Capítulo IV

Jaime Cubides-Cárdenas
Juan González Agudelo
Leonardo Paéz Nova

El ciberespacio. Un escenario de derechos digitales como derechos humanos y la relación con la fuerza pública

Introducción

La presente investigación tiene por objeto demostrar que a través del ejercicio de las nuevas tecnologías también se encuentren presentes diversas prerrogativas de índole cardinal, que deben ser motivo de respeto y reconocimiento por parte de los Estados, al momento de asumir su compromiso de protección efectiva de los derechos. Ese escenario tecnológico reconocido como derecho humano (DDHH), propicio para armonizar y ejercer dichas libertades fundamentales, se denomina *ciberespacio*. En él los Estados deben propender por su amparo para que las sociedades evolucionen y profundicen en el ámbito tecnológico; así como en las demás competencias bajo los parámetros del respeto, adecuado acceso y libre ejercicio de la información en dicho ámbito, sin irrumpir en los DDHH.

Uno de los factores reales de poder encargado de brindar dicha protección en el *ciberespacio* dentro de un Estado es la fuerza pública. Pero ¿cómo se puede llegar a ese postulado? Como momento coyuntural de la historia que es producto de revolución de las convencionalidades, durante la era de la globalización se plantea dentro del ciberespacio la creación de innumerables redes de telecomunicaciones para generar una intensa innovación social y cultural (Giddens, 2000).

Debido a esa dinámica constante el hombre se mantiene en permanente búsqueda de nuevas alternativas para que prosiga en su evolución, permitiendo desenvolverse ante mejores escenarios. Allí donde imperen los medios tecnológicos que promuevan el acceso al *ciberespacio* y susciten la difusión de la información; máxime que nos encontramos en coyuntura de cambio. Tal como lo enunció el profesor Bauman (2008): "Olvidar por completo y con rapidez la información obsoleta y las costumbres añejas puede ser más importante para el éxito futuro que memorizar jugadas pasadas y construir estrategias basadas en un aprendizaje previo" (p. 8).

Como respuesta a esa mutabilidad se ha reconocido la existencia de un catálogo de derechos y libertades fundamentales que deben ser objeto de promoción, respeto y garantía por parte de los Altas Partes Contratantes, consignados de forma expresa en algunos tratados internacionales de DDHH. Allí dichos Estados se ven compelidos a brindar un adecuado acceso y ejercicio de la información en el ámbito del ciberespacio.

En virtud del esbozo anteriormente planteado surge una inquietud de actualidad que de forma progresiva se hace más visible y el ente colectivo exige absolver: ¿Es también la fuerza pública la encargada de brindar efectiva protección en el ciberespacio, escenario propicio para la adecuada interacción y ejercicio de los DDHH?

La metodología utilizada es la cualitativa; el desarrollo capitular fue orientado por preguntas para comprender de forma didáctica los hallazgos de la investigación. Por consiguiente, se hace un análisis sistemático de la normatividad internacional y de las investigaciones relacionadas con el objeto de estudio. En ese sentido, se busca dar una comprensión amplia desde lo descriptivo deductivo, desde un diseño metodológico y análisis crítico propositivo.

¿Cuáles son los instrumentos internacionales de protección del ciberespacio, escenario catalogado como un derecho humano?

Dentro de este escenario se destacan los siguientes instrumentos del concierto internacional que van a otorgar la respectiva protección frente al acceso del ciberespacio; así como a otros bienes jurídicos objeto de difusión y desarrollo cultural, los cuales se enuncian de la siguiente manera.

En primer lugar, en la *Declaración Universal de los Derechos Humanos* (10 de diciembre de 1948), en su Preámbulo reconoce que el desconocimiento y menosprecio de los DDHH puede llegar a originar actos de barbarie ultrajantes para la conciencia de la humanidad. Allí los Estados miembros deben promover la aplicabilidad de medidas progresivas para garantizar su ejercicio.

Igualmente, se consagra de manera puntual y expresa la existencia de un catálogo de derechos que son objeto de promoción, reconocimiento y respeto por parte de las Altas Partes Contratantes, especialmente en los Preceptos 19[1] y 27 del mentado tratado internacional. Son entendidos como la protección de la *libertad de opinión* y de *expresión* a través de cualquier medio, sin que haya discriminación por motivos de raza, sexo, idiosincrasia y religión; al igual que las producciones científicas, literarias

[1] La Declaración Universal de los Derechos Humanos adoptada por la Asamblea General de las Naciones Unidas mediante la Resolución 217 de 1948, en su Artículo 19, dice a tenor literal que, "(…) Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

o artísticas que sean resultado de los intereses morales y materiales elaborados por las propias personas[2] (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2002).

En segundo lugar, el *Pacto Internacional de Derechos Civiles y Políticos* (16 de diciembre de 1966), especialmente en el Artículo 27 identifica y promueve la estimulación del plurilingüismo y reconoce la existencia de minorías étnicas, religiosas o lingüísticas[3]. (Asamblea General de las Naciones Unidas, Pacto Internacional de Derechos Civiles y Políticos, 1966).

A partir de este instrumento internacional se pretende reconocer el derecho que tienen los pueblos del ejercicio de libre determinación, y a no ser objeto de discriminación. También el derecho que tienen los individuos que pertenezcan a las minorías, donde su accionar dentro de una entidad política sea el de difundir su cultura, su idioma, su idiosincrasia y su lengua –o dialecto, su religión, en el que se les permita el acceso y disfrute de estos escenarios culturales con su participación (Barrena, 2012, p. 82)–.

En tercer lugar, el *Pacto Internacional de Derechos Económicos, Sociales y Culturales* (16 de diciembre de 1966) reconoce el ejercicio y goce de los derechos culturales en igualdad de condiciones entre hombres y mujeres, tal como lo consagra su Artículo 3[4]. De igual manera, en el ordinal 1º del Precepto 15 aduce que todas las personas tienen derecho a participar de la vida cultural, a gozar de los beneficios del progreso científico y de sus aplicaciones; así como de la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas,

[2] El Artículo 27 de la Declaración Universal de los Derechos Humanos, en su literalidad enuncia lo siguiente: "1. Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten. 2. Toda persona tiene derecho a la protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autora".

[3] El Pacto Internacional de Derechos Civiles Políticos (PIDCP), adoptado por la Asamblea General de las Naciones Unidas mediante la Resolución 2200A (XXI), en su Artículo 27, enuncia lo siguiente: "En los Estados en que existan minorías étnicas, religiosas o lingüísticas, no se negará a las personas que pertenezcan a dichas minorías el derecho que les corresponde, en común con los demás miembros de su grupo, a *tener su propia vida cultural* [Énfasis agregado], a profesar y practicar su propia religión y a emplear su propio idioma".

[4] El Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC), adoptado por la Asamblea General de las Naciones Unidas mediante la Resolución 2200 A (XXI), en su Precepto 3º, a tenor literal enuncia lo siguiente, "(…) Los Estados Parte en el presente Pacto se comprometen a asegurar a los hombres y a las mujeres igual título a gozar de todos los derechos económicos, sociales y culturales enunciados en el presente Pacto".

literarias o artísticas de que sea autora[5]. (Asamblea General de las Naciones Unidas, 1966).

En cuarto lugar, la *Declaración sobre los derechos de las personas pertenecientes a minorías nacionales o étnicas, religiosas y lingüísticas* (18 de diciembre 1992) busca promover la protección de los individuos que hagan parte de grupos poblacionales que tengan la condición étnica o ancestral, lingüística o religiosa, o que hagan parte de minorías poblacionales. Donde se reconozca y se respete la identidad, la idiosincrasia y la cultura de dichos pueblos; además de permitir la participación efectiva en las decisiones adoptadas para preservar su tradición sin discriminación alguna. Es decir, el reconocimiento de la existencia de minorías y de grupos poblacionales que buscan mantener en el tiempo el ejercicio de sus tradiciones como expresión de cultura y plurilingüismo[6] *(Asamblea General de las Naciones Unidas, 1992).*

En quinto lugar, la *Declaración del Milenio* (13 de septiembre de 2000) promueve el respeto por los principios: de la dignidad humana; de la igualdad y la equidad; el derecho a la libre determinación de los pueblos frente a la dominación colonial y la ocupación extranjera; a la no injerencia en los asuntos internos de los Estados; al reconocimiento de los derechos y libertades fundamentales; la igualdad en su ejercicio sin distinción por motivo de raza, sexo, idioma o religión; así como a la promoción de la cooperación internacional para resolver los problemas de carácter económico, social, cultural o humanitario.

Asimismo, la solidaridad, la justicia, la tolerancia, el respeto por la naturaleza y la responsabilidad común son vistos como valores fundamentales para las relaciones en el siglo XXI, bienes preciados para la humanidad. Igualmente, con esta declaración se busca promover la paz, la seguridad y el desarme, para concientizar la liberación de los pueblos de la guerra, el respeto por el derecho internacional humanitario (DIH) y el derecho internacional de los DDHH. A su vez, promover el *derecho al desarrollo* con miras a erradicar la pobreza extrema en las poblaciones,

[5] Además, en sus ordinales 2º al 4º del Artículo 15 del PIDESC, manifiesta lo siguiente: "(…) 2º. Entre las medidas que los Estados Parte en el presente Pacto deberán aportar para asegurar el pleno ejercicio de este derecho, figurarán las necesarias para la conservación, el desarrollo y la difusión de la ciencia y de la cultura. 3º. Los Estados Parte en el presente Pacto se comprometen a respetar la indispensable libertad para la investigación científica y para la actividad creadora. 4º. Los Estados Parte en el presente Pacto reconocen los beneficios que derivan del fomento y desarrollo de la cooperación y de las relaciones internacionales en cuestiones científicas y culturales".

[6] Este instrumento internacional fue adoptado por la Asamblea General de las Naciones Unidas mediante Resolución 47/135 de 1992.

brindando una protección a su entorno común, especialmente para satisfacer las necesidades de las minorías[7], como mandato de democracia y buen gobierno[8] (Asamblea General de las Naciones Unidas, 2000).

Con esta declaración se pretendió que las Altas Partes Contratantes ejecutarán ocho grandes objetivos que pueden ser motivo de avance y desarrollo, como es el caso de: 1) Erradicar el hambre y la pobreza extrema; 2) Lograr la matriculación primaria universal; 3) Promover la igualdad de los géneros y potencia a la mujer; 4) Reducir las tasas de mortalidad infantil; 5) Reducir las tasas de mortalidad materna; 6) Luchar contra el VIH/SIDA, el paludismo y otras enfermedades; 7) Garantizar la sostenibilidad del medioambiente y 8) Fomentar una asociación mundial en pro del desarrollo (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2003).

En sexto lugar, la *Declaración sobre la promoción y el uso del plurilingüismo, y el acceso universal al ciberespacio* (15 de octubre de 2003) puso en conocimiento la existencia de un escenario denominado *ciberespacio.* Allí existen unos derechos que ostentan todas las personas que deseen acceder y participar en la difusión de la cultura; en la circulación de las ideas a través de la palabra y de la imagen; en la promoción del plurilingüismo facilitando el acceso a la información que fluye en el ámbito cibernético y las redes; en la adquisición de las nuevas tecnologías en pro de quienes no puedan tener acceso en materia de la información. Por último, en que se reduzcan los obstáculos lingüísticos fomentando los intercambios humanos en internet para la promoción de la creación y el tratamiento de contenidos educativos, culturales y científicos de forma digital, así como su acceso.

Otros derechos de las personas que acceden y participan en la difusión de la cultura serían: la creación de capacidades de contenidos de origen local e indígena en internet; la generación de productos electrónicos

[7] Tal como lo denota la *Declaración del Milenio* mediante Resolución A/52/L.2, la cual fue aprobada por la Asamblea General de las Naciones Unidas en fecha 13 de septiembre de 2000, durante su quincuagésimo quinto periodo de sesiones, el cual en el tercer ítem del acápite 25 se define: "(…) 25. Decidimos, por tanto: Aumentar en todos nuestros países la capacidad de aplicar los principios y las prácticas de la democracia y del respeto de los derechos humanos, incluidos los derechos de las minorías" (p. 7).

[8] En el séptimo ítem del apartado 30 de la mentada declaración se menciona: "(…) 30. Decidimos, por consiguiente: - Instar a la Secretaría a que, de conformidad con normas y procedimientos claros acordados por la Asamblea General, aproveche al máximo esos recursos en interés de todos los Estados Miembros, aplicando las mejores prácticas y tecnologías de gestión disponibles y prestando una atención especial a las tareas que reflejan prioridades convenidas en los Estados Miembros" (p. 9).

sobre la enseñanza de idiomas y la facilidad de acceso libre y gratuito para mejorar las actitudes del capital humano en este ámbito; la elaboración de estrategias y modelos en materia de información para facilitar el acceso de las comunidades y llegar a todos los sectores de la sociedad fomentando la cooperación internacional mediante la interconexión entre puntos nacionales de intercambio directo de tráfico (*peering points*) de los países en desarrollo y los países industrializados. Por último, la garantía de soluciones de acceso libre de acuerdo con normas técnicas y metodológicas de intercambio, sin discriminación alguna de tipo geográfico, económico, social o cultural[9], entre otros, según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2003).

¿Es el ciberespacio un derecho humano?

Para poder dar respuesta a esta inquietud procederemos a enunciar algunos tratadistas que se han pronunciado sobre el tema, a quienes destacamos a continuación. El autor Salazar (2014) manifestó de forma muy puntual que el internet es un derecho fundamental, el cual tiene dos connotaciones relevantes: derivado y autónomo. El primero consiste en:

> (…) medio de comunicación masivo, facilita, permite y materializa el derecho de propiedad individual y colectiva, los derechos de libertad de pensamiento, conciencia y religión, como su libertad manifestarlos, el derecho de libertad de opinión y de expresión, también facilita la participación del individuo en las actividades culturales. (p. 283)

Por otra parte, como derecho fundamental con una connotación autónoma. Al respecto, Salazar aduce:

> De manera autónoma, la internet es un derecho al avance científico y tecnológico y a sus beneficios, como lo son el derecho al estudio y al trabajo virtual, etc., además, concede unos derechos subjetivos patrimoniales por la producción en ella, de carácter científico, material o literario. (pp. 283-284)[10]

Asimismo, la información que circula en internet tiene como trasfondo la existencia de unos derechos de autor; toda vez que dentro de

[9] Esta Declaración fue adoptada mediante Resolución 32C/41 de 2003 por la UNESCO.
[10] Salazar (2014) definió internet como "un derecho fundamental derivado y autónomo" (p. 283).

dicho escenario cibernético fluye una serie de datos, imágenes, archivos y documentos que deben tener un titular que los respalde. Sin embargo, cuando ingresan a un sistema de información dentro de la red también hay unos derechos sobre el hardware y el software que pasan en este ciberespacio (Salazar, 2014).

En el ciberespacio existen mecanismos que permiten hacer expansión de la información, con la posibilidad de que todas las personas puedan tener acceso a ella. De igual manera están los derechos que surgen con motivo de dicha promoción, para quienes ostenten la calidad de usuario, en un mundo donde la tecnología cada vez tiene mayores índices de empleabilidad para alcanzar su máximo nivel de difusión.

El autor Riofrío (2014) indicó de forma estricta que hay una cuarta ola o generación de DDHH que debido a esa coyuntura tecnológica en el manejo de la información se les conoce como *derechos digitales*. Dentro de este contexto comunicativo, en el escenario del ciberespacio surgen unos derechos derivados del mundo digital que deben ser objeto de reconocimiento y protección legal, para garantizar su debido ejercicio. Tal es el caso de:

> a) El derecho a existir digitalmente; b) El derecho a la reputación digital; c) La estima digital; d) La libertad y responsabilidad digital; e) La privacidad virtual, el derecho al olvido, el derecho al anonimato; f) El derecho al big-reply; g) El derecho al domicilio digital; h) El derecho a la técnica, al update, al parche; i) El derecho a la paz cibernética y a la seguridad informática; y j) El derecho al testamento digital. (p. 31)

Con base en ello toda persona tiene derecho a estar presente en el mundo digital de diversas formas, a través de fotos o imágenes, archivos, opiniones, entre otras; condicionante o pilar para que los demás derechos digitales existan. Asimismo, a tener *una identidad digital* o que se le permita estar identificado individualmente como persona física o jurídica en el mundo virtual, para ser objeto de reconocimiento frente a los demás, adoptando un *core identity, nickname,* o una identidad fragmentada, según su rasgo digital de identificación.

También a tener un trato digno en relación con su honor y su honra, debiendo ser tratado más como un fin que como un instrumento, con respeto, siendo dicha reputación cuantificable por el número de usuarios que

accedan a dicha información. A la existencia de una libertad asumiendo su responsabilidad frente a lo que no está permitido; toda vez que en internet no hay límites físicos. A tener privacidad virtual, que no es igual a intimidad, puesto que esta la ostenta el cibernauta– sea como persona natural o jurídica –en el que el mismo usuario puede limitar su acceso, máxime cuando el mundo virtual es de exposición.

Por otro lado, a tener *derecho a una dirección virtual* o donde permanezca el cibernauta para ser contactado, con un nombre de dominio (DNS). A poder *contestar, repetir y publicar un mensaje* dentro de la red para poder difundirlo a más usuarios con suma responsabilidad. *Acceder al conocimiento*, al intercambio y al desarrollo en el ciberespacio, bajo un costo razonable, permitiendo mejorar los programas con avances tecnológicos (*update*) arreglando los bienes informáticos que se encuentren defectuosos (*parche*), *A tener paz* en un mundo digital donde los intranquilizan los hackers, los crackers, las intromisiones, las injurias en red, los robos de identidad, el *cyberbullying*, entre otros. Finalmente, tener la posibilidad de *prolongar su existencia en el mundo digital,* aunque no se encuentre vivo, a modo de conmemoración (Riofrío, 2014).

Por ejemplo, cuando actuamos en el ciberespacio, más que hablar del derecho a la intimidad se debe hacer alusión de forma correcta a *la protección de la privacidad*; toda vez que en dicho escenario de manera frecuente se presentan algunas contingencias en la difusión de ciertos asuntos relativos a la persona, para lo cual se concretan dos tipos de interés objeto de protección legal. Por una parte, a la vida privada del usuario; por otro, el interés de la sociedad de acceder a la circulación de dicha información.

Además, la infraestructura de la red está basada en datos personales (o IP), donde se utilizan instrumentos técnicos para circular la información y tener conexión con otros usuarios. Cuando se habla de protección de datos personales el navegador debe informar al usuario qué información se pretende transferir y con qué objeto. Cuando existan hipervínculos, el navegador debería indicar el sitio en su totalidad y, finalmente, poner en conocimiento qué información pretende almacenar señalando el objeto y periodo de validez[11] (Viega, 2015).

[11] Como referente de interpretación, el legislador europeo ha estimado frente a la protección de datos que, "(…) el legislador europeo se propuso adoptar un concepto amplio de datos personales, aunque ese concepto no es ilimitado. Nunca hay que olvidar, indica este documento del Grupo de expertos europeos, que el objetivo de las disposiciones de la Directiva es proteger los derechos y libertades fundamentales individuales, en especial el derecho a la intimidad, en lo que se refiere al tratamiento de datos personales. Por ello, estas normas se concibieron para ser aplicadas en situaciones en las que los derechos individuales pueden correr peligro y, por tanto, necesitar protección" (Ordóñez, 2012, p. 78).

Otros escenarios internacionales que reconocen al ciberespacio como un derecho humano

Desde el año 2005 en la Cumbre de Túnez se llevaron a cabo dos coaliciones para la conformación de un documento de importancia de reconocimiento de derechos digitales: Una Coalición Dinámica de la Declaración de Derechos de Internet, designada a desarrollar una Carta de Derechos Humanos; así como una Coalición Dinámica por un Marco de Principios para Internet, destinada a enfocarse en principios de gobernanza de internet.

Para el año 2009 las dos asociaciones se fusionaron formando la Coalición Dinámica de Principios y Derechos de Internet (IRPC), para combinar su esfuerzo y recursos dentro de un modelo de participación de múltiples partes. Esa *Carta de Derechos y Principios para Internet* fue el resultado del ejercicio de la IRPC quien participó activamente en el Foro Anual sobre la Gobernanza de Internet (IGF), consagrando la existencia de unos derechos que deben ser objeto de reconocimiento y protección dentro del ciberespacio[12] (Internet Rights and Principles Coalition, 2015).

Lo anterior se puede evidenciar en algunas profesiones objeto de salvaguarda legal por parte de ciertas organizaciones de derecho internacional. Por ejemplo, el Consejo de Derechos Humanos mediante el *Informe del relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión,* Frank La Rue (4 de junio de 2012) realiza una serie de recomendaciones a los Estados parte para brindar seguridad y protección frente a actos de impunidad que atenten contra quienes actúan

[12] Para los cuales se enuncian los siguientes: 1º.) El acceso a internet (donde se busca la calidad del servicio, la libertad de elección del sistema y del software, la inclusión digital y la neutralidad e igualdad de la red); 2º.) La no discriminación en el acceso, uso y gestión de internet (garantizando la igualdad de acceso y de género, y especial atención a grupos marginados); 3º.) La libertad y seguridad en internet (brindando protección contra todas las formas de delincuencia, y seguridad en el internet); 4º.) El desarrollo a través de internet (estimulando la reducción de la pobreza y el desarrollo humano, y la sostenibilidad del medio ambiente); 5º.) La libertad de expresión e información en internet (promoviendo la libertad de protesta en línea, la libertad ante la censura, el derecho de información, la libertad de los medios de comunicación, y la libertad frente al discurso de odio); 6º.) La libertad religiosa y de creencias en internet; 7º.) La libertad de reunión y de asociación online (permitiendo la participación en la asamblea y asociación en internet); 8º.) La privacidad en internet (donde se debe establecer en la legislación nacional: el tema de la privacidad, la política de configuración de privacidad, las normas de confidencialidad e integridad de los sistemas TIC, la protección de la personalidad virtual, el derecho al anonimato y a utilizar cifrado, la libertad ante la vigilancia y ante la difamación); 9º.) Protección de los datos digitales (donde se establecen las obligaciones a los colectores de datos, se formulan normas mínimas sobre el uso de los datos personales y la monitorización de la protección de datos); 10º.) Educación en internet y sobre internet (donde se busca promover la educación sobre la red y los DDHH).

con frecuencia en internet– difamación, injuria, bloqueo de sitios web, restricciones al acceso a internet y a los servicios de mensajería móvil, etc. –como son los periodistas, comunicadores sociales, blogueros, activistas y demás que estén amenazados por difundir información o especial tipo de noticia, en países que prefieren optar por la represión en vez de la reforma; además de la aceptación de opiniones discrepantes, o escuchar a la población para construir adecuadamente una sociedad sólida atendiendo el consentimiento de los gobernados, preferentemente de las minorías. Tal es el caso de Libia, República Árabe, Siria y Yemen, entre muchos otros.

Este informe va direccionado a aquellos países que presentan dificultad en la protección de los periodistas y de la libertad de prensa en situaciones que no son de conflicto armado[13], incluyendo a Colombia (Asamblea General de las Naciones Unidas, 2012).

Luego, mediante *The Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue* (17 de abril de 2013) se continuó realizando recomendaciones a los Estados Parte para brindar seguridad y protección a los derechos de la libertad de expresión y de opinión. Lo anterior, toda vez que se busca promover la innovación e implementación de la tecnología para facilitar el acceso a las comunicaciones, fomentando el máximo respeto por la libertad de expresión. Asimismo, se pretende promover la habilidad de permanecer en el anonimato permitiendo compartir rápidamente la información para generar un cruce cultural; especialmente a través de técnicas que faciliten el procesamiento de la información personal.

Por su parte, las Tecnologías de la Información y las Comunicaciones (TIC) se han convertido entonces en un instrumento para la lucha contra la pobreza, prácticamente como requisito indispensable para el desarrollo. A partir de las TIC les permiten a los países tercermundistas aprovechar el potencial de los *derechos digitales* para ir obteniendo un crecimiento económico y un progresivo bienestar humano, admitiendo robustecer la democracia y la participación ciudadana.

Es decir, se debe extender el acceso a la sociedad de la información para llevar a cada individuo, hogar y escuela a la era digital. Donde el objetivo no solo sea de orden local; también global para así cubrir las necesidades más básicas como el derecho a buscar, recibir y transferir información

[13] Dentro de los cuales se enuncian los Gobiernos de los siguientes Estados: Angola, Azerbaiyán, Bielorrusia, China, Cuba, Ecuador, Egipto, El Salvador, Emiratos Árabes Unidos, España, Etiopía, La Federación Rusa, Georgia, Honduras, República Islámica de Irán, Iraq, Kazajistán, Libia, Madagascar, Malasia, Malawi, Maldivas, Marruecos, México, Pakistán, Panamá, República Árabe Siria, Sri Lanka, Sudán, Tailandia, Túnez, Turquía, Uganda, Uzbekistán, República Bolivariana de Venezuela, Vietnam y Yemen.

e ideas a través de cualquier medio sin ningún tipo de limitación. Toda iniciativa global y regional deberá construirse bajo programas diseñados por los gobiernos y las organizaciones regionales e internacionales, contando con el apoyo, participación e implicación del sector privado y de la misma sociedad civil (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2003).

Además, el desarrollo de la sociedad de la información va a cambiar sustancialmente al ente colectivo en su interior, como es el asunto de la organización de las grandes y pequeñas empresas; la prestación de los servicios educativos y sanitarios; el funcionamiento de las instituciones políticas y administrativas; los comportamientos de los individuos en el orden social y cultural; así como la reconfiguración del mapamundi económico del mundo. Es decir, estamos en el cambio de era, muy parecido al de la Revolución Industrial que obligó a los responsables políticos a reflexionar sobre las medidas que tendrían que implementar para asumir los nuevos retos para convertirlos en oportunidades.

Tal es el caso de las TIC, que implica el fin de las distancias más no de los lugares. Las regiones y ciudades constituyen la escala más idónea para el desarrollo de la sociedad de la información; los gobiernos estarán obligados a recopilar una visión histórica para proporcionar un adecuado liderazgo el cual será estratégico. A su vez, la necesidad de generar modelos básicos para el impulso de la sociedad de la información; por un lado, donde se permita la extensión y uso de nuevas tecnologías (lo cual sería generalizable), por otro, centrarse en la potencialización de su producción (que sería más selectiva).

En adición, las TIC suponen la necesidad de generar recursos económicos reales por parte de los gobiernos para poder impulsar las sociedades de la información, pensando en función de la realidad y así proporcionar ventajas competitivas. Igualmente, contar con recursos humanos cualificados para estimular un éxito en dichas sociedades. Por último, promover en las universidades el estudio y desarrollo de esta sociedad de la información como eje central del Sistema Regional de Innovación y Conocimiento (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, 2003).

Sin embargo, a medida que se va reconociendo la existencia de ciertos derechos y libertades fundamentales que circulan en el ciberespacio; asimismo, se van presentando conductas desviadas que atentan de forma flagrante contra estos, haciendo que la criminalidad vaya mutando y empleando mejores mecanismos que rebasen la legalidad, para impedir el

acceso a la información que circula en las redes. Para ello, se formuló el Convenio de Budapest que determinó la existencia de la ciberdelincuencia, con la que se demostró la presencia de delitos informáticos, o cometidos en internet. Este es el primer instrumento internacional que formuló la búsqueda de técnicas de investigación efectivas para contrarrestar la lesión o puesta en peligro de los derechos digitales; así como de tipos de delitos de alta reprochabilidad social como la pornografía infantil.

Igualmente, la búsqueda e implementación de la recopilación de datos personales en el ciberespacio; la promoción de nuevos desafíos e ideas, y una adecuada cooperación armónica entre los Estados Parte para dar cumplimiento efectivo en materia de protección de los DDHH y las libertades fundamentales en el mundo cibernético (Bélanger, 2017).

Por ello, desde el siglo XXI se ha pensado en un escenario estratégico para solventar los riesgos y amenazas internacionales contra la paz, el equilibrio, la estabilidad y la seguridad; frente al caso del terrorismo de carácter transnacional y de alcance global, con una gran capacidad de ocasionar daño de forma indiscriminada, dando lugar a diversas formas de ataques que pueden llegar a presentarse en el ciberespacio.

Es allí donde la superioridad militar tradicional no constituía un factor de disuasión eficaz, no garantizaba más seguridad, ni tampoco aseguraba la prevención efectiva contra ataques terroristas o ciberataques. Por consiguiente, las organizaciones internacionales en seguridad y defensa se trazaron como meta la lucha contra las nuevas amenazas, incluyendo dentro de sus estrategias el apoyo logístico, el mando y control de sus fuerzas, la información de inteligencia en tiempo real, dándole prioridad a los avances tecnológicos para dotar de capacidad a los miembros de la fuerza en el ciberespacio.

Por ende, dentro de las operaciones cibernéticas en las redes se emplean las Operaciones sobre redes de computadores (CON, por sus siglas en inglés *Computer Network Operations*)[14]. Como acciones incluye el *Computer Network Defense* –para proteger, monitorizar, analizar, detectar, reaccionar y recuperarse con celeridad de los ataques, intrusiones, perturbaciones u otras acciones no autorizadas que podrían comprometer la información y los sistemas que manejen; –el *Computer Network Exploitation* (CNE)– para la inteligencia encaminada a la recolección de información sobre sistemas de información del enemigo, así como su explotación–. Finalmente, *Computer Network Attack* (CNA)– para perturbar,

[14] Entendido como "las acciones tomadas de forma deliberada para obtener la superioridad en la información y denegarle esta al enemigo" (Ministerio de Defensa de España, 2010, p. 227).

denegar, degradar o destruir información que circula por los sistemas enemigos –(Instituto Español de Estudios Estratégicos, 2010).

¿Cómo se da la protección a los derechos digitales en Colombia?

El creciente uso de internet es uno de los avances tecnológicos y políticos más interesantes de los últimos años del siglo XX, donde las redes tienen el potencial para convertirse en el medio más propicio para el desarrollo del mercado global de una sociedad; además de la ejecución de las actividades políticas tradicionales para que el ente colectivo siga evolucionando de forma progresiva, especialmente en ese espacio virtual (Rueda-López, 2007).

Sin embargo, para poder darle viabilidad a ese desarrollo prominente fue necesario acudir a la tendencia dominante del ejercicio de soberanía del poder (teoría de cosoberanía). En este sentido, el ejercicio del poder supremo del Estado sobre ese espacio virtual podía ser de un grupo de individuos que convergen, independientemente de su ubicación geográfica, en donde como miembros del Estado se despojan de sus banderas para interactuar.

De ello surge una inquietud de entender qué pautas actúan y dónde reside dicha "soberanía" si nos posicionamos en un espacio sin fronteras; toda vez que el espacio virtual o "ciberespacio" es tan extenso. Para ello, la tendencia mundial se direcciona a las relaciones internacionales y a la creación de organismos supranacionales que tengan un papel preponderante para afrontar dicha inquietud, a través de lo que se llamó "derecho de integración"[15].

Por ende, internet ofrece un mayor servicio de apoyo a los sistemas de los gobiernos nacionales e internacionales, desde su visión liberal; cada vez que con las redes se puede brindar el mismo apoyo al Estado de derecho internacional y al estado de derecho nacional; así como contribuir al desarrollo de una interdependencia económica entre Estados y pueblos. A su vez, incrementar su participación en las relaciones internacionales mediante el uso de internet a través de los actores no estatales como pueden ser las organizaciones no gubernamentales internacionales. Finalmente, reforzar las operaciones de paz y seguridad colectiva utilizando los mecanismos de comunicación que brinda la internet (Rabinad, 2008).

[15] Para entender ello se puede traer a colación el ejemplo de la comunidad europea donde los Estados miembros están cediendo derechos que tradicionalmente se consideraban indelegables en los órganos comunitarios.

Para el caso colombiano, ante las diversas las amenazas que pueden afectar nuestro Estado en el ciberespacio se han acudido a otras medidas legales, aparte de los instrumentos ya citados del concierto internacional, para fortalecer la seguridad y así garantizar la protección integral de la información durante el ejercicio de los *derechos digitales.* Al respecto se citan los siguientes:

1. Convenio sobre Ciberdelincuencia 14 del Consejo de Europa (CCC). Conocido como *Convenio sobre Cibercriminalidad de Budapest,* adoptado en noviembre de 2001 y con entrada en vigor desde el 1 de julio de 2004[16].
2. Resolución AG/RES de 2004 (XXXIV–O/04), de la Asamblea General de la Organización de los Estados Americanos[17].
3. Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 2004[18].
4. Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT), en el seno de las Naciones Unidas, para el desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005[19].
5. Resolución A/RES/64/25 de 2009 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional" Asamblea General de las Naciones Unidas. (2009)[20] (Centro Superior de Estudios de la Defensa Nacional, 2012).

[16] También conocido como Convenio de Budapest, pretende que se adopte una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal, que permitan detectar, investigar y sancionar las conductas antijurídicas (Conseil de L'Europe, 2001).

[17] Este instrumento se adoptó con el fin de establecer una estrategia integral para combatir las amenazas a la seguridad cibernética, con un enfoque multidimensional y multidisciplinario y así generar "una Cultura de Seguridad Cibernética" (Resolución 2040 [XXXIV-O/04[de 2004).

[18] Este instrumento se establece en aras de forjar los lineamientos de la Política de Seguridad Externa de la Comunidad Andina, especialmente para prevenir, combatir y erradicar las nuevas amenazas a la seguridad; así como cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientados a enfrentar los desafíos que representen dichas amenazas (Resolución 2040 (XXXIV-O/04) de 2004).

[19] Este documento se estableció en aras de fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones; así como de promover la cultura de ciberseguridad, para mejorar el acceso y su comercio, teniendo en cuenta el nivel de desarrollo social y económico de cada país, y respetando los aspectos inherentes al desarrollo de la sociedad de la información (Secretaria Ejecutiva de la CMSI, 2006).

[20] Este instrumento busca promover el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en dicho ámbito (Resolución A/RES/64/25 de 2009).

Asimismo, de acuerdo con su misión la institucionalidad ha acudido a la implementación de medidas para salvaguardar el acceso a la información y la consecuente protección para quienes se encuentren navegando en dicho espacio virtual, como es el caso del Ministerio de Tecnologías de Información y Comunicaciones de Colombia (MinTIC). En aras de reducir los obstáculos lingüísticos y fomentar los intercambios humanos en internet, dicha entidad consideró importante brindar especial protección al acceso universal del ciberespacio, asumiendo y dando cumplimiento a las recomendaciones formuladas por la UNESCO. Estos últimos compelían a los Estados Parte a promover la creación y tratamiento de contenidos educativos, culturales y científicos en formato digital; así como su acceso, para garantizar que todas las culturas puedan expresarse y acceder al ciberespacio en todas las lenguas, comprendiendo también las indígenas[21] (Ministerio de Comunicaciones, 2006).

Para el Estado colombiano ello representa la necesidad de seguir efectuando la formulación de recomendaciones y la aplicación de medidas efectivas sobre política informática de forma progresiva y a la vanguardia de los cambios; para lograr la implementación de una infraestructura que facilite la difusión de las tecnologías de la información y la comunicación; así como de medidas de seguridad que permitan infundir sensación de confianza para quienes naveguen en dicho espacio virtual.

Tanto es así que desde antes del año 2006 el Gobierno nacional ya empezaba a asumir los compromisos nacionales e internacionales para con su población al configurar un Sistema de Información y Seguimiento a Metas de Gobierno (SIGOB). Con este se registran módulos de programación, gestión por resultados, correspondencia y archivos oficiales, gestión de despachos, centro de gestión y monitoreo, análisis de consejos municipales, de ministros y de seguridad, entre otros (Ministerio de Comunicaciones, 2006).

[21] Más de 65 lenguas indígenas han sido reconocidas en Colombia, siendo agrupadas en 12 familias lingüísticas, información que ha sido obtenida y puede ser complementada en el Centro de Documentación en Lenguas Indígenas Palabra y Memoria (s.f.) del Departamento de Lingüística de la Universidad Nacional de Colombia.

¿La Fuerza Pública de Colombia es la encargada de brindar efectiva protección en el ciberespacio, escenario propicio para la adecuada interacción y ejercicio de los derechos digitales como derechos humanos?

Así como el sector de las nuevas tecnologías y de la comunicación ha efectuado la implementación de medidas para salvaguardar el acceso y uso de la información por parte de los cibernautas; existen otras instituciones que hacen parte de esa estrategia encaminada a dicha protección. Por mencionar algunos, se encuentra el Departamento Nacional de Planeación (DNP), el Ministerio de Defensa Nacional, la Comisión de Regulación de Comunicaciones (CRC), el Ministerio de Justicia y del Derecho, el Departamento Administrativo de Seguridad en Procesos de Supresión, la Fiscalía General de la Nación y el Ministerio de Relaciones Exteriores (Ámbito Jurídico, 2015).

Como consecuencia, desde el año 2009 se consagraron diferentes tipos penales en materia de ciberdelitos a nivel normativo. Con la implementación de nuevas tecnologías se presentan nuevas amenazas o riesgos que pueden afectar intereses jurídicos y libertades fundamentales de las personas. Por ende, era necesario codificar aquellas conductas que quebrantasen esos derechos digitales, ampliando aquellos comportamientos que trastoquen derechos de autor, el derecho de habeas data, o se haga alusión al uso o acceso transfronterizo indebido de datos informáticos almacenados (Ley 1273 de 2009)[22].

Por otro lado, a través del documento CONPES 3701 se establecieron los lineamientos en política pública para contrarrestar las amenazas cibernéticas de la que pueda ser objeto el Estado colombiano. El Ministerio de Defensa Nacional es parte de esa estrategia nacional en ciberseguridad y ciberdefensa, quien a través del Comando Conjunto Cibernético será el encargado de la defensa del país en el ciberespacio. Dentro de sus parámetros misionales se estableció:

[22] La Ley 1273 de 2009 consagró otros comportamientos conocidos como ciberdelitos, dentro de los cuales se establecen los siguientes: atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos; acceso abusivo a un sistema informático; obstaculización ilegítima de sistema informático o de red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; violación de datos personales; suplantación de sitios web para capturar datos personales; hurto por medios informáticos y semejantes; transferencia no consentida de datos, entre otros.

6. La implementación de unas instancias para prevenir, atender, controlar y generar recomendaciones que regulen incidentes o emergencias cibernéticas.
7. Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa.
8. Fortalecer el cuerpo normativo para dar cumplimiento en dichas competencias.
9. Defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país; así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia.

Bajo estos parámetros se destaca el respeto y la protección frente a los derechos de autor y conexos a internet, a la privacidad y a los datos personales o información de los usuarios; así como a la infraestructura crítica en el ciberespacio del Estado colombiano (Departamento Nacional de Planeación, 2011). Con dicho documento se creó el Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), componente importante y ejecutor para el desarrollo de la estrategia en ciberseguridad y ciberdefensa de Colombia. Lo anterior, toda vez que era necesario asegurar la defensa de ese espacio virtual frente a los ciberdelincuentes, y de los demás infractores o hackers que usurpen información de quienes acceden a la internet.

Aunado a ello, se gestó la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), del Centro Cibernético Policial (CCP). También la adopción del mecanismo de coordinación intersectorial más adecuado para emitir los lineamientos rectores del ColCERT; la emisión de modelos de seguridad en el ciberespacio que minimicen el nivel de riesgo al que las entidades están expuestas; el diseñar campañas de sensibilización y concienciación en temas de seguridad cibernética bajo coordinación del MinTIC; la implementación gradual de asignaturas en seguridad de la información, ciberdefensa y ciberseguridad (teórico-prácticas) en las escuelas de formación y capacitación de oficiales y suboficiales; el planteamiento de capacitación en temas de seguridad de la información de funcionarios del Estado, con el apoyo de

organismos internacionales; así como el diseño e implementación de planes de capacitación en lo referente a seguridad informática, investigación y judicialización de delitos informáticos para policía judicial, entre otros aspectos misionales (Ámbito Jurídico, 2015).

Para el año 2016 el Ministerio de Defensa Nacional ya había planteado una iniciativa de "Transformación y futuro de la fuerza pública 2030", de acuerdo con las capacidades de las fuerzas militares y de la policía nacional y según sus diversas especialidades (sean jefes de operaciones, inteligencia o planeación), para enfrentar los retos en operaciones conjuntas e interagenciales. Lo anterior, en aras de propender por la seguridad y defensa de los intereses nacionales y contribuir al bienestar de todos los colombianos, tal como lo define el artículo 4° del Decreto 1512 del 11 de agosto de 2000[23].

Es decir, formas de combatir las nuevas amenazas asumiendo los retos emergentes para preservar la paz y el medio ambiente, contribuyendo activamente en el logro de los fines esenciales del Estado y en el desarrollo tecnológico, científico, social y económico del país, con un absoluto arraigo por el respeto a la dignidad humana[24] (Ministerio de Defensa Nacional, 2016).

Ahora bien, con el documento CONPES 3854 se estableció una Política Nacional de Seguridad Digital para contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de defensa del país y lucha contra el cibercrimen, posicionando a Colombia como uno de los líderes en esta materia a nivel regional. Lo importante con este documento es el fortalecimiento de la institucionalidad frente al grupo de ColCERT del Ministerio de Defensa Nacional, en comunión con otras entidades dirigidas a la protección de los derechos digitales[25].

Además, se planteó la coordinación y orientación superior de la seguridad digital en cabeza del Gobierno nacional, estableciendo enlaces en

[22] Véase el Decreto 1512 de fecha 11 de agosto de 2000, Por el cual se modifica la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones", que a tenor literal del artículo 4° se adujo lo siguiente: "(…) El Ministerio de Defensa Nacional tiene como objetivos primordiales la formulación y adopción de las políticas, planes generales, programas y proyectos del sector administrativo defensa nacional, para la defensa de la soberanía, la independencia y la integridad territorial, así como para el mantenimiento del orden constitucional y la garantía de la convivencia democrática" [Énfasis agregado].

[24] El mentado decreto establece como objetivos principales los siguientes: "(…) 1°.) Garantiza el control del Estado sobre la totalidad del territorio nacional; 2°.) Enfrentará de manera exitosa una crisis de seguridad interna y otra de defensa externa, de manera simultánea; y, 3°.) Empleará las capacidades disponibles para responder a misiones de carácter no principal: contribución al desarrollo, cooperación en el mantenimiento de la seguridad y atención de desastres".

las entidades de la rama ejecutiva en todo el país. Igualmente, se buscó la implementación de acciones para manejar el riesgo en seguridad digital mediante mecanismos de participación, permanentemente por parte de miembros del ente colectivo; así como la adecuación del marco legal-regulatorio en la materia y la determinación de la responsabilidad frente a comportamientos contrarios en el ejercicio del entorno digital. Finalmente, se busca fortalecer la defensa y seguridad nacional en el medio cibernauta, tanto a nivel nacional como transnacional, enfocado a la gestión de los riesgos frente a actividades económicas y sociales (Departamento Nacional de Planeación, 2016).

Por último, el CCOC del Ministerio de Defensa Nacional tiene como meta específica determinar las infraestructuras críticas del país en todos los sectores, como es el petroquímico, el hídrico, el minero, el eléctrico, el educativo y el de alimentos, entre otros; especialmente en seguridad de redes, protección de datos del usuario, preservación de evidencia digital, etc. (Ámbito Jurídico, 2015).

Entonces, los miembros de la fuerza pública estarán en búsqueda de la implementación de mejores y efectivas medidas de seguridad y protección de los cibernautas. Lo anterior, para contrarrestar los posibles efectos nocivos que recaigan en los diferentes escenarios en que los seres humanos se desenvuelvan, especialmente cuando se encuentren navegando en el espacio virtual: *un verdadero* DDHH.

Conclusiones

Todos los Estados deben incursionar en estimular el uso y acceso de las TIC; toda vez que es un ámbito que le permite al ser humano desenvolverse en su integridad, posibilitando adquirir herramientas invaluables para estar a la vanguardia de los cambios. Además, es una forma de poder adquirir información actualizada en el menor tiempo posible y a muy bajo costo, al encontrarse a la mano de cualquier persona que desee acceder.

[25] Las instituciones que en colaboración armónica actuarán para brindar dicha protección digital son: el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), la Delegatura de protección de datos en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de Ciberdefensa de las Fuerzas Militares, y las Unidades Cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana (Ministerio de Defensa Nacional, 2016, pp. 13-14).

En dicho espacio virtual se permite a las sociedades contribuir de forma segura en la construcción del tejido social, en la mejora de sus instituciones. Su fin último consiste en que, en colaboración armónica con otros factores, puedan dinamizar de forma efectiva las soluciones al instante frente a la problemática existente en dicho ente colectivo.

Sin embargo, a medida que esa sociedad avance en su innovación cultural, social y productiva, se van presentando innovadores retos, nuevos riesgos o amenazas gestadas por los ciberdelincuentes para afectar bienes jurídicos que reclaman desde ya una justa y efectiva protección. A medida que se van reconociendo innovadoras creaciones, va mutando la forma de usurpar o defraudar expectativas contra quienes ejercen de forma legítima su derecho digital, conllevando a estar actualizando de forma constante la seguridad y defensa del ciberespacio.

Ello sobrellevó a que los Estados suscribieran diversos instrumentos del concierto internacional para generar herramientas que permitiesen la protección de una serie de derechos y libertades fundamentales inmersos dentro de ese espacio virtual de interacción tecnológica, llegando a ser considerado DDHH al fomentar el intercambio de contenido cultural, social, científico, tecnológico y productivo de forma digital. Sin embargo, esto no es óbice para desconocer otros escenarios en que puedan incursionar las nuevas tecnologías, como es el eléctrico, el hídrico, el petroquímico, el minero, en el campo de la medicina, de la robótica o nanotecnología, el educativo, entre muchos otros.

Ahora, en nuestra sociedad estructurada existe un factor real de poder expresado en el Ministerio de Defensa Nacional. Allí los integrantes de la fuerza pública serán los encargados de la defensa del país y de la seguridad ciudadana en el ciberespacio, a través del CCOC de las fuerzas militares y del CCP respectivamente. En ese sentido, formularán parte de las medidas efectivas para dar adecuado desarrollo a esa estrategia de ciberseguridad y ciberdefensa. Por ende, respeto a los derechos que interactúan en dicho espacio virtual, para así minimizar los efectos colaterales que puedan realizar los ciberdelincuentes; así como frente a otros flagelos de alta reprochabilidad social en nuestro ente colectivo, por ejemplo, los delitos cibernéticos; la pornografía y explotación sexual con menores de edad; explotación, pornografía y el turismo sexual con niños.

De acuerdo con la especialidad de algunos miembros de la fuerza pública en tecnologías, les atribuye un deber de salvamento constitucional con el cual deberán actuar como *garantes* en la seguridad y protección efectiva de los intereses jurídicos preminentes de nuestra sociedad colombiana, que interactúan en ese espacio virtual y humano: el *ciberespacio*.

Referencias

AG/RES. 2040 (XXXIV-O/04). Reunión de ministros de justicia o de ministros o procuradores generales de las américas. 8 de junio de 2004. Departamento de Derecho Internacional OEA.

A/RES/64/25. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. 14 de enero de 2010. Asamblea General Naciones Unidas.

Ámbito Jurídico. (2015, agosto 13). CRC identifica posibles acciones regulatorias en materia de ciberseguridad (2:50pm). https://www.crcom.gov.co/recursos_user/Documentos_CRC_2015/Actividades_regulatorias/Ciberseguridad/Doc_Ciberseguridad28_07_15.pdf.

Barrena, G. (2012). *El pacto internacional de derechos civiles y políticos (Fascículo 3)* (1ª ed.). Comisión Nacional de los Derechos Humanos.

Bauman, Z. (2008). *Tiempos líquidos. Vivir en una época de incertidumbre* (1ª ed.). Tusquets Editores. https://catedratesv.files.wordpress.com/2016/07/bauman-zygmunt-tiempos-liquidos.pdf

Bélanger, P. (2017). Derechos Humanos y el Derecho Penal en el Ciberespacio. *Revista de la Secretaría del Tribunal Permanente de Revisión, 5*(10), 274-286. http://scielo.iics.una.py/pdf/rstpr/v5n10/2304-7887-rstpr-5-10-00274.pdf

Centro Superior de Estudios de la Defensa Nacional. (2012). El ciberespacio. Nuevo escenario de confrontación. *Monografías del CESEDEN,* (126). Ministerio de Defensa de España.

Conseil de L'Europe. (2001). Convenio sobre la ciberdelincuencia. Serie de *Tratados Europeos,* (185). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Decisión 587 de 2004 [Consejo Andino de Ministros de Relaciones Exteriores]. Lineamientos de la Política de Seguridad Externa Comunidad Andina. 10 de julio de 2004. www.sice.oas.org/trade/junac/decisiones/dec587s.asp

Decreto 1512 de 2000. Por el cual se modifica la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones. 11 de agosto de 2000. Ministerio de Defensa Nacional.

Departamento Nacional de Planeación. (2016, abril 11). *Documento CONPES 3854. Política Nacional de Seguridad Digital.* Consejo Nacional de Política Económica y Social. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Declaración del Milenio. 13 de Septiembre de 2000. http://www.un.org/spanish/milenio/ares552.pdf

Declaración sobre los derechos de las personas pertenecientes a minorías nacionales o étnicas, religiosas y lingüísticas. 18 de Diciembre de 1992. https://www.ohchr.org/Documents/Issues/Minorities/Booklet_Minorities_Spanish.pdf

Declaración Universal de los Derechos Humanos. Artículo 19, 27. 10 de diciembre de 1948.

Decreto 1512 de 2000 [Presidencia de la República de Colombia]. Por el cual se modifica la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones. 11 de agosto de 2000.

Departamento Nacional de Planeación. (2011, julio 14). *Documento CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Consejo Nacional de Política Económica y Social. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Giddens, A. (2000). *Un mundo desbocado. Los efectos de la globalización en nuestras vidas.* Taurus.

Instituto Español de Estudios Estratégicos. (2010). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia, (149).* Ministerio de Defensa de España. http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

Internet Rights and Principles Coalition. (2015). *Carta de derechos humanos y principios para internet* (1ª ed.). Naciones Unidas.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado– denominado "de la protección de la información y de los datos" –y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. 5 de enero de 2009. D.O. No. 47223.

Ministerio de Comunicaciones. (2006). *Informe de Colombia relativo a la "Recomendación de la UNESCO sobre la promoción y el uso del plurilingüismo y el acceso universal al Ciberespacio"*. República de Colombia. http://www.acnur.org/fileadmin/Documentos/Pueblos_indigenas/recomedacion_plurilinguismo_unesco_informe_colombia.pdf?view=1

Ministerio de Defensa Nacional. (2016). *Visión de futuro de las fuerzas armadas*. Imprenta Nacional de Colombia. https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estrategia_planeacion/proyeccion/documentos/vision_futuro_FA.pdf

Naciones Unidas Asamblea General. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40. https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Naciones Unidas Asamblea General Consejo de Derechos Humanos. (2012). *Informe del Relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue.* A/HRC/2017: https://www.acnur.org/fileadmin/Documentos/BDL/2014/9691.pdf

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2002). *Derechos humanos. Compilación de Instrumentos Internacionales. Instrumentos de carácter universal* (Vol. 1). Naciones Unidas.

Ordóñez, A. (2012). *El derecho de protección de datos personales y medios de comunicación con sede social en Sevilla: deberes y derechos en prensa, radio y televisión* [Tesis doctoral, Universidad de Sevilla]. Repositorio institucional Universidad de Sevilla. https://idus.us.es/xmlui/bitstream/handle/11441/70602/2012ordonelder.pdf?sequence=1.

Pacto Internacional de Derechos Civiles y Políticos. Artículo 27. 16 de diciembre de 1966.

Pacto Internacional de Derechos Económicos, Sociales y Culturales. Artículo 15. 16 de diciembre de 1966.

Rabinad, M. (2008). La soberanía del ciberespacio. Algunas reflexiones sobre el concepto de Estado, soberanía y jurisdicción frente a la problemática que presenta Internet. *Lecciones y Ensayos,* (85), 85-107. http://www.derecho.uba.ar/publicaciones/lye/revistas/85/05-ensayo-maria-gimena-rabinad.pdf

Resolución 2040 (XXXIV-O/04) de 2004 [Asamblea General de la Organización de Estados Americanos]. Reunión de ministros de justicia o de ministros o procuradores generales de las Américas. 8 de junio de 2004. http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

Resolución A/RES/64/25 de 2009 [Asamblea General]. Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. 2 de diciembre de 2009. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/25&Lang=S

Rabinad, M. (2008). La soberanía del ciberespacio. Algunas reflexiones sobre el concepto de Estado, soberanía y jurisdicción frente a la problemática que presenta Internet. *Lecciones y Ensayos,* (85), 85-107. http://www.derecho.uba.ar/publicaciones/lye/revistas/85/05-ensayo-maria-gimena-rabinad.pdf

Riofrío, J. (2014). La cuarta ola de derechos humanos: los derechos digitales. *Revista Latinoamericana de Derechos Humanos, 25*(1), 15-45.

Rueda-López, J. (2007). La tecnología en la sociedad del siglo XXI: albores de una nueva revolución industrial. *Aposta. Revista de Ciencias Sociales,* (32), 1-28. https://www.redalyc.org/pdf/4959/495950225001.pdf

Salazar, R. (2014). Derechos humanos e internet. *Derecho y Realidad,* (24), 279-288. https://revistas.uptc.edu.co/index.php/derecho_realidad/article/view/4518/4238

Secretaria Ejecutiva de la CMSI. (2005). *Informe de la Fase de Túnez de la Cumbre Mundial. Túnez, Palexpo Kram, 16-18 de noviembre de 2005.* WSIS-05/TUNIS/DOC/9. Naciones Unidas, UIT. https://www.itu.int/net/wsis/docs2/tunis/off/9rev1-es.pdf

Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. (2003). *La sociedad de la información en el siglo XXI: un requisito para el desarrollo. Reflexiones y conocimiento compartido* (Vol. 2). ENRED Consultores S.L. http://www.anamorenoromero.net/documentos/requisito_desarrollo.pdf

UNESCO. (2003). *Recomendación sobre la promoción y el uso del plurilingüísmo y el acceso universal al Ciberespacio.* UNESCO.

Viega, M. (2015). *Los derechos humanos en el ciberespacio.* Biblioteca VirtualCEJA.http://biblioteca.cejamericas.org/bitstream/handle/2015/615/LosDerechosHumanosenelCiberespacio.pdf?sequence=1&isAllowed=y