Foucault, el cual se entiende como un sistema que "se ejerce sobre los individuos a la manera de vigilancia individual y continua, como control de castigo y recompensa

y como corrección, es decir, como método de formación y transformación de los individuos en función de ciertas formas" (Foucault, 1980, p. 117), el cual está fundamentado en tres elementos rectores: vigilancia, control y corrección. A pesar de que este es un modelo de vigilancia formado para la materialización de un proceso de ortopedia social, encaminado a la rehabilitación de sujetos que hayan infringido la ley y el orden, es posible su implementación como un medio de control anticipado a la posible comisión del delito, el cual podría implicar el control estatal de la experiencia del internauta.

Además de esta forma de vigilancia, este método también busca el establecimiento de una cultura de denuncia y control descentralizado, de la cual son parte los mismos usuarios. Esto potencia dinámicas de criminalización en el seno de la estructura social (Ariza, 2018), en la cual también intervienen los medios de comunicación como aparatos de reproducción de una ideología punitiva (Barragán y López, 2018; Velandia, 2018), que se enclava en las formas de interacción de la ciudadanía, estableciendo un sentido de la justicia y del proceso penal (Moya, 2018) frente a la construcción del fenómeno de lo delictivo. Esta estrategia toma como asidero la vigencia de principios éticos y morales como factores que permiten una operatividad de un sistema descentralizado de vigilancia ciudadana en el ciberespacio lo cual ha permitido que se inauguren debates como el relacionado con el derecho a la intimidad en este tipo de redes (Castro, 2016). Además de esto, la implementación de este elemento depende del control de contenido y el límite al acceso de información como mecanismos para fijar una frontera entre lo legal y lo ilegal.

Sin embargo, una gran limitante de esta forma de control se basa en el hecho de presunción del delito como un *fait accompli*, el cual no solamente compromete al principio de *bona fides* como garantía necesaria del derecho al debido proceso, sino también puede ser un elemento que

condicione la legitimidad de la autoridad por la comisión de actos ilegales para el cumplimiento de sus funciones. Además, este sistema de vigilancia puede incidir en una amenaza latente al principio de *habeas data* para la salvaguarda de la información personal de los usuarios, además de condicionar la libertad individual bajo los intereses y elementos que definen las perspectivas de seguridad de los Estados.

Vigilancia y control sobre la experiencia del cibernauta

Recordemos que, tal como lo hemos enunciado, el internet ha creado un nuevo territorio virtual que en principio escapa de las fronteras estatales. El ciberespacio puede ser asimilado en términos conceptuales a las aguas internacionales que escapan de la soberanía de los Estados; sin embargo, los usuarios que navegan en la red se encuentran físicamente emplazados en un territorio estatal. Esta situación genera una tensión latente que genera cuestionamientos a la soberanía de los Estados.

Respecto a esta dicotomía podemos observar que los Estados han logrado reafirmar su soberanía en el ciberespacio. Esto se ha logrado por medio de la vigilancia, el control y la regulación estatal de la experiencia cibernética del internauta como espacio de control del biopoder. Si bien el internet vuelve difusas las fronteras estatales debido a la interconexión transnacional en tiempo real, el acceso a internet depende de una infraestructura que se encuentra territorialmente localizada en los Estados. De esta forma el control del contenido al que tienen acceso los internautas se ha transformado en una forma de reafirmación de la soberanía estatal. Esto se puede evidenciar a través del desarrollo de políticas públicas estatales en diversos Estados para la regulación del contenido al que los usuarios tienen acceso en internet.

Por otra parte, la relación entre la justicia (los derechos constitucionales básicos que garantiza cada Estado de manera particular) y el internet es

observable en el contenido que se puede producir y al cual se puede acceder en la red. En términos generales existen acciones punibles que, de acuerdo con la normativa de cada Estado, en caso de ser cometidas por parte de algún ciudadano, el sistema judicial se pone en marcha para juzgar dicha conducta. En el caso de internet, el Estado reclama de igual forma su capacidad para juzgar y disciplinar a los ciudadanos que cometan acciones ilegales en el ciberespacio.

Supongamos que un ciudadano colombiano hace uso de internet para la venta de drogas, armamento militar o cualquier otro producto de la actividad delictiva. En este caso, dado que la legislación colombiana prohíbe este tipo de conductas, el internauta que transgrede la normativa estatal en internet es susceptible de ser vigilado y disciplinado por parte del Estado colombiano. Este tipo de ejemplos pueden ser rastreados en todo el mundo, como en el caso del desmantelamiento por parte de las agencias de seguridad estadounidenses de una serie de dominios en la *deep web* en los que se llevaba a cabo actividades delictivas por medio del internet (Weimann, 2016).

Ahora, la garantía del paquete de derechos constitucionales básicos que garantiza cada Estado también se hace extensiva en el ciberespacio. Derechos como, por ejemplo, la protección de la niñez (Velandia et ál., 2018) son garantizados a través del veto. Un ejemplo de esto es la prohibición de la publicación y descarga de contenidos que se encuentren relacionados con pornografía infantil, dado que en la mayoría de Estados esta es una conducta prohibida en sus marcos normativos. De esta forma, si recordamos que los Estados son construcciones sociales que actúan conforme a los valores de una población, podemos entender por qué estos buscan imponer dichos marcos normativos en un ciberespacio que, dada su naturaleza, podría escapar de su jurisdicción.

A pesar de la posibilidad de acción mediante el uso del principio de razón de Estado, como lo mencionaba Burdeau, un ejercicio de soberanía en el que se apela a dicha "característica, atribución o facultad esencial del poder del Estado que consiste en dar órdenes definitivas" (Burdeau, 1973, p. 248), sigue entablada la disyuntiva entre la garantía de derechos y libertades de la ciudadanía y la protección y la respuesta ante posibles amenazas contra la seguridad y la salvaguarda del Estado. En este sentido, la libertad individual y el control del Estado vuelven a encontrarse de manera conflictiva.

Por otra parte, recordemos los planteamientos de Michel Foucault que dieron forma al surgimiento de la teoría de la biopolítica, la cual le otorga al Estado la condición de ser una forma de poder heredera de las prácticas del poder pastoral que ejerce vigilancia y control sobre todos los espacios de la vida ciudadana y ata la identidad y el diario transcurrir de los sujetos a los marcos de posibilidad de acción del Estado. Frente a esta concepción del Estado, podríamos también preguntarnos si realmente dicha forma de poder ha perdido relevancia frente al fenómeno del internet y la consolidación del ciberespacio.

Atendiendo a este cuestionamiento, entrevemos que la extensión de las prácticas del poder pastoral al ciberespacio es la evidencia del ejercicio de control estatal que reclama la vigencia de su soberanía. Por lo tanto, con al advenimiento del ciberespacio y la alta volatibilidad y liquidez de las relaciones que allí se desarrollan, el Estado, tradicionalmente ligado a la condición burocrática weberiana, debe replantear sus mecanismos y estrategias de ortopedia política para superar dicha burocracia anquilosada y acelerar sus respuestas a la misma velocidad que el fenómeno globalizador del internet demanda.

Ahora, el control del acceso al internet y de la experiencia del internauta no es la única forma a través de la cual el Estado reafirma la vigencia de su

soberanía en el ciberespacio. Tal como lo demuestra Valderrama (2018), el internet se ha transformado en un derecho fundamental que cada vez ingresa con mayor fuerza en las agendas constitucionales, los cuales deben estar en la capacidad de proveer este servicio a sus ciudadanos. En este sentido, si recordamos las discusiones respecto al Estado desarrolladas al inicio de este artículo, su legitimidad está directamente relacionada con su capacidad de garantizar un paquete de derechos básicos a su población, por lo tanto, su relación con el fenómeno del internet también podría ser entendida como un potencial foco de legitimidad y objeto de responsabilidad social (*social accountability*), particularmente en sistemas democráticos. En este sentido, podríamos observar cómo, incluso, la forma que adquiere la relación del Estado con el fenómeno del internet podría influir en la percepción democrática que se tiene de dicho Estado. La legitimidad democrática (Agudelo y Prieto, 2018) podría verse condicionada, dentro de un modelo integral (De Los Santos et ál., 2018) no solo por el reconocimiento del internet como derecho fundamental, sino por la forma particular de control y regulación que pesa sobre este.

Esta situación guarda relación con la promesa de salvación que Foucault describe en el poder pastoral. Este poder, cuya génesis se encuentra en la institución de la Iglesia, promete a quienes siguen las reglas de juego del Estado su salvación terrenal a través de una economía de derechos. Dicha economía distribuye y asigna derechos a quienes se encuentran atados y no transgreden los márgenes de posibilidad de acción del Estado. Por el contrario, quienes rompen con dichos márgenes son objeto de una redistribución de sus derechos, frente a la cual una de las posibilidades más comunes es la privación del derecho a la libertad. En este sentido, dentro de la narrativa de la salvación de los Estados modernos, el internet es un elemento condicionado por las reglas de juego estatales, realidad a la

cual se ata a los sujetos a partir de un proceso “objetivizador naturalizado”, como derecho que es objeto de distribución (Perafán et ál., 2020).

Por otra parte, podríamos preguntarnos: ¿sobre qué tipo de contenidos los Estados han reclamado la necesidad de control y regulación? Tal como indica Chenou (2014), a lo largo de la historia de la gobernanza global de internet, algunos de los asuntos más recurrentes han sido la ciberseguridad y los derechos humanos, los cuales se han expresado en los diversos escenarios de discusión sobre el internet, tales como la World Summit on Information Society (WSIS), el Working Group on Internet Governance (WGIG), el Internet Governance Forum (IGF) y la World Congress on Information Technology (WCIT). Estos dos aspectos se relacionan de manera directa con los dominios sustanciales del Estado mencionados anteriormente (seguridad, justicia y paquete constitucional de derechos básicos).

Existen amenazas latentes en internet que han sido securitizadas por parte de los Estados. Gran parte de los Estados desarrollados y en vías de desarrollo han formulado políticas estatales de ciberseguridad y ciberdefensa debido al incremento exponencial de ataques cibernéticos a páginas gubernamentales, filtración de contenidos clasificados de seguridad y a la posible violación de protocolos que controlan la infraestructura militar (Vargas, 2014). Esta preocupación estatal por las amenazas en materia de seguridad que se originan desde internet no solo se ha evidenciado en el desarrollo de políticas estatales, sino también en el trabajo conjunto entre Estados para la formulación de políticas internacionales de ciberseguridad. Un ejemplo de esto es la elaboración del manual de ciberseguridad de la International Telecommunication Union (ITU), el manual para la ciberguerra de la OTÁN (Organización del Tratado del Atlántico Norte) y la política pública de seguridad digital

colombiana, la cual desarrollaremos como ejemplo en las siguientes páginas.

Proteger el ciberespacio colombiano para garantizar la seguridad ciudadana y la defensa nacional

La comisión de ilícitos en el ciberespacio ha tenido un crecimiento exponencial desde el año 2010, desde cuando es posible realizar análisis estadísticos sobre el comportamiento de estos delitos gracias a la adopción de nueve bienes jurídicos tutelados relacionados en el Código Penal colombiano. Si bien en casi una década de estudio sobre estos datos es posible afirmar que los casos de delitos informáticos han incrementado con el paso de los años, el 2020 es un año tan atípico como preocupante: han crecido en forma exponencial todos los delitos definidos por la Ley 1273 debido a la virtualización de la vida producto de las medidas de aislamiento (tanto obligatorio como voluntario) definidas por el Gobierno nacional y los Gobiernos territoriales para mitigar el contagio y la saturación de los sistemas de salud con ocasión de la pandemia. Solo por dar algunos ejemplos, del 25 de marzo al 8 de noviembre de 2020 (periodo covid-19), la interceptación de datos informáticos varió en un 235 % (975 casos en 2020 en comparación a 291 casos del 2019) y la suplantación de sitios web en un 377 % (3499 casos en 2020 en comparación a 733 casos del 2019) (Policía Nacional, 2020).

Los delitos informáticos son, entonces, los de mayor crecimiento en el país (incluso por encima de los delitos de alto impacto como el homicidio, el hurto y la extorción). Por esa razón demandan soluciones colectivas, intersectoriales y mancomunadas, pero, sobre todo, flexibles y vanguardistas que permitan anteceder y predecir la gran agilidad con la que los ciberdelincuentes crean mecanismos y herramientas más

sofisticadas para afectar los sistemas informáticos del Estado, las empresas y la ciudadanía.

Como se ha expuesto a lo largo de este documento, los ciberdelitos transcienden las fronteras nacionales, por lo cual requieren respuestas que emanen de la concertación entre los diversos actores del sistema internacional (estatales y no estatales). Es por este motivo que esta sección busca desarrollar algunos antecedentes elaborados desde la Unión Europea (UE) y la Organización de Estados Americanos (OEA) en materia de ciberseguridad, para después enunciar algunos elementos propios a la política pública y la normativa colombiana que dan cuenta de los avances y las capacidades del país en materia de seguridad cibernética.

Respuestas regionales a la seguridad y la defensa cibernética: los casos de la UE y la OEA

Para combatir las actividades ilegales en el espacio cibernético, la Unión Europea ha comenzado a legislar en el marco de la ciberseguridad para la ciudadanía europea. Una de las últimas actuaciones que realizó la UE en este sentido fue el desarrollo de la estrategia de ciberseguridad europea, como un marco de acciones encaminada a solventar y mejorar el espacio en la red (Medina, 2019). El documento nace respaldado por una serie de órganos, instituciones y políticas que ya están trabajando en torno a las diversas dimensiones de la seguridad desde finales de 1990 (Machín y Gazapo, 2016).

La estrategia de ciberseguridad de la UE establece los planes de esta organización para prevenir y responder a las perturbaciones y ataques que pudieran afectar a los sistemas de telecomunicaciones del viejo continente. En este contexto, la UE tiene una extraordinaria importancia no solo porque agrupa a 28 países industrializados que juegan un papel relevante en la economía digital mundial, sino que en ellos las tecnologías digitales

son fundamentales en la economía y la sociedad en su conjunto. Lo anterior también está relacionado con el nivel de amenaza al que estos países deben responder, comparados con otros actores del sistema, como los crecientes ciberataques dirigidos por grupos de delincuencia organizada internacionales que operan con un elevado nivel técnico (Wegener, 2014).

En la más reciente Directiva del Parlamento Europeo y del Consejo de la Unión Europea (UE) (6 de julio de 2016) relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión para fin de mejorar el funcionamiento del mercado interior, se definieron las siguientes prerrogativas:

> 1. Establecer obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;
>
> 2. Crear un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;
>
> 3. Crear una red de equipos de respuesta a incidentes de seguridad informática (*computer security incident response teams*, CSIRT) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;
>
> 4. Establecer requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales;
>
> 5. Establecer obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información. (Unión Europea, 2016)

Por su parte, la OEA ha trabajado para fortalecer las capacidades de seguridad cibernética entre los Estados miembros desde principios de la década de 2000. Con los años se ha convertido en un líder regional en asistencia a los países para fortalecer la capacidad técnica y de seguridad cibernética en materia de políticas que garanticen un ciberespacio seguro y resiliente. Además, la OEA promueve un especial cuidado por los derechos humanos y las posibles tensiones que pudiesen surgir frente al paradigma de la seguridad (Carvajal, 2018). En este contexto, el programa de seguridad cibernética de la OEA apoya las iniciativas sobre la base de un análisis en profundidad y en la comprensión de la magnitud de las amenazas (OEA, 2015).

En el año 2004, los Estados miembros de la OEA aprobaron la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, la cual aboga por un esfuerzo coordinado de múltiples partes interesadas en la lucha contra las amenazas cibernéticas en el hemisferio, y proporcionan un marco inicial para cultivar y guiar dicho enfoque. Los Estados miembro fueron extraordinariamente previsivos cuando adoptaron tal estrategia ya que ha mejorado la protección de la infraestructura de las tecnologías de la información y las comunicaciones (TIC), fortaleciendo la capacidad de los Gobiernos para responder y mitigar incidentes cibernéticos. Estos compromisos se han reafirmado y fortalecido con los años, a partir de la adopción de numerosas declaraciones oficiales, incluyendo la más reciente, relacionada con el papel y las responsabilidades de la OEA y sus Estados miembros en la promoción de la seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica (Medina, 2019).

Respuestas del Estado colombiano a las amenazas cibernéticas

Entender las capacidades de Colombia en ciberseguridad también amerita comprender el lugar de este país en cuanto a su madurez cibernética. De acuerdo con el Reporte de Ciberseguridad 2020 realizado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), Colombia está en una etapa consolidada, lo cual significa que "los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida" (2020, p. 42).

Entre los esfuerzos desarrollados por el Estado para mejorar su madurez cibernética, el país expidió una nueva Política Nacional de Confianza y Seguridad Nacional (CONPES 3995 de 2020), y un Comité de Seguridad Digital al interior de la Presidencia de la República. Asimismo, Colombia también cuenta con un Grupo de Respuesta a Emergencias Cibernéticas (COLCERT) en cabeza del Ministerio de Defensa Nacional. Estos avances indican que existen necesidades que están siendo cubiertas por el Estado, pero falta invertir mayor recursos (financieros y humanos) para atender efectivamente los riesgos de la masificación en el uso de nuevas TIC y la extensión de la virtualización en todos los espacios de la vida.

Por su parte, el *National Cyber Security Index* elaborado por e-Governance Academy (eGA)[2] ubica a Colombia en el puesto 60 de 161 países analizados. De acuerdo con este índice, el país tiene un 46.75 en el índice de seguridad cibernética nacional (el cual mide las capacidades

[2] Organización de consultoría y tanque de pensamiento sin ánimo de lucro construida como una iniciativa conjunta del Gobierno de Estonia, Open Society Institute y el Programa de las Naciones Unidas para el Desarrollo (PNUD). Su objetivo es crear y transferir conocimiento y buenas prácticas en el área de la transformación digital: gobierno y democracia electrónica, y ciberseguridad nacional.

implementadas por los Gobiernos), mientras que se evalúa en un 56.09 los aspectos relacionados con el cumplimiento promedio del porcentaje en el índice de desarrollo de las TIC y el índice de preparación en red. Es decir, la posición de Colombia en el mundo es similar a la que tiene en su región: existen esfuerzos normativos y en política pública, pero falta una mayor inversión en diversas capacidades para que el país pueda convertirse en un líder y referente en esta materia.

Estructura y desarrollo de la política nacional de seguridad digital, y las políticas en seguridad ciudadana y defensa nacional relacionadas con el espacio cibernético

Colombia es reconocida por la puesta en marcha de diversos planes, estrategias y políticas que conciernen a la seguridad y defensa nacional. La evolución histórica del conflicto armado en Colombia (Bernal, 2018) ha llevado a que la seguridad sea una prioridad en el ámbito gubernamental. Inclusive, con la firma de los Acuerdos de Paz con la extinta guerrilla de las FARC, la seguridad continúa en el centro de la discusión nacional (Cubides et ál., 2018). Sin embargo, algunos cambios en el panorama político colombiano, como la firma de los acuerdos anteriormente mencionados que han sido acompañados por una transformación transitoria de ciertos espectros del andamiaje institucional para su implementación (Pérez, 2018), han llevado al Estado colombiano a reconocer, priorizar y fortalecer otros aspectos de las políticas nacionales de seguridad y defensa. En este contexto, surgen nuevos retos que deben ser considerados, como el robustecimiento y reflexión sobre la pertinencia de la Política Nacional de Seguridad Digital, la Política de Defensa y Seguridad (Ministerio de Defensa Nacional, 2020) y la Política Marco de Convivencia y Seguridad Ciudadana (Ministerio de Defensa Nacional, 2019).

El nuevo documento CONPES 3995, “Política Nacional de Confianza y Seguridad Digital”, expedido en 1 de julio de 2020, tiene como

antecedentes en política pública el documento CONPES 3701, "Lineamientos de Política para Ciberseguridad y Ciberdefensa" (2011), y el documento CONPES 3854, "Política Nacional de Seguridad Nacional" (Departamento Nacional de Planeación, 2016). Ambos documentos han sido fundamentales en la construcción de lineamientos y capacidades, pero carecían de un componente realmente eficaz en la construcción de confianza digital. El CONPES 3995 busca:

> Establecer medidas para desarrolla la confianza digital a través de la mejora a la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías. (Departamento Nacional de Planeación, 2020, p. 27)

Para cumplir con este objetivo, y considerando lo relativo exclusivamente al sector defensa y seguridad, las diferentes instituciones del Estado con competencias en esta materia deberán, entre otros:

- Elaborar un diagnóstico y plan de mejoramiento continuo de capacidades operativas, administrativas, humanas científicas y de infraestructura.
- Definir lineamientos para la confirmación de una red de participación cívica digital para mejorar la interacción y cooperación frente a amenazas cibernéticas.
- Establecer un Modelo Nacional de Gestión de Incidentes para el manejo en gestión de riesgos e incidentes relacionados con la seguridad digital.
- Diseñar un registro central único de incidentes de seguridad digital a nivel nacional.

- Definir un modelo de divulgación periódica de vulnerabilidades en todos los sectores.
- Crear e implementar un sistema de intercambio de información cibernética.

En materia de políticas sectoriales vigentes, la Política de Defensa y Seguridad "para la legalidad, el emprendimiento y la equidad" (2019) contempla la "innovación, inteligencia estratégica, prospectiva e inteligencia artificial" como una de las acciones de sus líneas de política que busca dar un salto tecnológico hacia los nuevos avances de ciencia y tecnología (específicamente con el uso de inteligencia artificial y analítica de datos) para facilitar el procesamiento de la gran cantidad de información que las Fuerzas Armadas recogen y que incide en la toma de decisión estratégica, pero también en la operativización táctica de las Fuerzas Militares y de la Policía Nacional.

Sin embargo, es la Política Marco de Convivencia y Seguridad Ciudadana (Ministerio de Defensa Nacional, 2020) la que define lineamientos específicos en protección del ciberespacio, en adopción de nuevas capacidades (de una manera más específica) que protejan a los ciudadanos de aquellos factores de riesgo que atenten contra su integridad física, mental y financiera, y que son propias del espacio digital.

La primera línea relacionada es "tecnología para la convivencia y la seguridad ciudadana". Esta busca optimizar los recursos y aumentar la capacidad de control y vigilancia a través de cámaras para el reconocimiento facial que contribuyan a la persecución penal, la identificación de vehículos y placas, la protección de los derechos humanos en procedimientos policiales; el incremento de aeronaves remotamente tripuladas (RPAS), el fortalecimiento de las capacidades de análisis del Observatorio del Delito y del Centro Nacional de Análisis Criminal de la

Dirección de Investigación Criminal (DIJIN e Interpol), entre otras. La segunda se enfoca en los "ciudadanos ciberseguros", centrando su atención en tres acciones específicas: la prevención de los delitos en el ciberespacio, la persecución contra el ciberdelincuente y la articulación institucional contra el ciberdelito (Ministerio de Defensa Nacional, 2020, pp. 71-75).

Capacidades sectoriales en ciberseguridad y ciberdefensa

Para dar respuesta a las nuevas amenazas que emergen del ciberespacio, la Policía Nacional de Colombia tiene un despliegue y unas capacidades desarrolladas en materia de investigación criminal e inteligencia policial para perseguir, anticipar y atender los requerimientos ciudadanos relativos a los delitos que ocurren en el espacio cibernético. Desde el 2001, en coordinación con la Fiscalía General de la Nación, se creó el Grupo Investigativo de Delitos Informáticos que posteriormente se convirtió en el Grupo de Investigaciones Tecnológicas. Sin embargo, no es hasta el 2010, con ocasión de la Ley 1273 del 2009, que se crea un equipo especializado administrativo para la protección de datos e información. Un año más tarde, en el 2011, por orden del CONPES 3701 de 2001, se crea el Comando Conjunto Cibernético, el Grupo de Respuestas de Emergencia Cibernética Nacional y el Centro Cibernético Policial, el cual acoge el CAI Virtual.

La Policía Nacional de Colombia actualmente cuenta con un Centro de Capacidades para la Ciberseguridad (C4), y una Estrategia contra los Delitos Informáticos que en el 2018 fue transformada en la Estrategia Integral de Ciberseguridad (ESCIB). Todos estos elementos buscan contrarrestar fenómenos que atentan contra la ciberseguridad; fortalecer la economía digital y el comercio electrónico; proteger a la población especialmente vulnerable a delitos en el espacio cibernético como niños, niñas y adolescentes; prevenir y anticipar amenazas que devengan de espacios digitales; mejorar la educación y la capacitación en temas

cibernéticos; fortalecer alianzas nacionales e internacionales para la mejora de las capacidades, entre muchos otros.

Frente al caso específico a la ciberdefensa, cabe señalar que

> [...] los Estados la organizan mediante el establecimiento de una estrategia nacional de seguridad. De acuerdo con las amenazas y los consiguientes riesgos, se planean y definen unas estrategias de defensa desde los diferentes espacios estratégicos que dan lugar sus distintas facetas, como la defensa territorial, la defensa aérea, la defensa de las fronteras, la defensa económica y, en el dominio del ciberespacio, una ciberdefensa que garantice la ciberseguridad. (Feliu, 2013, p. 2).

En este contexto,

> [...] la ciberdefensa es entendida como el conjunto de acciones u operaciones activas o pasivas desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos y teleinformáticos de la defensa a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que fuerzas enemigas los utilicen para cumplir los suyos. Se ha planteado iniciar el proceso de la ciberdefensa por la inteligencia informática, con el ciberespacio como ambiente, para obtener los elementos descriptores que conformen la identificación de los escenarios y, a la vez, parametrizar las amenazas para dimensionar los riesgos y así posibilitar el diseño de los instrumentos de defensa. (Becerra et ál., p. 92)

A partir de lo anterior, la ciberdefensa ejerce la defensa activa y pasiva del centro de operaciones, de los medios de información que posee la institución con el fin de repeler los ataques cibernéticos que sufra, al cual su arma rectora, por disposición, son las comunicaciones militares, y apoya la protección cibernética de la infraestructura crítica del país (Carreño et ál., 2020). Se trata de una estrategia determinada de adquirir una capacidad de defensa del ciberespacio, combinando la protección

interior de los sistemas, la vigilancia permanente de redes sensibles y la respuesta rápida en caso de ataque, contrarrestando las amenazas ciberespaciales y garantizando acceso al ciberespacio. Además, es la estrategia para la protección de los activos relacionados con los sistemas de información a través de controles de detección, corrección y disuasión que contrarresten las posibles amenazas (Ejército Nacional de Colombia, 2015).

El Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) define su misión como

> [...] la coordinación de la ciberseguridad y ciberdefensa nacional, la cual está enmarcada dentro del proceso misional de gestión de la seguridad y defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. (2013)

Además, mediante el Sistema de Información del Centro de Operaciones del Ejército Nacional (SICOE) las unidades operativas mayores y menores reportan todos y cada uno de los eventos y situaciones operacionales que se presentan en todo el territorio nacional. Su objetivo primordial es promover la información en el momento requerido, permitiendo realizar análisis cuantitativos y cualitativos de cualquier situación operacional, bajo los niveles de seguridad que garanticen la integridad y la reserva de la información (Medina, 2019). Por otra parte, el Sistema de Información Geográfica del Ejército (SIGE) es una herramienta para la captura, almacenamiento, manipulación, análisis, modelación y presentación de datos militares referenciados que se apoya en información cartográfica y herramientas necesarias para el planeamiento y seguimiento de operaciones militares. El SIGE es una herramienta de análisis espacial que

brinda información geográfica detallada para facilitar el proceso militar en todas las decisiones (Fuerzas Militares de Colombia, 2017), el cual es dirigido desde el Comando Conjunto Cibernético (CCOC).

Conclusiones

Lo que en principio surgió como una iniciativa en gran medida privada que sentó las bases de la creación de un nuevo espacio virtual, el ciberespacio, rápidamente fue reclamado por parte de los Estados como un espacio susceptible de ejercicio de su soberanía. El recorrido que hasta ahora hemos desarrollado nos ha permitido evidenciar el rol determinante de los Estados en la gobernanza global de internet.

Si bien los Estados no son el único actor en la gobernanza global de internet, juegan un papel fundamental en términos de control y regulación, debido a que el internet involucra asuntos sustantivos del quehacer estatal, como la seguridad, la legalidad y los derechos constitucionales básicos. En este sentido, el Estado hace extensivos estos elementos en el ciberespacio, justifica su accionar en internet con base en las amenazas latentes a su seguridad y reafirma su soberanía en el ciberespacio.

Lo anterior se puede evidenciar en el desarrollo de políticas estatales que condicionan la experiencia del internauta al marco normativo del Estado, el cual emana de una construcción social basada en los valores particulares de cada sociedad. El desarrollo de técnicas y estrategias de control y vigilancia de la experiencia del internauta por parte del Estado es la forma a través de la cual el ejercicio de la soberanía estatal ha mutado. De igual forma, estas formas de vigilancia y control son discutidas en los escenarios internacionales en donde se construye la gobernanza global de internet.

Dichas posturas son defendidas y debatidas en estos escenarios por parte de los Estados que poseen la mayor proporción de representatividad respecto a los demás grupos de interés en la gobernanza global de internet. Entre estas posiciones encontramos dos modelos característicos que acaparan gran parte de la discusión respecto a dicha gobernanza, uno amplio, promulgado por parte de Estados Unidos, y uno restrictivo por parte de China.

A pesar de estas condiciones que han posibilitado un desarrollo sistemático de un ordenamiento paradigmático a nivel institucional, funcional e instrumental, el debate sigue vigente. Es de imperiosa necesidad que todos los sectores de la sociedad y de la comunidad internacional comprendan la magnitud de esta problemática como una ventana de oportunidad para contribuir al debate y al hallazgo de soluciones para garantizar un acceso más seguro e íntegro a estos medios que, a pesar de las amenazas anteriormente mencionadas, siguen siendo un medio comunicación e información sin parangón.

Finalmente, si bien los avances que tiene el país en materia normativa y en desarrollo de capacidades para proteger a la población y al Estado de amenazas cibernéticas es significativo, es importante reconocer que hay algunos retos que persisten y que, con el paso del tiempo, parecen aumentar. Entre estos desafíos sobresalen la necesidad de medir la percepción de seguridad de los ciudadanos en materia de seguridad cibernética; fortalecer la gestión de riesgos enfocada en las personas, los procesos y las tecnologías; la relación que existe entre las amenazas cibernéticas con el mundo tangible, por ejemplo: la captación mujeres, y de niños, niñas y adolescentes con fines de tráfico y explotación sexual a través de redes sociales; los mecanismos de prevención del sabotaje a través de sistemas informáticos necesarios en comicios democráticos; las alianzas público-privadas que puedan mejorar la capacidad de las

empresas y del Estado en estrategias anticipativas y de mitigación frente a riesgos cibernéticos; la necesidad difundir más datos abiertos para que académicos y tomadores de decisión puedan generar documentos científicos y políticas públicas basadas en evidencia; la relación que existe entre las criptomonedas, la *dark web*, y el lavado de activos que provienen de economías ilícitas, entre otros.

Referencias

Acosta, E. y León, J. E. (2018). Una mirada al derecho internacional desde H. L. A. Hart. *Utopía y Praxis Latinoamericana*, *23*(1), 50-57.

Agudelo, O. A. y Prieto, C. H. (2018). A vueltas con la legitimidad democrática. El caso de la explotación minera. *Utopía y Praxis Latinoamericana*, 23 (Extra 2), 26-36. https://doi.org/10.5281/zenodo.1798342

Ariza, R. A. (2018). Los feos, los sucios, los malos: criminalización surrealista de los acontecimientos urbanos. *Utopía y Praxis Latinoamericana*, 23(1), 170-178.

Banco Interamericano de Desarrollo y Organización De Estados Americanos. (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barragán, P. A. y López, A. L. (2018). Las decisiones judiciales: un dilema entre la legitimidad y la influencia de los medios de comunicación. *Novum Jus*, *12*(2), 189-200.

Bauman, Z. (2015). *Modernidad líquida***.** Fondo de Cultura Económica.

Becerra, J., Cotino-Hueso, L., León, I. P., Sánchez-Acevedo, M. E., Torres-Ávila, J. y Velandia-Vega, J. (2018). *Derecho y big data*. Editorial Universidad Católica de Colombia.

Bernal, C. A. (2018). Mutaciones de la criminalidad colombiana en la era del posconflicto. *Utopía y Praxis Latinoamericana*, *23*(1), 80-95.

Blanco, C. (2013). Aproximación a la noción de soberanía estatal en el marco del proceso andino de integración. *Revista Republicana*, *15*, 91-103.

Bobbio, N. (1989). *Estado, gobierno y sociedad: por una teoría general de la política*. Fondo de Cultura Económica.

Burdeau, G. (1973). *Traité de science politique*, tomo II. Librairie Generale de Droit et de Jurisprudence.

Burgos, G. (2018). El Estado moderno en cuanto "abstracción armada". Algunas reflexiones. *Revista Republicana*, 24, 105-126.

Caldera, J. 2018. La democracia como derecho fundamental: ideas sobre un modelo de democracia integral. *Opción*, *34*(87), 584-624.

Callahan, W. (2015). Identity and Security in China: the negative soft power of the China dream. *Politics, 35*(3-4), 216-229.

Carreño, D. y Sánchez, M. (2018). La asunción del Hiper-Estado. *Utopía y Praxis Latinoamericana*, *23*(2), 38-48.

Carreño, D., Restrepo, J. y Martínez, J. (2020). El ver: fundamento teórico del sistema modular. En D. Carreño (ed.), *Aplicación del método del ver, juzgar y actuar al fundamento teórico y a la práctica del sistema* (pp. 10-64). Editorial USTA.

Carvajal, J. E. (2018). El paradigma de la seguridad y las tensiones con los derechos humanos. *Utopía y Praxis Latinoamericana*, *23*(1), 97-110.

Castro, M. A. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. *Novum Jus*, *10*(1), 113-133.

Chenou, J. M. (2014). *Global internet policy: a fifteen-year long debate*. Springer

Commission On Global Governance. (1995). *Our global neighbourhood: The report of the commission on global governance*. Oxford University Press,

Consejo Argentino para las Relaciones Internacionales. (2013). *Ciberdefensa-ciberseguridad riesgos y amenazas*. http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Cubides, J., Caldera, J. y Ramírez, E. (2018). La implementación del Acuerdo de Paz y la seguridad en Colombia en el posconflicto. *Utopía y Praxis Latinoamericana*, *23*(2), 178-193.

De Los Santos, I., Ávila, F. y Caldera, J. E. (2018). La forja del Estado democrático constitucional en Venezuela y su relación con la democracia integral. *Utopía y Praxis Latinoamericana*, *23*(2), 75-97.

Departamento Nacional de Planeación. (2011). Documento CONPES 3701.

Departamento Nacional de Planeación. (2016). Documento CONPES 3854.

Departamento Nacional de Planeación. (2020). Documento CONPES 3995. https://colaboracion.dnp. gov.co/CDT/Conpes/Económicos/3995.pdf

Ejército Nacional de Colombia. (2015). *Procedimiento comunicaciones operacionales y Ciberdefensa*. https://www.ejercito.mil.co/?idcategoria=357574&download=Y

European Union Institute For Security Studies (EISS). (2016). *Discurso inaugural del alto representante de la Unión*. http://www.iss.europa.eu/uploads/media/speech4.pdf

Feliu, L. (2013). *Aproximación conceptual: ciberseguridad y ciberdefensa*. Escuela Superior de Ingenieros de Telecomunicaciones

Flórez, G., Salazar, S. y Acevedo, C. (2018). De la indiferencia pública a la protección de los autores e intérpretes de las producciones de cine en Colombia, a propósito de la ley Pepe Sánchez de 2017. *Vniversitas, 67*(136), 57-79.

Foucault, M. (1980). *La verdad y las formas jurídicas*. Gedisa.

Galán, A. R. (2017). Entre justicia y moralidad: criterios metateóricos en cuanto a la justicia la moral y el derecho. *Novum Jus*, *10*(2), 103-118.

Gallego, J. (2014). Paradoja y complejidad de los derechos humanos en la sociedad moderna. Sentido y comunicación. *Revista IUSTA*, *40*, 143-165.

Grupo de Respuesta a Emergencias Cibernéticas de Colombia. (2013). Grupo de respuesta a emergencias cibernéticas de Colombia. http://www.colcert.gov.co/

Hobbes, T. (2009). *Leviatán*. Alianza.

Huntington, S. (2015). *Choque de civilizaciones*. Paidós.

Instituto Español de Estudios Estratégicos. (2012). *Ciberespacio: nuevo escenario de confrontación*. https://dialnet.unirioja.es/servlet/libro?codigo=547632

International Telecommunication Union. (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad - Participación estratégica en la ciberseguridad*.

Internet Society. (2016). *Informe de políticas: gobernanza de internet*. http://www.internetsociety.org/es/policybriefs/internetgovernance

Kelsen, H. (1949). *Teoría general del derecho y del Estado*. Imprenta Universitaria.

Koerner, A. y Perafán, E. A. (2020). Direito social e tecnologías digitais. *Via Inveniendi et Iudicandi*, *15*(2), 249-276. https://doi.org/10.15332/625

Kosutic, J. (1949). *Ciberseguridad en 9 pasos: el manual sobre seguridad de la información para el gerente*. EPPS Services.

Krasner, S. (1983). *International regimes*. Cornell University Press.

Laidi, Z. (1998). *A world without meaning*. Routledge.

Machín, N. y Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*, *42*, 47-68.

Mansell, R. y Raboy, M. (eds.). (2011). *The handbook of global media and communication policy*. Wiley Blackwell.

Maquiavelo, N. (2010). *El príncipe*. Alianza.

Medina, G. E. (ed.). (2019). *La seguridad en el ciberespacio: un desafío para Colombia*. Escuela Superior de Guerra.

Ministerio de Defensa Nacional. (2019). *Política de defensa y seguridad para el emprendimiento, la legalidad y la equidad*.

Ministerio de Defensa Nacional. (2020). *Política marco de convivencia y seguridad ciudadana*.

Moya, M. F. (2018). Sentido de justicia y proceso penal. *Utopía y Praxis Latinoamericana*, *23*(1), 50-63.

Navas, F. y Montoya, S. (2018). The need of having an intercultural approach, in the welcome mechanisms of migrants and refugees in Bogotá. Policy review, learning from others, making proposals. *Utopía y Praxis Latinoamericana*, *23*(2), 114-126.

Observatorio de la Ciberseguridad en América Latina y El Caribe. (2016). *Ciberseguridad Estamos preparados en América Latina y el Caribe*. https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx

Oppenheimer, F. (2014). *El Estado: su historia y evolución desde un punto de vista sociológico*. Unión Editorial.

Organización de los Estados Americanos. (2004). Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética.

Organización de los Estados Americanos. (2015). Iniciativa de seguridad cibernética de la OEA. Foro global sobre experticia cibernética (GFCE). https://www.sites.oas.org/cyber/ES/Paginas/Documents.aspx

Organización del Tratado del Atlántico Norte. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN.

Ostau, F. R. y Niño, L. A. (2016). Incidencia del derecho internacional del mundo del trabajo en el marco de los derechos humanos en Colombia. *Revista Republicana*, 20, 65-96.

Ostau, F. R. y Niño, L. A. (2017). La filosofía del mundo del trabajo en el siglo XXI. *Revista Republicana*, 22, 21-46.

Palencia, E. A., León, M. V., Ávila, F. M. y Carvajal, P. M. (2019). El precedente judicial: herramienta eficaz para jueces administrativos del Distrito de Barranquilla. *Opción*, *35*(89-2), 396-434.

Pardo, J. (2009). *El desconcierto del Leviatán: Política y derecho ante las incertidumbres de la ciencia*. Marcial Pons.

Perafán, E. A., Polo, S. y Caro, J. L. (2020). ¿Mirror box: ¿una reivindicación estética sobre el capital erótico de la mujer? *Revista Latinoamericana de Sociología Jurídica*, *1*(1), 183-206.

Peralta, R. (1999). Soberanía nacional y Estado constitucional. *Revista de Estudios Políticos*, 105, 309-334.

Pérez, B. (2018). Construcción de paz en el orden del derecho transnacional penal: el caso colombiano. *Utopía y Praxis Latinoamericana*, *23*(1), 65-78.

Policía Nacional. (2020*). Balance cibercrimen 2020*. https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

Polo, S. y Serrano, E. (2018). Nueva república, nuevo horizonte, nuevo porvenir: las migraciones colombianas hacia Chile, 1990-2016. *Novum Jus*, *12*(1), 165-188. https://doi.org/10.14718/NovumJus.2017.12.1.7

Ramírez, A. H. y Noguera, D. L. (2017). Garantía de los derechos constitucionales de los pueblos indígenas en el multinacionalismo y el neoconstitucionalismo. *Novum Jus*, *11*(2), 19-51.

Restrepo, J. (2018). Feminizar a los hombres para prevenir la criminalidad. *Utopía y Praxis Latinoamericana*, *23*(1), 112-129.

Rodríguez, A (2020). Nuevos derechos, derechos emergentes: entre rupturas y continuidades. En M. C. Ballesteros y A. M. Jiménez, (eds.), *Derechos humanos emergentes y justicia constitucional* (pp. 11-39). Ediciones USTA.

Ruiz-Rico, G. y Silva, G. (2018). Tendencias y problemas actuales del sistema parlamentario en España. *Utopía y Praxis Latinoamericana*, *23*(2), 195-209.

Saidiza, H. y Carvajal, J. (2016). Crisis del Estado de derecho en Colombia: un análisis desde la perspectiva de la legislación penal. *Revista IUSTA*, *44*(1), 17-39.

Salazar, M. A. (2016). Incidencia de las normas internacionales para la protección de los trabajadores migrantes irregulares en Colombia. *Novum Jus*, *10*(2), 89-101.

Schwartz, G. (2019). Donde derecho y política se acoplan estructuralmente: las constituciones. *Novum Jus*, *13*(2), 17-37.

Silva, G. y Pérez, B. (2019). Nuevas estrategias de construcción de la realidad del delito en el orden de las sociedades en red. *Utopía y Praxis Latinoamericana*, *24*(2), 124-133.

Silva, G., Vizcaíno, A. y Ruiz-Rico, G. (2018). El objeto de estudio de la criminología y su papel en las sociedades latinoamericanas. *Utopía y Praxis Latinoamericana*, *23*(1), 11-31.

Soengas-Pérez, X. (2013). El papel de internet y de las redes sociales en las revueltas árabes: una alternativa a la censura de la prensa oficial. *Revista Comunicar*, *21*(41), 147-155.

Torres, H., Tirado, M. y Trujillo, S. (2018). El funcionalismo radical penal a partir de la bioética. *Revista Republicana*, 25, 179-198.

Unión Europea. (2016). Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148

Valencia, D. (2015). *El Estado en la era de la globalización y las nuevas tecnologías*. Ibáñez.

Valderrama, D. E. (2018). El acceso a internet como derecho fundamental: caso costarricense y su viabilidad en Colombia. *Novum Jus*, *12*(2), 165-185.

Vargas, M. (2014). *Ciberseguridad y ciberdefensa: ¿Qué implicaciones tienen para seguridad nacional*? Editorial Universidad Militar Nueva Granada.

Velandia, R. (2018). Medios de comunicación y su influencia en la punitividad de la política penal colombiana. *Utopía y Praxis Latinoamericana*, 23(1), 146-168.

Velandia, R., Tirado, M. y Gómez, A. (2018). Cadena perpetua y predicción del comportamiento. un análisis sobre la delincuencia en contra de menores de edad y la política penal en Colombia. *Revista Republicana*, 25, 241-263.

Weber, M. (1964). *Economía y sociedad*. Fondo de Cultura Económica.

Wegener, H. (2014). Ciberseguridad en la Unión Europea. Instituto Español de Estudios Estratégicos. http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO77bis-2014_CiberseguridadProteccionInformacion_H.Wegener.pdf

Weimann, G. (2016). *Going darker? The challenge of dark net terrorism*. *Studies in Conflict & Terrorism*, *39,* 195-206. The Woodrow Wilson Center.

Wendt, A. (2003). *Social theory of international relations*. Cambridge University Press.

Woolcott, O. (2015). La indemnización de las víctimas de riesgos médicos allende los límites tradicionales de la responsabilidad civil. *Revista Criminalidad*, *57*(1), 61-74.

Woolcott, O. y Flórez, G. (2014). El régimen de exención de responsabilidad de los ISP por infracciones de propiedad intelectual en el TLC Colombia Estados Unidos: Una explicación a partir de la DMCA y la DCE. *Vniversitas, 63*(129), 385-416.

Woolcott, O. y Fonseca, P. (2018). Los medicamentos y la información: implicaciones para la imputación de la responsabilidad civil por riesgo de desarrollo en Colombia. *Revista Criminalidad*, *60*(1), 79-93.