

LOS DERECHOS FUNDAMENTALES EN EL CIBERESPACIO

FUNDAMENTAL RIGHTS IN THE CYBERSPACE

Rodolfo Núñez Robinson*

Amprimo, Flury, Barboza & Rodríguez Abogados

Fundamental rights must evolve to address the challenges of the contemporary digital environment. Building on the constitutional recognition of unenumerated rights, this work supports the existence of a fourth generation of human rights, centred on interconnectivity and the inherent risks and threats of cyberspace. Cybersecurity is presented not merely as a technical issue, but as a structural condition for the effective exercise of both traditional and emerging fundamental rights.

This paper examines cyber threats and risks, emphasizing the need for a comprehensive risk management approach to safeguard individuals and their digital environment. It then identifies new fundamental digital rights: digital existence, digital identity, digital honour and reputation, digital freedom and responsibility, privacy, anonymity, the right to be forgotten, digital domicile, and the right to peace in cyberspace. Each is analysed from a constitutional, technical, and social perspective, highlighting its core content and the corresponding duties of both the State and private actors.

The article concludes that in a hyperconnected society, the law cannot remain static. Protecting human dignity requires adapting the constitutional framework to the digital environment, recognizing and guaranteeing fourth-generation rights as essential tools to preserve individual freedom, autonomy, and well-being in cyberspace.

KEYWORDS: Cybersecurity; interconnectivity; fourth generation rights; constitutional rights; cyberspace.

Los derechos fundamentales deben evolucionar para responder a los desafíos del entorno digital contemporáneo. Partiendo del reconocimiento constitucional de los derechos innominados, se concuerda con la existencia de una cuarta generación de derechos humanos, centrada en la interconectividad y los riesgos y amenazas inherentes al ciberespacio. La ciberseguridad se presenta no solo como una cuestión técnica, sino como una condición estructural para el ejercicio de los derechos fundamentales tradicionales y emergentes.

En este trabajo se examinan amenazas y riesgos cibernéticos, detallando la necesidad de un enfoque integral de gestión que proteja al individuo y su entorno digital. A partir de ello, se identifican nuevos derechos fundamentales digitales: existencia digital, identidad digital, honor y reputación digital, libertad y responsabilidad digital, privacidad, anonimato, olvido, domicilio digital y el derecho a la paz en el ciberespacio. Cada uno es analizado desde una perspectiva constitucional, técnica y social, destacando su contenido esencial y las obligaciones del Estado y los privados.

El artículo concluye que, en una sociedad hiperconectada, el Derecho no puede permanecer estático. La protección de la dignidad humana exige adaptar el marco constitucional al nuevo entorno digital, reconociendo y garantizando los derechos de cuarta generación como herramientas indispensables para preservar la libertad, autonomía y bienestar del individuo en el ciberespacio.

PALABRAS CLAVE: Ciberseguridad; interconectividad; derechos de cuarta generación; derechos constitucionales; ciberespacio.

* Abogado. Maestrando en Derecho (LL.M.) en Ciberseguridad, Ciberterrorismo y Derecho Internacional por la Universidad para la Paz de las Naciones Unidas (UPEACE) y el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI). Asociado senior del Estudio Amprimo, Flury, Barboza & Rodríguez Asociados (Lima, Perú). Código ORCID: <https://orcid.org/0009-0006-6533-9832><https://orcid.org/0009-0006-6533-9832>. Contacto: munez@amprimoabogados.com

Parte de las ideas desarrolladas en el presente artículo se apoyan en avances de investigación elaborados por el autor en el marco de su tesina para optar por el grado de Master of Laws en Ciberseguridad, Ciberterrorismo y Derecho Internacional, impartido por la UPEACE y el UNICRI. El contenido ha sido revisado, actualizado y adaptado específicamente para su publicación como artículo académico.

Nota del editor: El presente artículo fue recibido por el Consejo Ejecutivo de THÉMIS-Revista de Derecho el 29 de mayo de 2025, y aceptado por el mismo el 16 de diciembre de 2025.

I. REPENSANDO LOS DERECHOS FUNDAMENTALES: EL DESARROLLO TECNOLÓGICO Y EL NECESARIO SURGIMIENTO DE LOS DERECHOS DE CUARTA GENERACIÓN

Los derechos fundamentales son los más básicos de los derechos de las personas. Estos encuentran su fundamento en la dignidad del individuo; “[...] y que, a su vez, constituyen el fundamento del Estado y de la sociedad en su conjunto” (Landa Arroyo, 2017, p. 11). Así lo entiende nuestra Constitución al establecer en su primer artículo¹ que el fin supremo del Estado y la sociedad es la defensa de la persona humana y el respeto de su dignidad.

Dicha norma, como uno de los principales cimientos para el desarrollo de los derechos constitucionales, permite definirlos como “[...] el conjunto de derechos y libertades que, por ser inherentes al ser humano, se encuentran reconocidos en el ordenamiento jurídico constitucional y positivo. Son, así, los derechos humanos positivizados en la Constitución” (Rubio *et al.*, 2010, p. 19). La importancia de estas garantías ha sido recogida por nuestro Tribunal Constitucional en la sentencia recaída en el Expediente 1042-2002-AA/TC (fundamento jurídico 2.2):

[los] derechos fundamentales reconocidos en nuestra Constitución constituyen componentes estructurales básicos del conjunto del orden jurídico objetivo, puesto que son la expresión jurídica de un sistema de valores que por decisión del constituyente informan todo el conjunto de la organización política y jurídica. (2002, p. 3)

Sin duda, los derechos fundamentales ostentan una posición de medular importancia en el desarrollo de un Estado Constitucional y Democrático de Derecho, pues, como señala Loewenstein, son el más eficaz “[...] reconocimiento jurídico de determinados ámbitos de autodeterminación individual en los que el Leviatán no puede penetrar” (2018, p. 391). Es decir, sirven como una garantía que limita el ejercicio del Estado frente a privados, como a privados entre sí.

Los derechos constitucionales fueron pensados clásicamente para favorecer a la persona humana frente a libertades puntuales (como el derecho de petición, derecho a la propiedad, derecho a la rebelión, derecho a la vida, derecho a la libertad, entre otros), tal como lo explica Freixes Sanjuán. Sin embargo, hacia la mitad del siglo XIX “[...] la es-

tructura y la función de los derechos propios del constitucionalismo liberal se complementan con las nuevas aportaciones de la dogmática que intentan, [...] resolver el problema de la eficacia de los derechos con contenido económico-social [...]” (1992, pp. 15-19).

Precisamente, esta naturaleza fenoménica nos obliga a repensar los derechos constitucionales y a dejar de concebirlos como instituciones rígidas. Por el contrario, su propia esencia exige entenderlos como normas institucionales dinámicas que deben adaptarse continuamente a una realidad social en constante transformación (Landa, 2002, pp. 62-63). Loewenstein comparte esta perspectiva al afirmar que, a lo largo de los años, se ha dedicado considerable esfuerzo a clasificar y a fijar los límites de estas libertades fundamentales. Algunas de ellas, como la libertad de opinión y de asociación, que en un principio eran inequívocas, han tenido que ser de nuevo definidas y profundizadas a la luz de la experiencia empírica y el dinamismo social (2018, p. 391).

Y es que mientras la sociedad avance, los derechos fundamentales que la Constitución reconoce deben adaptarse y reformarse a sus cambios para servir de la mejor manera a la población a la que se deben. Hablar de Derecho Constitucional y tecnología es complicado, pues los asentados en esta materia tienen —e insisten en sostener— una concepción anacrónica y estéril sobre el alcance de protección de los derechos fundamentales que la Carta de 1993 debe proteger. Esta crítica no es reciente y ha sido advertida por autores como Flores Dapkevicius quien afirma:

[...] Otro tema fundamental es el desarrollo de la tecnología. [...] es una realidad que el constitucionalista no puede obviar aunque haya generaciones de constitucionalistas en actividad que hasta los cuarenta años no sabían qué era una computadora. La afirmación es cierta y obvia. (2021, p. 40)

Claramente, ya la tecnología ha avanzado a un paso avasallador y el Derecho está en la obligación de adaptarse a la nueva realidad que el texto de la norma fundamental no contempló expresamente en su momento.

Precisamente por ello es que el constituyente, previendo el dinamismo inherente a la condición humana, incorporó a nuestra carta magna el artículo 3 como cláusula de apertura que prevé, de manera

¹ Artículo 1.- La defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado (1993).

expresa, la posibilidad de que existan derechos de orden constitucional innominados no regulados literalmente en el texto fundamental:

La enumeración de los derechos establecidos en este capítulo no excluye los demás que la Constitución garantiza, ni otros de naturaleza análoga o que se fundan en la dignidad del hombre, o en los principios de soberanía del pueblo, del Estado democrático de derecho y de la forma republicana de gobierno. (1993)

Esta norma, encuentra su antecedente en la IX Enmienda de la Constitución de los Estados Unidos de América la cual establece que: “no se interpretará la enumeración de ciertos derechos en la Constitución como negativa o menosprecio de otros que retenga el pueblo” (1789, p. 13) [traducción libre]². Esta visión iusnaturalista nos dejó una importante máxima que ha perdurado hasta la fecha: todo derecho que se encuentre taxativamente regulado en la Constitución tiene un valor declarativo, mas no constitutivo, al ser los derechos fundamentales inherentes al propio ser humano por ser su existencia más antigua, incluso, que la concepción del Derecho positivo. Sobre el particular, resulta importante citar a McClellan:

Redactada para servir como principio general de construcción, la Novena Enmienda declara que «la enumeración en la Constitución de ciertos derechos no debe interpretarse en el sentido de negar o menospreciar otros retenidos por el pueblo». El razonamiento que subyace a la enmienda procede de los ensayos 83 y 84 de Hamilton en El Federalista. Madison la introdujo simplemente para evitar una aplicación perversa de la antigua máxima jurídica de que una denegación de poder sobre un derecho especificado no implica una concesión afirmativa de poder sobre un derecho innominado. (2000, p. 346) [traducción libre]

En nuestro ordenamiento jurídico, lo siguiente ha sido concluido por el supremo intérprete de la Constitución en el fundamento jurídico 5 de la sentencia recaída en el Expediente 0895-2001-AA/TC:

[...] para que los textos constitucionales y, en particular, aquellos nuevos derechos directamente vinculados con el principio de dignidad no sean desmerecidos en su condición de auténticos derechos fundamentales como consecuencia de la existencia de nuevas necesidades o situaciones, de avances científicos, tecnológicos, culturales o sociales, las constituciones

suelen habilitar una cláusula de “desarrollo de los derechos fundamentales”, cuyo propósito no solo es prestarle el reconocimiento como derechos de la más alta consideración, sino incluso, dotarlos de las mismas garantías de aquellos que sí lo tienen expresamente. Ese es el propósito que cumple, por cierto, el artículo 3° de nuestra Constitución. (2001)

La interpretación definitiva que brinda el Tribunal Constitucional respecto a la naturaleza abierta de los derechos fundamentales es palmarmente clara y garantista de cara a la protección que debe el Estado a su sociedad; siendo que los avances de la sociedad requieren de la habilitación normativa de poder crear nuevos derechos que permitan un mayor alcance de tutela en virtud de la evolución tecnológica. Precisamente, en este proceso evolutivo destacan los avances de la ciencia, tecnología y los datos como activos. No cabe duda de que, desde 1993 a la fecha de publicación de este artículo, la sociedad ha tenido una serie de cambios estructurales y económicos sin precedentes, siendo uno de ellos el fenómeno de la interconectividad, el desarrollo y el acceso masivo al internet.

Así lo ha entendido Bustamante Donas al considerar tales advenedizos derechos tecnológicos dentro de la denominada ‘cuarta generación de derechos humanos’, luego de los civiles y políticos (primera generación); económicos y sociales (segunda generación); y los de la solidaridad (tercera generación):

Hablar de derechos humanos supone hablar de calidad de vida y de acceso a mejores condiciones para diseñar y realizar nuestras propias vidas, reconociendo en ellas algo mucho más digno que la simple existencia biológica. Hablar de calidad de vida y no mencionar a la tecnología es como hablar del desierto sin mencionar la arena. [...] Quizá la clave para el desarrollo de estos derechos humanos de cuarta generación esté en un concepto simple pero paradójico: el concepto de archipiélago. Por definición, un archipiélago es un conjunto de islas unidas por aquello que las separa. También, los seres humanos estamos profundamente unidos por aquello que nos diferencia los unos de los otros. En el valor de esta diferencia, y en el reconocimiento de la misma, se encuentra el principio de unidad que permitirá extender universalmente los estándares de calidad de vida de los que hoy en día sólo unos pocos gozan, y con los que muchos sueñan. Siguiendo con la metáfora, la tecnología será ese conjunto de

² Texto original: “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people (The Constitution of the United States, 1789, Amendment IX).”

instrumentos que nos permita otear el océano, viajar de una isla a otra –ya sea un cuerpo o en alma–, y también contemplar las lejanas estrellas en el cielo de la noche. (2001, p. 16)

Comprender los derechos fundamentales como fenómenos vivientes implica situarlos en un flujo dinámico, siempre dispuesto a renovarse conforme a las exigencias de la sociedad. Esta premisa, que dota de vida al derecho parte de la idea de Ehrlich, quien acuñó la noción de derecho vivo para describir el derecho como un fenómeno social –no meramente normativo– que se manifiesta y transforma en función de las necesidades reales de la población a la que sirve. Es, en buena cuenta, “[...] un orden espontáneo de la sociedad [...]” que responde a los hechos que se producen en su realidad (citado en Monereo Pérez, 2023, p. 344).

Hoy, esa adaptación jurídica se ve catalizada por la interconectividad: ya no somos sujetos aislados de derechos, sino nodos en redes globales de información y comunicación. Así, la garantía de la libertad de expresión, de la privacidad o del debido proceso depende de infraestructuras tecnológicas que configuran nuestra experiencia cotidiana. Ignorar esta nueva realidad –la de un individuo siempre conectado– es condenar al derecho a quedarse atrás de la propia vida que pretende tutelar hasta llegar a su obsolescencia.

Por ello, para que los derechos fundamentales sigan siendo el escudo más eficaz contra la arbitrariedad estatal y el espacio de autodeterminación individual, es imprescindible reconocerlos como instituciones fenoménicas, vivas, contextuales y sujetas a la innovación normativa. Esta situación no solo obliga a repensar su alcance, sino que legitima la creación de nuevas garantías –derechos de cuarta generación– destinadas a protegernos en este mundo digital al que, de manera inevitable, estamos tan entrelazados que constituyen nuestra nueva condición de ser.

II. LA INTERCONECTIVIDAD COMO VECTOR DE ATAQUE GLOBAL: CIBERAMENAZAS Y CIBERRIESGOS EN UN MUNDO HIPERCONECTADO

El inexorable entrelazamiento entre nuestro ser con la tecnología se debe al fenómeno de la interconectividad, la cual es la capacidad de encontrarse en un estado permanente de conexión con el internet y demás usuarios dentro del ciberespacio. Sobre este tema hemos escrito extensamente en otra oportunidad (Núñez, 2025), pero resulta indispensable recordar las premisas que constituyen este fenómeno; las ciberamenazas y ciber riesgos asociados. Si bien, el acceso irrestricto al internet es sumamente útil, trae consigo un altísimo costo

debido a las brechas generadas por el exponencial crecimiento de las tecnologías digitales, creándose un panorama de riesgos y amenazas cibernéticas conocido como el *cyberthreat landscape*.

Esta situación se agrava notoriamente por la ausencia de controles de seguridad –físicos, técnicos y administrativos– y, aún más, por la escasa sensibilización hacia la cultura de la ciberseguridad en personas y organizaciones. En particular, sus líderes, a menudo reacios a aceptar los avances tecnológicos por motivos generacionales, subestiman la importancia de protegerse en el entorno digital.

Es innegable que, a la fecha, prácticamente todo ser humano se encuentra inmerso, de alguna u otra manera, en el ciberespacio. Según la norma técnica ISO/IEC TS 27100, desarrollada por la Organización Internacional de Normalización (en adelante, ISO) y la Comisión Electrotécnica Internacional (en adelante, IEC), este se concibe como un dominio global del entorno informativo, integrado por una red interdependiente de infraestructuras de sistemas de información –incluyendo el internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos– cuya finalidad es posibilitar la comunicación y la interacción activa e ininterrumpida entre actores diversos (2020, pp. 2-3). Aunque su acceso es, en esencia, público, gran parte de sus componentes físicos y lógicos está en manos de empresas privadas, lo que genera un espacio híbrido de carácter tanto público como privado.

Si bien se ha intentado incorporar al ciberespacio dentro de la categoría *res communis omnium* y equiparlo con alta mar o el espacio aéreo internacional, resulta más preciso considerarlo como un dominio global o como el quinto dominio –además del aire, mar, tierra y espacio, toda vez que las actividades realizadas en este espacio involucran objetos, redes e individuos que operan dentro de un territorio nacional (Schmitt *et al.*, 2017, p. 12) y se encuentran sometidas a la soberanía de cada Estado sobre la porción de estos elementos que discurren por su territorio. En consecuencia, cada Estado será soberano de cómo regula su ciberespacio y las reglas, prohibiciones y permisiones que prescriba para su uso dentro del margen de la ley. A efectos regulatorios, este dominio se estructura en tres capas interrelacionadas, las cuales deben ser tomadas en cuenta al momento de diseñar cualquier política o marco normativo:

- a) **Capa física:** compuesta por hardware, cables y dispositivos de interconexión.
- b) **Capa sintáctica:** conformada por protocolos, normas y estructuras de datos que permiten el flujo de información.

- c) **Capa semántica:** donde reside el contenido y el significado de los datos transmitidos.

Este modelo multicapa facilita el análisis de vulnerabilidades específicas y el diseño de estrategias de protección adecuadas para cada nivel de infraestructura. Entre las características distintivas del ciberespacio destacan su falta de fronteras territoriales, la casi nula barrera de entrada y salida, el anonimato o la ofuscación de los actores, y la capacidad de propagación casi instantánea de cualquier acción o incidente en cualquier punto del globo. Estas particularidades hacen que un ataque o una vulnerabilidad tengan consecuencias asimétricas: mientras el agresor invierte recursos mínimos, la respuesta y mitigación suelen requerir esfuerzos y costos desproporcionados.

Este alcance es conocido como la superficie de ataque, entendida como la suma de los distintos puntos de acceso –o vectores de ataque– a través de los cuales un actor malicioso puede intentar penetrar un sistema y comprometer información o activos digitales (United States Government Accountability Office, 2024, p. 18). En un contexto marcado por la interconectividad permanente de dispositivos, redes y servicios; dicha superficie deja de ser local o delimitada y adquiere una dimensión transnacional, en la medida en que los ataques pueden originarse y desplegarse desde cualquier parte del mundo, con independencia de la ubicación del sistema afectado y de las motivaciones específicas del atacante.

Este fenómeno ha sido conceptualizado en la literatura especializada como ‘superficie de ataque global’. Al respecto, Hubbard y Seiersen advierten que esta comprende el conjunto agregado de vulnerabilidades existentes a lo largo de todos los sistemas, redes y organizaciones interconectadas, configurando un entorno de riesgo sistémico en permanente expansión (2016, p. 10). Se trata, así, de una realidad estructural del ciberespacio contemporáneo que no solo ha llegado para quedarse, sino que redefine los parámetros tradicionales de seguridad, responsabilidad y protección de derechos en el entorno digital.

Dada la magnitud de los riesgos –operativos, reputacionales y legales– y la creciente sofisticación de las amenazas (*malware*, ingeniería social, *advanced persistent threats* –APTs–, *astroturfing*, etc.), resulta imprescindible adoptar un enfoque holístico de gestión de riesgos. Este enfoque se basa en marcos reconocidos internacionalmente en la distribución de responsabilidades desde el nivel operativo hasta la alta dirección; en procesos continuos de evaluación de vulnerabilidades y en planes integrales de respuesta y recuperación ante incidentes.

Las amenazas cibernéticas se componen de todo aquello que puede causar daños o pérdidas a una persona (natural o jurídica), aprovechando las vulnerabilidades de los sistemas de información o las medidas de ciberseguridad de una organización. Como he identificado anteriormente (Núñez, 2025, p. 18-19), existen cuatro tipos de amenazas cibernéticas:

- a) **Amenazas externas impremeditadas:** son aquellas que ocurren accidentalmente –ya sea por impericia, negligencia o simple descuido– en la relación de la organización con agentes externos, como terceros, socios comerciales, exempleados, entre otros, que en el lenguaje técnico se conocen como *third-party vendors* (TPV). Aunque no existe la intención de causar daño, este igual se produce y persiste.
- b) **Amenazas externas premeditadas:** son actos dolosos perpetrados por agentes externos con la intención de obtener accesos no autorizados a los sistemas de información críticos de una organización con fines ilícitos, para provecho personal o ideológico. Pueden involucrar a un TPV, a un exempleado insatisfecho u otros agentes criminales.
- c) **Amenazas internas premeditadas:** son actos dolosos cometidos por personas internas a la organización, con la intención de acceder de manera no autorizada a los sistemas de información –críticos o no– con fines ilícitos, buscando provecho personal o ideológico.
- d) **Amenazas internas impremeditadas:** son actos accidentales realizados por personas internas a la organización que pueden afectar negativamente a los sistemas, redes o datos, como consecuencia de negligencias, impericias o errores humanos. Aunque no exista intención de causar daño, este igualmente se produce y persiste.

Las amenazas cibernéticas deben analizarse junto con los riesgos cibernéticos para realizar un análisis integral de las vulnerabilidades que son aprovechadas por los cibercriminales, quienes las explotan con el objetivo de obtener un provecho ilícito. A diferencia de las amenazas cibernéticas, los riesgos cibernéticos son aquellos daños, pérdidas o interrupciones en las operaciones comerciales generadas por el uso de sistemas de tecnologías de la información. Estos riesgos se dividen en tres grupos principales que a menudo son pasados por alto por las gerencias empresariales al realizar un estudio de contingencias (Falco & Rosenbach, 2022, p. 6):

- a) **Riesgos operacionales empresariales:** potenciales pérdidas directas o indirectas causadas por el personal o por el colapso (*downtime*) de sistemas empresariales clave, procesos o procedimientos.
- b) **Riesgo reputacional:** potenciales pérdidas o daños causados a la reputación o imagen pública de una organización o persona.
- c) **Riesgos legales y de cumplimiento:** potenciales pérdidas o daños derivados de acciones legales en contra de una empresa o persona por haber infringido alguna ley o marco normativo –ya sea por usuarios o entidades reguladoras–, así como responsabilidad civil, administrativa o penal.

Todo este panorama de riesgos y amenazas cibernéticas ponen al ser humano en constante y patente peligro, ya que, en cualquier momento y desde cualquier lugar, puede ser objeto de un ciberataque a su integridad y activos digitales. He, ahí, la necesidad de contar con una ciberseguridad idónea.

Esta disciplina puede ser intimidante por su naturaleza eminentemente técnica y debido al sinfín de definiciones sobre el particular (Núñez, 2025, pp. 29-30). Sin embargo, como he desarrollado en publicaciones anteriores (Núñez, 2024), compartimos la tesis del European Union Agency for Network and Information Security en que no es necesario definir a la ciberseguridad y que, en todo caso, deben brindarse definiciones contextuales

que encajen el modelo que se le quiera dar en cada documento técnico y dependiendo del ámbito que se quiera proteger:

No es necesaria una definición de la ciberseguridad en el sentido convencional que solemos aplicar a las definiciones de cosas sencillas como la autenticación de una identidad (un mecanismo de seguridad que permite verificar la identidad proporcionada). El problema es que la ciberseguridad es un término envolvente, no siendo posible elaborar una definición que abarque todo lo que realmente engloba este término. Por ello, debería considerarse una definición contextual, basada en una que sea relevante, encaje y que ya esté siendo utilizada por una organización o SDO³ en concreto (2015, p. 28). (Citado en Núñez, 2024) [traducción libre]⁴

En ese sentido, más que brindar una definición adicional a las ya existentes, las cuales son altamente técnicas y consensuadas entre naciones, así como entre organismos nacionales e internacionales; consideramos que debemos guiarnos por el análisis o entendimiento de toda persona sobre la ciberseguridad, como la búsqueda de maneras y buenas prácticas que garanticen un uso seguro de las computadoras, redes o sistemas, y, a su vez, permitan salvaguardar la información contenida, a fin de asegurar la confidencialidad, integridad y disponibilidad (*CIA Triad*⁵)

Debido a la patente interconectividad al internet de las personas –tanto naturales como jurídicas–,

³ Un SDO es una *Standard Developing Organization* que tiene como finalidad desarrollar y aprobar estándares técnicos consensuados, tales como el ISO/IEC o la ITU-T (Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones).

⁴ Texto original:

There does not need to be a definition for Cybersecurity in the conventional sense that we tend to apply to definitions for simple things like authentication of an identity (a security mechanism allowing the verification of the provided identity). The problem is that Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers.

Therefore, a contextual definition, based on one that is relevant, fits, and is already used a particular SDO or organization should be considered. (European Union Agency for Network and Information Security, 2015, p. 28)

⁵ Es un estándar técnico de aplicación universal que busca garantizar, como mínimo, tres principios fundamentales en la seguridad de la información. Estos principios, como se podrá apreciar, también se presentan como bienes jurídicos protegidos en el Derecho Interno:

- a) **Confidencialidad (*confidentiality*):** se refiere a la prevención del acceso no autorizado a información privada o sensible. Como se mencionó anteriormente, el acceso puede ser malicioso o intencionado –como cuando un agente, interno o externo, ingresa sin autorización a los sistemas y accede a la información–, o imprevisto –cuando un agente, interno o externo, debido a descuido, impericia o negligencia, genera una vulnerabilidad o filtra información–. En pocas palabras, la confidencialidad busca mantener la información privada o sensible fuera del alcance de personas no autorizadas.
- b) **Integridad (*integrity*):** hace referencia a la consistencia de los sistemas, redes y datos, asegurando que no sufran alteraciones no autorizadas o no intencionadas. Esto garantiza que los sistemas, redes y datos funcionen según lo previsto cuando un usuario autorizado accede a ellos, evitando que se borren o modifiquen de manera indebida. Lo esencial es que la información se mantenga tal como la organización la necesita (sin adiciones ni eliminaciones no autorizadas), evitando modificaciones o supresiones no autorizadas.
- c) **Disponibilidad (*availability*):** la disponibilidad se refiere a la capacidad de los usuarios autorizados para acceder a sus sistemas, redes o datos cuando lo necesiten. Es decir, garantiza el acceso inmediato a los recursos cuando sea necesario para los fines correspondientes. (Núñez, 2024)

el desarrollo de la sociedad ha variado de un aspecto físico a uno cibernético, siendo que ahora existen peligros que nunca antes habríamos considerado: la violación sexual en el metaverso⁶, atentados contra la integridad sexual y dignidad de una persona sobre la base *deepfakes* o *revenge porn*, la muerte de personas por un ataque de ransomware a una clínica que genera *downtime* en los sistemas críticos⁷, o ataques a sistemas de control industrial Supervisory Control and Data Acquisition con el fin de detener sectores críticos de industrias en un país, como manifestación del *cyberwarfare*⁸.

Las ciberamenazas han trascendido a lo meramente técnico y ahora vulneran directamente derechos fundamentales. Precisamente por ello es que la ciberseguridad es importante, pues puede mitigar y hasta evitar daños catastróficos con la adopción de medidas adecuadas. Por esa razón es que debemos darle la importancia debida a esta materia y entender su impacto constitucional en la sociedad, debiendo ser el enfoque desde un ámbito de protección iusfundamental y emplearlo como una herramienta para lograr el fin perseguido: asegurar la libertad y dignidad de la persona humana y el desarrollo de su proyecto de vida en el quinto dominio.

III. LOS NUEVOS DERECHOS DEL CIBERESPACIO: LOS DERECHOS DE CUARTA GENERACIÓN

Con el acceso irrestricto al internet, la interacción cotidiana del ser humano ha cambiado radicalmente como consecuencia del desdibujamiento de los límites entre el mundo físico y el ciberespacio. Antes era imposible pensar que uno pasaría más tiempo en el ciberespacio que en la realidad física, pero esa impensable premisa se ha vuelto nuestra realidad. Consecuentemente, el derecho debe proteger esta nueva forma de interacción mediante limitaciones y garantías que permitan

el uso seguro de este nuevo estilo de vida. La ciberseguridad no es un agregado tecnológico o una disciplina baladí; todo lo contrario: es una condición estructural para el ejercicio de –casi– todos los derechos fundamentales, desde la primera generación hasta la cuarta.

Y esta nueva realidad no es exclusiva de las personas naturales; las personas jurídicas, en su calidad de actores activos del entorno virtual, también requieren garantías efectivas para operar, proteger su integridad y relacionarse jurídicamente dentro de un ciberentorno seguro. En este contexto, los derechos digitales de cuarta generación emergen como respuesta a las transformaciones sociotécnicas del siglo XXI, y la ciberseguridad constituye el eje transversal que garantiza su plena efectividad y goce.

Si la red es el nuevo espacio público y privado, entonces la protección frente a ataques, fraudes, filtraciones de datos, manipulación algorítmica o vigilancia no autorizada; resulta esencial para preservar la dignidad, autonomía y existencia digital de los sujetos. Para poder determinar su naturaleza de derecho, la doctrina ha fijado dos criterios: el ‘criterio objetivo’, que define cómo es que estos nuevos derechos se dirigen a resolver un problema de la sociedad actual; y el ‘criterio subjetivo’, que se centra en un sector de la población que ha pasado desapercibido hasta entonces (Riofrío, 2014, pp. 17-18). La conclusión de Riofrío es útil para introducir este tema:

La posibilidad de que exista una cuarta generación de derechos humanos relacionada con el mundo digital está condicionada al cumplimiento de estos dos criterios. En cuanto al criterio objetivo, es muy probable que las peculiares características del mundo digital sean capaces de dotar a los derechos de siempre

⁶ Véase a Sales (2024). El caso de la menor de dieciséis años que en el año 2024 fue víctima de violación sexual virtual en grupo en el metaverso.

⁷ Lamentablemente, existen casos trágicos así. Uno de ellos tuvo como víctima a Nicko Silar, un bebé que justo nació justo cuando el Springhill Medical Center fue atacado por un *ransomware*. Debido a que los sistemas de la clínica habían caído por el ciberataque, el personal médico no pudo acceder a la historia clínica de la madre ni monitorear los signos vitales de ella y del bebé. Como resultado, no pudieron detectar que el cordón umbilical estaba ahorcando a Nicko. Aunque nació, el daño causado por la sofocación resultó en un daño cerebral irreparable, que le costó la vida nueve meses después. Todo esto fue consecuencia de un ataque a un sistema informático médico (Srinivasan & Ni, 2023). Otro caso ocurrió en Düsseldorf, Alemania, en septiembre de 2020. El Hospital de la Universidad de Düsseldorf fue atacado por un *ransomware*, lo que hizo que los sistemas del hospital dejaran de funcionar, incluyendo el sistema encargado de admitir pacientes en emergencias. Lamentablemente, durante ese ataque, una mujer de 78 años, afectada por un aneurisma aórtico, sufrió un deterioro de salud que motivó su traslado de emergencia para recibir atención médica urgente. El centro médico más cercano era el Hospital de la Universidad de Düsseldorf. Sin embargo, al informar sobre la llegada de esta paciente, no pudieron admitirla debido al ciberataque –se informó que no estaban atendiendo emergencias–, por lo que se rechazó su ingreso y se redirigió la ambulancia al Hospital Universitario Helios de Wuppertal, a 32 kilómetros de distancia, lo que retrasó una hora el tratamiento de la paciente. Lamentablemente, murió poco después (Ralston, 2020).

⁸ Entre otros casos, véase a Styczynski & Beach-Westmoreland (2019). Notable ciberataque de Rusia a los sistemas de generación eléctricas ucranianos el 23 de diciembre de 2015 que causó un apagón masivo que afectó a 225,000 personas.

una configuración del todo especial que los distinga. Más adelante se analizará con mayor detenimiento este asunto. Respecto al criterio subjetivo, parece casi evidente que los ciudadanos del mundo virtual (los cibernautas) no cuentan hoy con instrumentos jurídicos suficientes capaces de proteger sus derechos con algún grado de eficacia. Todavía puede decirse que, en buena medida, internet es una tierra de todos y de nadie.

En conclusión, es pertinente mencionar que la aparición y vigencia de los derechos tradicionales en el mundo virtual adquiere una amplia gama de matices nunca antes vistos, cuya protección resulta muy deficiente en la actualidad. Ha aparecido en el siglo XX un grandísimo sector de la sociedad desprotegido que debe redimirse. Estos elementos bastarían para poder hablar con justicia de una nueva generación de derechos humanos. (2014, p. 18-19)

De manera esquemática vamos a ver cuáles son estos nuevos derechos digitales y su contenido esencial. Lo anterior deberá entenderse como derechos constitucionales de configuración legal, los cuales han sido definidos por el Tribunal Constitucional en la sentencia recaída en el Expediente 04138-2016-PA/TC, fundamento jurídico 22:

El contenido y la efectividad [de los derechos] requiere[n] ser concretado[s] y regulado[s] por ley. En tal sentido, puede afirmarse que se trata de un derecho de configuración legal. Ciertamente, el legislador cumple con su rol al definir mediante ley la política social dentro de un Estado social y democrático de Derecho, así como el Gobierno cumple con las suyas cuando elabora las regulaciones que le corresponden (directivas y reglamentos) las cuales contienen políticas públicas, siempre bajo los márgenes legales y constitucionales. (2020)

Este proceso de reconocimiento y concreción normativa de los derechos fundamentales en el ciberespacio, encuentra su fundamento directo en el artículo 3º de la Constitución que consagra una cláusula abierta de derechos fundamentales al reconocer aquellos que; aun no estando expresamente enumerados en el texto constitucional, se derivan de la dignidad de la persona humana, de los principios del Estado Democrático de Derecho y de la soberanía del pueblo. Lejos de tratarse de una disposición residual o meramente programá-

tica, el artículo 3 cumple una función estructural dentro del sistema constitucional, en tanto impide que el catálogo de derechos quede petrificado en las categorías históricas vigentes al momento de promulgación de la carta de 1993 y habilita su adaptación a nuevas realidades sociales, económicas y tecnológicas.

Desde esta perspectiva, la Constitución no impone una lógica de autorrestricción interpretativa que obligue a circunscribir los derechos fundamentales a los ámbitos de ejercicio imaginables en 1993. Por el contrario, el artículo 3 opera como una auténtica norma de habilitación dinámica que permite ampliar, proyectar y reconfigurar el alcance de los derechos fundamentales existentes; de modo que, estos puedan desplegarse eficazmente en contextos no previstos por el constituyente, como el ciberespacio. Así, derechos clásicos como la privacidad, la libertad de expresión, la identidad personal o la tutela jurisdiccional efectiva no se agotan en su formulación tradicional; sino que adquieren nuevas manifestaciones, riesgos y exigencias cuando se ejercen a través de entornos digitales, plataformas tecnológicas e infraestructuras informáticas complejas.

No obstante, esta función adaptativa de la cláusula abierta de derechos no se limita a una reinterpretación extensiva de derechos previamente reconocidos. En determinados supuestos, las transformaciones tecnológicas generan riesgos, bienes jurídicos y formas de afectación que no pueden ser adecuadamente comprendidos ni protegidos mediante una simple proyección de categorías clásicas. En tales casos, el artículo 3 de la Constitución habilita también la identificación y construcción dogmática de nuevos derechos fundamentales, en la medida en que estos resulten necesarios para salvaguardar la dignidad humana y asegurar condiciones reales de libertad e igualdad en el ciberespacio.

En este marco, los denominados derechos digitales o derechos de cuarta generación no constituyen creaciones arbitrarias ni expansiones infundadas del catálogo constitucional, sino respuestas constitucionalmente legítimas a escenarios de ejercicio de derechos radicalmente distintos a los tradicionales. El derecho a la ciberseguridad, en particular, se presenta como una manifestación paradigmática de esta lógica evolutiva: un derecho que no solo proyecta garantías clásicas, sino que emerge como una categoría autónoma orientada a

⁹ Artículo 3.-

La enumeración de los derechos establecidos en este capítulo no excluye los demás que la Constitución garantiza, ni otros de naturaleza análoga o que se fundan en la dignidad del hombre, o en los principios de soberanía del pueblo, del Estado democrático de derecho y de la forma republicana de gobierno. (1993)

preservar las condiciones estructurales –técnicas, organizativas y normativas– que hacen posible el ejercicio efectivo de los derechos fundamentales en el ciberespacio. De este modo, el artículo 3 de la Constitución actúa como el puente normativo que conecta la teoría constitucional clásica con la realidad digital contemporánea; asegurando que el sistema de derechos fundamentales mantenga su vigencia, coherencia y eficacia en un contexto de transformación tecnológica permanente.

Esta comprensión dinámica de los derechos fundamentales explica que los derechos digitales, en tanto expresión contemporánea de la dignidad humana en el entorno digital, hayan encontrado un reconocimiento y desarrollo progresivo en el ordenamiento jurídico nacional. No solo han sido objeto de regulación específica mediante normas con rango de ley o disposiciones infralegales, sino que también han sido interpretados y perfilados a través de la jurisprudencia del Tribunal Constitucional, el cual ha reafirmado su naturaleza de derechos fundamentales de configuración legal. Ello implica que su contenido esencial, sin dejar de estar protegido por el bloque de constitucionalidad, requiere de una concreción normativa por parte del legislador, quien debe garantizar su ejercicio efectivo en armonía con los principios del Estado Social y Democrático de Derecho.

Asimismo, resulta relevante destacar que el derecho nacional ha comenzado a incorporar, de forma explícita o implícita, principios y estándares provenientes de la denominada *lex mercatoria* digital, tales como la neutralidad de la red, la portabilidad de los datos, la autodeterminación informativa, la interoperabilidad o la transparencia algorítmica. Esta progresiva integración normativa no solo evidencia una voluntad estatal de responder a las exigencias del entorno digital globalizado, sino que confirma el carácter dinámico, evolutivo y no autorre restrictivo del sistema de derechos fundamentales en la era digital.

En consecuencia, no nos encontramos ante derechos meramente accesorios ni ante manifestaciones secundarias del constitucionalismo contemporáneo, sino frente a verdaderos derechos fundamentales cuya tutela resulta indispensable para asegurar la plena vigencia de los valores democráticos, la libertad individual y la justicia social en el nuevo escenario digital.

Antes de abordar el análisis individual de los derechos fundamentales en el ciberespacio, es necesario precisar una advertencia metodológica. El desarrollo de cada derecho no responde a un criterio uniforme de extensión, sino a su distinto grado de autonomía conceptual, densidad constitucional

y nivel de consolidación doctrinal. En ese sentido, algunos derechos –como la existencia digital, la identidad digital o la reputación en línea– reciben un tratamiento más amplio por constituir categorías estructurales del estatuto jurídico de la persona en el entorno digital, mientras que otros se presentan de manera más sintética en atención a su carácter instrumental, derivado, o aún incipiente, desde el punto de vista dogmático.

Cabe subrayar que esta diferenciación no implica una jerarquización de derechos, sino una opción metodológica orientada a destacar aquellos que permiten comprender de manera más clara la transformación del paradigma constitucional en la era digital, sin perjuicio de que el desarrollo dogmático de otros derechos digitales continúe evolucionando en función de los cambios tecnológicos y sociales.

A. El derecho a existir digitalmente

Es el derecho de génesis, el presupuesto *sine qua non* de todos los derechos digitales. La razón es sencilla: mientras uno no pueda existir en el ciberespacio, no podrá ejercer ninguno de los derechos digitales. No se le debe considerar como el simple acto de conectarse, por el contrario, este derecho implica un reconocimiento jurídico y técnico de la personalidad del sujeto en un espacio que, a diferencia del entorno físico, es construido y sustentado por infraestructuras tecnológicas.

Sin esta agencia, la persona se convierte en un ente inexistente, invisible e inoperante, incapaz de acceder a servicios, de participar en transacciones o de ejercer otros derechos, por ejemplo: a la identidad, reputación, participación en la vida social, etc. La continuidad de esta existencia digital debe entenderse con vocación de permanencia. Así como la personalidad física persiste a lo largo del tiempo, la existencia en el ciberespacio requiere mecanismos de preservación frente a la obsolescencia, la pérdida de credenciales o el cierre de plataformas.

El contenido esencial de este derecho es claro y directo: se debe poder contar con la capacidad para existir y operar en el ciberespacio, pues sin esta existencia digital no se podrán ejercer ni gozar de los derechos en dicho entorno. En ese sentido, el núcleo duro siempre deberá comprender una garantía de existencia con vocación de permanencia, pues el entorno digital existirá mientras la sociedad exista, siendo obligación del Estado asegurar las condiciones para que ello se mantenga así. Esta protección no puede ser efímera ni condicional y bifurca obligaciones del Estado, así como de privados.

Por un lado, el Estado tiene la obligación positiva de: (i) proveer y regular infraestructuras de acceso universal a internet y servicios de autenticación (certificados digitales, pasarelas de identidad, etc.), garantizando una conectividad resiliente; (ii) establecer protocolos de preservación de datos y credenciales de identidad electrónica para evitar la desaparición o corrupción de los registros que sustentan la existencia digital; y, por último, (iii) implementar marcos normativos que obliguen a las plataformas de relevancia a mantener registros de usuarios y mecanismos de recuperación de cuentas tras contingencias (caídas de servicio, migraciones tecnológicas, quiebras empresariales, entre otros).

Respecto al privado, este comparte con el Estado las siguientes obligaciones negativas: (i) prohibir el bloqueo, suspensión o cancelación arbitraria de cuentas sin el debido proceso digital, con notificación previa y derecho de audiencia; (ii) sancionar el *account hijacking* (toma de cuentas) y la suplantación de identidad, imponiendo responsabilidades civiles y penales a quienes vulneren la existencia digital ajena; y (iii) prevenir políticas de diseño o prácticas de negocio (por ejemplo, vendor *lock-in* o discontinuidad de APIs –interfaz de programación de aplicaciones– y obsolescencia) que impidan al usuario trasladar o reconstruir su presencia digital en otras plataformas.

De alguna u otra manera, esto lo encontramos regulado en el segundo párrafo del artículo 2.4¹⁰ de la Constitución al prescribir la obligación del Estado de promover “[...] el uso de las tecnologías de la información y la comunicación en todo el país” (1993). Si bien esta norma iusfundamental recién se dio el 23 de setiembre de 2024, con la modificación causada por la Ley 31878, el enfoque que fluye del texto sobre la promoción del uso de la tecnología para garantizar la libertad de información es limitado y restrictivo de cara al avance y uso profundo del ciberespacio. Esta garantía deberá entenderse, en realidad, como la obligación estatal de promover el uso de la tecnología para garantizar el acceso irrestricto y libre de toda persona –sea natural o jurídica– al ciberespacio con las garantías antes descritas.

B. El derecho a la identidad digital

El derecho a la identidad digital garantiza que una persona que existe en el ciberespacio pueda ser caracterizada e identificada como esta desee exteriorizar su personalidad y gustos. Así como en la dimensión física, podemos adoptar apodos o pseudónimos, formas de hablar, expresiones, vestimentas, accesorios, tatuajes, alusiones hereditarias o genéticas, etc. Lo mismo ocurre en el ciberespacio.

Estudiosos de la materia, como Lin y Latoschik (2022, p. 2), han desarrollado este derecho expresando que la representación gráfica de las personas en el mundo virtual, mediante un *avatar*, constituye su ‘persona digital’ que hace las veces de la que la controla en el mundo físico. De esta manera se presentan tres tipos de alternativas de ‘autorrepresentación’ en el metaverso que influyen en el modo de evidenciar la identidad digital:

- a) Avatares prefabricados o de selección libre: se eligen entre una amplia variedad de opciones preestablecidas o incluso subir modelos creados por los propios usuarios, como ocurre en plataformas como *VRChat*, donde es posible representarse como personajes de estilo caricaturesco, criaturas fantásticas, robots, entre otros.
- b) Avatares altamente personalizables: en los que el usuario puede modificar color, forma y estilo de distintas partes del cuerpo (rostro, cabello, ojos, piel, marcas de piel, lunares, arrugas, etc.), reflejando características como género, raza, estética e intereses personales. Este tipo es común en entornos como *RecRoom*, *AltspaceVR* o *Baldur’s Gate*.
- c) Avatares hiperrealistas o fotorrealistas (autorreferenciales): buscan reproducir con precisión la apariencia física real del usuario, lo cual es una tendencia cada vez más presente en entornos sociales virtuales contemporáneos. Aunado a la apariencia física del avatar, las personas se identifican también con el nombre (*user*) que hará las veces de su nombre en el ciberespacio.

¹⁰ Artículo 2.- Toda persona tiene derecho a:

[...]

4. Las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley.

El Estado promueve el uso de las tecnologías de la información y la comunicación en todo el país. Los delitos cometidos por medio del libro, la prensa y demás medios de comunicación social se tipifican en el Código Penal y se juzgan en el fuero común.

Es delito toda acción que suspende o clausura algún órgano de expresión o le impide circular libremente. Los derechos de informar y opinar comprenden los de fundar medios de comunicación. (1993)

Dicho ello, el derecho a la identidad digital consiste en la facultad de poder, libre y voluntariamente, configurar, controlar y proteger los atributos y signos distintivos que permiten al sujeto ser reconocido y diferenciado en el entorno virtual. No se agota en la mera asignación de un nombre o un *avatar*, sino que comprende la autenticación segura, la integridad de los datos del perfil y la facultad de modificarlos conforme a la voluntad del titular en consonancia con el dinamismo propio de su identidad.

Este no es un simple reconocimiento baladí o lúdico. Un notable ejemplo que ratifica la importancia de la identidad digital es el caso de Mats Steen, mejor conocido en la comunidad de World of Warcraft como Ibelin Redmoore. Esta situación, reflejada en el documental noruego “La notable vida de Ibelin” (Ree, 2024) [traducción libre]¹¹, ilustra de manera excepcional cómo el derecho a la identidad digital trasciende lo meramente estético o recreativo para convertirse en un verdadero derecho a la autodeterminación y de ciudadanía en el ciberespacio. A pesar de vivir con distrofia muscular de Duchenne, Steen pudo configurarse a sí mismo un *avatar* plenamente habilitado —una figura esbelta, musculosa y con armadura— que encarnaba no solo sus aspiraciones en el juego, sino también su personalidad empática y colaborativa.

Bajo la identidad digital de Ibelin Redmoore, Steen estableció una red global de amistades profundas: compartía risas y confidencias con jugadores de todo el mundo, se enamoró por primera y única vez en su vida, y hasta pudo tener un trabajo como ‘investigador privado’. Cada interacción en Azeroth (planeta ficticio), reforzaba su sentido de pertenencia y reconocimiento como un igual; al mover su cuerpo virtual con la agilidad que su condición física le negaba, experimentó la camaradería sin barreras y todas las aventuras que implican los videojuegos de rol multijugador masivos en línea —*massively multiplayer online role-playing game*— (MMO-RPG). Su historia pone de relieve el factor humano del derecho a la identidad digital: la capacidad de forjar conexiones afectivas y profesionales, de extender los límites del propio cuerpo humano mediante la simulación virtual, y de ser reconocido gracias a la empatía y la solidaridad.

En su caso, la identidad digital no fue una mera persona, sino la construcción por casi una década de su verdadero ser y de su proyecto de vida; pudo experimentar emociones que, dada su condición física, nunca experimentaría al no ser considerado un igual en esta sociedad física (Fequiere, 2024). Gracias a la extensión que le brindó el ciberespacio, Steen pudo vivir en sus términos y desarrollarse en libertad. Su historia expone con crudeza cómo la identidad digital no es un mero accesorio visual o un entretenimiento efímero, sino una manifestación legítima de la personalidad humana y un vehículo esencial para el ejercicio de derechos fundamentales en el entorno virtual. Desde esta óptica, la identidad digital debe ser entendida como un bien jurídico autónomo y merecedor de protección integral, cuya afectación puede traducirse en un menoscabo directo a la dignidad, la libertad y la autodeterminación del individuo.

Así como en el mundo físico, toda persona debe respetar la identidad de la persona en el ciberentorno, siendo aplicables las mismas disposiciones que comprenden los alcances del artículo 2.1¹² de la Constitución¹³, tales como: (i) ser reconocido efectivamente como un sujeto titular de derechos; (ii) protección de nuestra integridad y autenticidad de las manifestaciones identitarias; (iii) acceso a mecanismos de tutela en caso de vulneración de nuestra identidad; y (iv) reconocimiento de cómo nos manifestamos en nuestro fuero interno.

Sin embargo, el contenido de este derecho no puede quedarse en las concepciones clásicas que la jurisprudencia ha desarrollado. Debemos considerar los elementos tradicionales del derecho a la identidad con la realidad del ciberespacio y buscar que se garantice, a su vez: (i) la creación de identificadores únicos (username, DID¹⁴, certificados digitales, entre otros); (ii) el mantenimiento de la exactitud y actualización de información personal y corporativa; (iii) la protección frente a la suplantación, falsificación o robo de credenciales; (iv) la interoperabilidad de sistemas de identidad que permita el reconocimiento mutuo entre plataformas; (v) la integridad digital; (vi) la portabilidad de la identidad digital; (vii) la protección *post mortem* de la identidad digital; y (ix) la adopción de estándares técnicos y sistemas de verificación

¹¹ Título original The remarkable life of Ibelin.

¹² Artículo 2.- Toda persona tiene derecho a: 1. A la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar. El concebido es sujeto de derecho en todo cuanto le favorece.

¹³ Véase las sentencias del Tribunal Constitucional recaídas en los Expedientes 04509-2011-PA/TC (fundamento jurídico 9); Expediente 02273-2005-PHC/TC (fundamento jurídico 13, 21 y 22); Expediente 1797-2002-HD/TC (fundamento jurídico 3); y Expediente 2333-2004-HC/TC (fundamento jurídico 2).

¹⁴ Acrónimo para *Decentralized Identifier* el cual es un estándar promovido por el World Wide Web Consortium que lo define como un formato de identificador global, único y verificable.

de identidad que respeten la privacidad del individuo –principio de *least revealing means*– (Abelson *et al.*, 1998).

C. El derecho a la estima, honor y reputación digital

Así como en el plano físico tenemos una reputación por las cosas que hacemos –siendo esta buena o mala dependiendo de nuestro accionar–, en el ciberespacio, el valor reputacional se edifica –o destruye– a través de publicaciones, valoraciones y, en general, comportamientos en línea. Un abogado procesalista de prestigio genera confianza entre sus clientes, de igual modo que un *seller* en plataformas de *e-commerce* como Amazon o Mercado Libre alimenta su prestigio con cada reseña y estrella recibida. En el ámbito del *gaming* ocurre lo mismo, tal como hemos visto el caso de Ibelin Redmoore, quien se forjó toda una identidad y fama gracias a su empatía en el juego de World of Warcraft. Sin embargo, esta misma reputación digital es vulnerable y, así como se puede construir, puede ser destruida. El caso de THQ Nordic, cuya sesión de preguntas y respuestas (AMA –*ask me anything*–) en 8chan en 2019 manchó su imagen corporativa y lo obligó a disculparse públicamente¹⁵ (Phillips, 2019).

Los alcances del contenido de este derecho fundamental siguen los pasos de lo desarrollado en el artículo 2.7¹⁶ de la Constitución, siendo que la tesis central es la protección de su titular en contra de agresiones a su autoestima y dignidad. Como lo ha desarrollado el Tribunal Constitucional en su sentencia recaída en el Expediente 4099-2005-AA/TC, fundamento jurídico 7:

[...] la Constitución hace referencia a dos dimensiones de protección de la dignidad humana, la primera referida a la persona en tanto que individuo dotado de inmunidad frente a cualquier agresión a su autoestima y su dignidad objetivada como ser libre e igual a los demás; la segunda como ser que forma parte de

un grupo social y se relaciona cotidianamente con sus semejantes. Mientras que la dimensión del honor individual se refiere a un derecho personalísimo indelegable, en su dimensión de buena reputación, el honor se expande como una posición iusfundamental que puede también ampliar sus efectos para proteger posiciones similares no solo de personas naturales, sino incluso en los entes que, amparados en alguna manifestación de personalidad jurídica que les confiere el sistema jurídico, actúan en la sociedad proyectando una imagen o un nombre o una ‘razón social’. (2006)

A la fecha, y con el uso de la inteligencia artificial, se han generado nuevas formas de atacar contra el honor y reputación de las personas. Por ejemplo, Silva y Pinheiro, refiriéndose a la violencia moral en el contexto de la difusión no autorizada de material audiovisual sexual en portales web destinados a la prostitución, deprecia su honor e imagen pública, causándole vergüenza y mermando su autoestima (2021). Lo mismo ocurre con los *deepfakes* de índole sexual. Según The Duc Tam, estas formas de ciberataques causan humillación y dañan la reputación de la víctima (2022, p. 30). Lo mismo sucede con el *cyberbullying*, el acto de usar medios de comunicación electrónica para acosar a una persona mediante el envío de mensajes intimidatorios o amenazantes (Agrawal & Bhattar, 2022, p. 141); el *cyberstalking*¹⁷, el acto de usar medios tecnológicos para perseguir y acosar indeseadamente a víctimas (Atta, 2022, p. 97); el *trolling*, una forma colectiva de acoso malicioso diseñada para provocar a otro usuario (Ortiz, 2020, pp. 2-3); o el *doxxing*, la difusión no autorizada de información personal de una persona (Dunn, 2020, p. 13).

Todos estos actos ocurridos en el ciberespacio pueden generar repercusiones en el plano físico. Recordemos el lamentable suicidio de la estrella de K-Pop Goo Hara (BBC News Mundo, 2019) quien se suicidó luego de enterarse de que un médico la había grabado mientras se cambiaba de ropa en un hospital local (Pevac, 2022); o el muy

¹⁵ Este es un ejemplo notable de una empresa que ha sufrido una crisis de reputación digital debido a su conducta en el ciberespacio. En 2019, la compañía organizó una sesión de preguntas y respuestas en 8chan, un sitio web conocido por alojar pornografía infantil y discursos de odio. Esta decisión generó una ola de críticas y dañó significativamente la imagen de la empresa, obligándola a emitir disculpas públicas y distanciarse del evento.

¹⁶ Artículo 2.- Toda persona tiene derecho:

[...]

7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agravada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley. (1993)

¹⁷ Desde el año 2015, la Asamblea General de las Naciones Unidas en la Resolución adoptada por el Consejo de Derechos Humanos del 2 de julio de 2015, ha reconocido al *cyberbullying* y al *cyberstalking* como formas de violencia contra la mujer y, de más está decir, contra el ser humano en general.

famoso caso de Amanda Todd¹⁸ quien se suicidó en el año 2014 luego de ser víctima de ‘sextorsión’ por un sujeto quien la amenazó de difundir material audiovisual de sus partes íntimas en una red social (Hainsworth, 2014).

Claramente, la concepción clásica del derecho al honor no contemplaba todos estos atentados en contra de la buena reputación de una persona, máxime cuando estas ocurren en un plano que trasciende a nuestra realidad –en el quinto dominio– y en una en la cual el constituyente nunca imaginó que podría ocurrir algo así. Por ello, dentro del contenido esencial de este derecho se deberá de considerar lo siguiente:

- a) El reconocimiento y protección legal del honor y reputación digital como una extensión de la dignidad humana, comprendiendo tanto la forma en que la persona se proyecta al ciberespacio como la percepción colectiva que se construye en torno a su accionar digital.
- b) La garantía de mecanismos eficaces y expeditivos de rectificación, respuesta o eliminación frente a publicaciones, valoraciones, calificaciones, imágenes, montajes o cualquier otro contenido digital que menoscabe de manera ilegítima la estima, honor o reputación del sujeto, ya sea persona natural o jurídica. Para ello, se tiene el *hábeas data* o proceso de amparo.
- c) La implementación de estándares normativos para las plataformas de relevancia sistémica, a fin de que incluyan herramientas de verificación, moderación proactiva y trazabilidad, con el objeto de impedir la proliferación de contenidos agravantes, falsos o dolosos que afecten injustificadamente la reputación de los usuarios.
- d) El derecho a ser informado y participar activamente en procesos que afecten la valoración pública de su persona digital, tales como sistemas de puntuación, reseñas o métricas algorítmicas, con posibilidad de oposición, corrección o supresión conforme a los principios del debido proceso digital.
- e) La tutela contra formas contemporáneas de violencia reputacional, como los ataques coordinados, campañas de difamación automatizadas (*bots*), *deepfakes* denigrantes,

manipulación algorítmica con fines discriminatorios, *astroturfing*, entre otros; estableciendo la responsabilidad entre autores, difusores y facilitadores tecnológicos.

- f) La previsión de medidas de reparación simbólica, económica o social en casos de daño reputacional grave, garantizando una respuesta que recupere la integridad moral de la víctima en el entorno digital y fuera de él.

Solo asegurando el respeto a la estima, el honor y la reputación digital, se protege, auténticamente, la condición de dignidad de la persona en el ciberespacio. Tal como lo exige nuestra Constitución para el plano físico, es necesario que se repliquen estas garantías, *mutatis mutandis*, al ciberespacio como una exigencia contemporánea que enfrenta nuestro Estado Constitucional y Democrático de Derecho.

D. El derecho a la libertad y responsabilidad digital

Como mencionamos previamente, una de las características del ciberespacio es que no existen barreras físicas. En palabras de Lessig, el ciberespacio no está limitado por las fronteras físicas ni geográficas del mundo real, ya que ‘el código es la ley’ que regula el espacio digital y puede moldear o eliminar barreras tradicionales, permitiendo una interconectividad global sin precedentes (1999, p. 201).

De esta manera, puedo comunicarme a cualquier hora, desde cualquier lugar, con quien yo desee; puedo visitar otros continentes con la ayuda de un programa e, incluso, puedo viajar al espacio o al fondo del océano y ver cómo se exploran las profundidades. Podemos, desde una clase universitaria –mientras tomamos apuntes, claro está–, jugar un videojuego masivo con personas de todos los continentes y, en paralelo, ver en tiempo real las cámaras del cuarto de nuestro hijo para ver qué está haciendo. El acceso irrestricto al ciberespacio amplifica exponencialmente nuestra capacidad de expresión y acceso al conocimiento.

Precisamente, la libertad digital engloba a la de expresión, pues permite que cualquier usuario exprese su punto de vista sobre cualquier materia sin mordaza –salvo en determinados países– o sometido a la línea de ninguna editorial. El internet pone en primera plana nuestros pensamientos y permite que resuenen en todo el planeta tierra mientras

¹⁸ Hasta ahora se encuentra su video en YouTube, en donde la desaparecida Todd, cuenta su historia antes de suicidarse. Véase a GATOYRATÓN, soluciones para el acoso escolar (2015).

se tenga acceso a él. De esa manera, esta libertad incluye tanto el derecho a transmitir ideas, contenidos y opiniones sin censura arbitraria, como el acceso irrestricto a servicios, plataformas y redes de información.

Esta libertad, sin embargo, no garantiza el libertinaje, sino al acceso sin obstáculos de la manera en cómo el individuo digital decide ejercer esta autonomía. Esta ausencia de obstáculos, como garantía negativa del Estado y del privado, hace referencia al principio digital de *net neutrality* definido por Wu como el principio según el cual los proveedores de servicios de internet (*Internet Service Provider*), deben tratar todos los datos en el internet de la misma manera, sin discriminar ni cobrar de forma diferente según el usuario, contenido, sitio web, plataforma, aplicación o método de comunicación (2003, pp. 149-151).

Este principio ha sido positivizado en el Perú en el artículo 6 de la Ley 29904, Ley de promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, estableciendo lo siguiente:

Los proveedores de acceso a Internet respetarán la neutralidad de red por la cual no pueden de manera arbitraria bloquear, interferir, discriminar ni restringir el derecho de cualquier usuario a utilizar una aplicación o protocolo, independientemente de su origen, destino, naturaleza o propiedad. El Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL determina las conductas que no serán consideradas arbitrarias, relativas a la neutralidad de red. (2015)

A mayor abundamiento, el artículo 10.1 del Decreto Supremo 014-2013-MTC, Reglamento de la Ley 29904 establece lo siguiente:

Los Proveedores de Acceso a Internet y los Operadores de Telecomunicaciones, no podrán limitar el derecho de un usuario a incorporar o utilizar cualquier clase de dispositivo o equipo terminal en la red, siempre que los mismos se encuentren debidamente homologados, no dañen o perjudiquen la red, y sean técnicamente compatibles con la red. Asimismo, los Operadores de Telecomunicaciones no deberán restringir, bloquear o inhabilitar arbitrariamente funciones o características originales de los dispositivos o equipos terminales que comercialicen en el territorio nacional, que impidan el libre uso de protocolos, aplicativos o servicios de Banda Ancha. (2013)

Esta libertad de neutralidad se debe de poder ejercer en igualdad de condiciones y evitar la discriminación al acceso digital, la cual es definida por la

Comisión Federal de Comunicaciones de los Estados Unidos como políticas o prácticas, no justificadas por problemas genuinos de viabilidad técnica o económica, que afectan de manera diferencial el acceso de los consumidores al servicio de internet de banda ancha en función de su nivel de ingresos, raza, etnia, color, religión u origen nacional, o que tienen la intención de tener tal impacto diferencial (2024, p. 4128).

Sin embargo, como todo derecho, esta libertad digital es limitada, pues su contrapeso lo sienta la responsabilidad digital. Como toda garantía constitucional, debe ser ejercida y gozada de manera armónica con los valores y principios de la sociedad; tal como lo haría un ciudadano en el plano físico. Por ejemplo, no por tener amplia libertad de expresión vamos a proferir mensajes de odio o incurrir en prácticas de *cyberbullying*. Del mismo modo, no por poder compartir imágenes irrestrictamente en tiempo real con otras personas vamos a dañar a otra persona mediante el *revenge porn*. Toda libertad ejercida en el ciberespacio debe ser equilibrada con la responsabilidad digital y la máxima de *neminem laedere*. Recordemos las premisas fijadas por Escobar de la Serna cuando comentaba la responsabilidad en el internet:

Responsabilidad significa la obligación de responder de los propios actos y de reparar y satisfacer al afectado —sea de carácter público o privado— por la infracción de las obligaciones contraídas. La aplicación de la responsabilidad —que se basará en el principio de proporcionalidad—, como contrapartida a la utilización y disfrute de un derecho, hace necesario: 1) La determinación del Derecho aplicable, tanto en los aspectos penal, civil o administrativo como en el procesal, en atención al criterio de territorialidad en la aplicación de las normas jurídicas. 2) El establecimiento de las indemnizaciones que procedan por los daños causados. 3) La creación de un sistema arbitral para la resolución de aquellos conflictos que no se diriman ante la autoridad judicial. (1998)

Desarrollar el contenido esencial de este derecho sería imposible, pues la libertad puede ejercerse de una infinidad de maneras que responden a la voluntad de la persona en su entorno digital. Sin embargo, el derrotero que regirá este derecho será la máxima de clausura privada (Riofrío, 2014, p. 36): todo lo que no está prohibido está permitido. Dependerá de la persona y, particularmente, en cómo es que prefiera ejercer su libertad para alcanzar los fines de su autodeterminación como individuo dentro del ciberespacio. En ese sentido, de manera enunciativa, vemos que se pueden ejercer los siguientes derechos en el ciberespacio como manifestación de la libertad:

- a) **Derecho a participar de la vida social, económica y política de la nación:** garantiza que cualquier persona pueda involucrarse activamente en los asuntos de su comunidad y del Estado a través de herramientas digitales, ya sea emitiendo su voto en sistemas electorales electrónicos, firmando peticiones o participando en debates públicos en foros y plataformas de deliberación ciudadana; o accediendo a servicios públicos en línea para realizar trámites, pagar impuestos y solicitar licencias. Asimismo, comprende la posibilidad de integrarse al mercado digital mediante el comercio electrónico, la banca en línea y el teletrabajo, promoviendo la inclusión económica sin barreras geográficas. En el ámbito social, habilita la conexión con redes de apoyo, comunidades culturales y educativas virtuales, fortaleciendo el sentido de pertenencia y colaboración.
- b) **Derecho a la libertad de conciencia, religión, opinión, información, educación y expresión:** este derecho garantiza que cualquier persona pueda utilizar espacios digitales –foros, redes sociales, blogs, plataformas de *streaming* y mensajería– para exponer sus creencias, intercambiar ideas, informar e informarse, criticar o difundir contenidos sin temor a censura previa, siempre que no vulnere derechos ajenos ni promueva la violencia o el odio.
- En el ámbito religioso, se extiende a la realización de ceremonias virtuales, la transmisión en línea de cultos o charlas de líderes espirituales, y la creación de comunidades de fe que compartan oraciones, textos sagrados y prácticas rituales. En materia de opinión e información, incluye la publicación de artículos de análisis, *podcasts*, vídeos de denuncia social y movimientos de activismo digital, así como la recepción de fuentes diversas para formarse un juicio crítico. A la fecha, incluso la educación se lleva de manera virtual vía Zoom, por lo que debe incluirse este derecho en esta categoría.
- c) **Derecho a la educación y alfabetización digital:** este derecho garantiza y asegura que toda persona tenga acceso a programas formativos –gratuitos o asequibles– que le permitan adquirir y perfeccionar las competencias necesarias para manejar con facilidad el *software* y *hardware*, evaluar la fiabilidad y veracidad de la información en línea, y protegerse ante riesgos como el *phishing*, el *malware* o el robo de identidad.
- d) **Derecho a la innovación, experimentación y a la libertad de creación (intelectual, artística, técnica y científica):** este derecho garantiza que cualquier persona pueda idear, desarrollar, adaptar y difundir nuevas soluciones, obras o descubrimientos en todos los ámbitos del conocimiento y la cultura; siempre que se respeten las normas de propiedad intelectual y los derechos de terceros. Así, un creador puede concebir un token no fungible (NFT –*Non-Fungible Token*–) que represente una obra digital única y ponerlo a la venta en un mercado virtual; o bien diseñar un prototipo mecánico o electrónico que, tras su puesta a prueba en un entorno de experimentación, sea patentado para proteger su invención. Del mismo modo, un artista visual o sonoro puede compartir libremente sus creaciones bajo licencias abiertas o comerciales, y un investigador puede publicar sus hallazgos en repositorios académicos o desplegar el *software* de código abierto para el beneficio colectivo.
- e) **Derecho a la libertad de asociación y reunión virtual:** este derecho garantiza que cualquier persona pueda crear, unirse y participar en colectivos digitales –como grupos de chat, foros temáticos, comunidades de videojuegos, clubes de lectura o asociaciones profesionales– así como promover y asistir a eventos en línea –seminarios web, conferencias, protestas virtuales o encuentros sociales– sin sufrir bloqueos arbitrarios, censura o vigilancia indebida. Incluye la facultad de elegir las plataformas y herramientas de comunicación (video-llamadas, espacios inmersivos de realidad virtual, redes descentralizadas), definir normas internas de funcionamiento, convocar actos públicos o privados y coordinar acciones colaborativas con total libertad de horario y formato.
- f) **Derecho a la libre circulación de ideas y bienes digitales:** este derecho garantiza que las personas puedan compartir y recibir información, *software*, contenidos multimedia y servicios a través de fronteras geográficas sin obstáculos ni discriminaciones arbitrarias, promoviendo el acceso universal al conocimiento y al mercado global. Comprende la descarga y el intercambio de documentos, el uso de plataformas de código abierto, la participación en foros internacionales y la contratación de servicios digitales extranjeros.
- No obstante, este flujo de información no es absoluto: pueden imponerse limitaciones

justificadas para proteger la propiedad intelectual –mediante licencias o acuerdos de derechos de autor–, garantizar la seguridad nacional o impedir el tráfico de contenidos ilícitos (como material de abuso infantil o información clasificada).

- g) **Derecho a la preservación del patrimonio digital:** este derecho faculta a cada individuo para recopilar, archivar y mantener accesibles los contenidos digitales –como documentos, grabaciones, obras de arte virtual, videojuegos o vivencias interactivas– que considere parte de su patrimonio. Le otorga libertad para crear sus propias copias de respaldo, organizar bibliotecas digitales y restaurar formatos obsoletos sin depender de la voluntad de terceros, así como para compartir este acervo con otros usuarios o comunidades de manera voluntaria, así este bien pierda exclusividad. Cabe destacar que este derecho faculta a su titular a exigir tanto al proveedor privado –con el que contrata un servicio de almacenaje, por ejemplo– como al Estado, que adopten las medidas necesarias para garantizar el acceso, la conservación y la interoperabilidad de dichos archivos, de modo que el usuario pueda preservar, consultar y difundir su legado digital según su propia voluntad. Las mismas reglas de inviolabilidad de la propiedad se aplican a este derecho fundamental (inviolabilidad, exclusividad, oponibilidad *erga omnes*, reivindicación, explotación, hereditable, libre disposición, disfrutable, etc.).

El ejercicio pleno de todas estas libertades digitales y de sus garantías esenciales debe sustentarse en tres principios rectores que, de forma conjunta, aseguren su efectiva realización:

- a) **Principio de neutralidad de la red (*net neutrality*):** garantiza que proveedores y operadores no prioricen, bloqueen ni limiten de manera discriminatoria ningún tipo de contenido, aplicación o servicio, asegurando a cada usuario acceso igualitario a la totalidad del ciberespacio.
- b) **Principio de no discriminación en el acceso al internet:** exige que la calidad de la conexión (ancho de banda, latencia, velocidad) sea la misma para cualquier persona, con independencia de su ubicación geográfi-

ca, condición socioeconómica o dispositivo empleado, y faculta al Estado a supervisar y sancionar prácticas como la restricción de velocidad o la segmentación de redes.

- c) **Principio *neminem laedere* (veda al daño digital):** impone la obligación de prevenir, cesar y sancionar conductas que vulneren la dignidad, la privacidad o la seguridad de los usuarios en línea –tales como discurso de odio, ciberacoso, *doxxing*, *revenge porn* o *deepfakes*–, garantizando un entorno virtual libre de agresiones y abusos.

Estos tres pilares configuran el andamiaje normativo y tecnológico imprescindible para que cada uno de los derechos de libertad digital descritos deje de ser meramente declarativo y se convierta en una realidad tangible, equitativa y duradera.

E. El derecho a la privacidad, al olvido, al anonimato y al domicilio digital

El entorno digital, además de ventajas, esconde peligros a menudo inadvertidos: cada clic, cada visita a una publicación y cada búsqueda quedarán registrados para siempre. Seamos conscientes de que la invisibilidad total en el ciberespacio es imposible, pues siempre existirá trazabilidad (incluso hasta al usar el navegador Tor). Dado que el internet es una red abierta de exposición voluntaria, se debe partir de una máxima: “la mejor manera de proteger tu privacidad en la red es asumir que no la tienes y modificar tu comportamiento en línea de acuerdo a ello” (O’Reilly, 2007, pp. 22-23) [traducción libre]¹⁹.

Es interesante –y curioso– cómo es que el derecho a la intimidad o privacidad ha reorientado su enfoque tan radicalmente. Inicialmente, este derecho fue pensado para que las personas naturales puedan contar con una ‘personalidad inviolada’ (Warren & Brandeis, 1890, pp. 193-220), gozar de la soledad (Corte de Apelaciones de Kentucky, 1927, Brents c. Morgan) y, en líneas generales, poder transitar por este mundo sin que sus asuntos personales o su imagen sean expuestos a terceros sin su consentimiento (Morales Godo, 1995, p. 106).

Ahora, sin embargo, existe un deseo de ser notado y de compartir dónde estamos, qué hacemos, con quién estamos, qué comimos, a dónde viajamos, qué nos gusta, qué nos disgusta, etc. A través de redes sociales como Instagram y Facebook, las personas comparten sus datos, ubicación y demás

¹⁹ Texto original: “The best way to protect your online privacy is to assume you have none, and modify your online behavior accordingly.”

datos personales con el mundo, lo cual evidencia que este derecho a la privacidad debe encontrar un nuevo enfoque, pues es relevante para el individuo ser notado a través de un *like*, un corazón o alguna reacción a sus publicaciones.

En otras palabras, la propia tecnología alimenta la pulsión de compartir emociones en tiempo real en una suerte de *performance* identitaria con el objetivo de obtener aceptación social (Syahrani & Rahmi, 2024, p. 130). Esta dicotomía —la voluntad de ser visto frente al riesgo de ser vulnerado— exige repensar este derecho: ya no basta con blindar un espacio privado, sino que es preciso dotar de herramientas activas tanto para controlar la propia exposición como para exigir la moderación de terceros y asegurar el ejercicio de esta libertad de manera segura.

En su núcleo esencial, este derecho exige la incorporación de elementos adicionales que respondan a los nuevos desafíos que plantea el ciberespacio, así como la formulación de dos principios rectores que orienten el uso de la información:

- a) El principio de los medios menos reveladores (*least revealing means*), que consiste en escoger la forma de identificación que minimice al máximo la información y solo se comparta la indispensable para cumplir con un propósito concreto (por ejemplo, la información estrictamente imprescindible para completar una transacción o para poder enviar un correo electrónico) (Abelson *et al.*, 1998).
- b) El principio de los medios más convenientes (*most convenient means*), el cual permite revelar mayor información, si con ello se obtiene una mayor comodidad o eficiencia (por ejemplo, para que un agente de *software* encuentre un producto que se ajuste a tus preferencias). Bajo este principio, se revelará la combinación de datos identificativos que ofrezca la máxima conveniencia, siempre que no se exceda un umbral máximo de información que el usuario no esté dispuesto a compartir y que resulten irrazonables para el propósito de la interacción digital (Abelson *et al.*, 1998).

A pesar de que uno es libre de compartir lo que guste en el ciberespacio, la Constitución también tutela el derecho al olvido en su dimensión digital. Este derecho nace a partir de la necesidad de ser-

vir como un mecanismo que preserve la dignidad y autonomía de la persona frente al paso del tiempo. Es innegable que la arquitectura del internet dificulta sobremanera la desaparición completa de la información para comenzar a promover el olvido de un hecho; pues una vez que algo obra en el ciberespacio, quedará ahí permanentemente, pues se podrán generar copias, archivos privados, fotos, etc.

Sin embargo, esta complicación no es un obstáculo para que el derecho actúe. En efecto, existe en nuestro país la potestad de exigir, sea mediante las normas de la Ley de Protección de Datos Personales o mediante un proceso de *hábeas data*, la supresión de datos que configuren un atentado contra la dignidad de la persona. La existencia de este derecho no está en discusión. El derecho al olvido digital ha sido reconocido expresamente por el Tribunal Constitucional en el fundamento jurídico 11 de la sentencia recaída en el Expediente 02839-2021-PHD/TC. Si bien es imposible que en el internet alguien se olvide de algo, dada su naturaleza abierta y pública, sí es posible en nuestro ordenamiento jurídico accionar mediante el proceso de *hábeas data* exclutorio²⁰. El objetivo de este derecho es el siguiente:

[garantizar] que el desarrollo tecnológico, cualquiera que sea las variantes que adopte, se realice de forma tal que no implique por efectos del tiempo una intervención arbitraria que, producto de la exhibición o difusión de la información personal a través de los sistemas informáticos, pueda producir lesividad permanente en el ejercicio de derechos fundamentales esenciales para desarrollar una vida en dignidad. (2022)

Por último, el derecho al anonimato en el entorno digital se configura como una manifestación esencial de la autodeterminación informativa y la libertad individual. Este derecho permite a las personas controlar la divulgación de su identidad en línea, protegiendo así su privacidad y seguridad frente a posibles amenazas como el acoso, la discriminación o la vigilancia indebida.

Sin embargo, el anonimato en el internet constituye un arma de doble filo: si bien protege derechos fundamentales y estimula la libre expresión, también puede facilitar conductas antisociales y delictivas. Según Lim, Zo y Lee (2011, p. 452), el anonimato garantiza la libertad de expresión y la protección de la privacidad. Ocultando nuestra

²⁰ Véase las sentencias del Tribunal Constitucional recaídas en los Expediente 02839-2021-PHD/TC (fundamentos jurídicos 9-12); y Expediente 03041-2021-PHD/TC (fundamentos jurídicos 6-16).

identidad física –y ‘real’ o, mejor dicho, legal–, los usuarios pueden compartir opiniones controvertidas o experiencias sensibles sin temor a represalias o estigmatización, lo que reduce la autocensura en foros en línea.

Además, esta característica promueve el bienestar psicológico al evitar discriminaciones basadas en características personales (género, raza, edad o atractivo), minimizando la ansiedad social. En contextos de desigualdad de poder, el anonimato es clave para el *whistle-blowing*, pues fomenta que las personas alcen la voz y digan la verdad sin miedo a sanciones en beneficio del interés público, impulsándose el control social.

A pesar de sus bondades, el anonimato en el ciberespacio trae consigo efectos negativos que no podemos ignorar. Al rebajar inhibiciones, puede alimentar conductas anti-normativas y antisociales (Martineau, Spiridon & Aiken, 2023, p. 463). Incluso se han documentado casos en que espectadores anónimos llegaron a instigar a un suicida a lanzarse, impulsados por la sensación de impunidad (Mann, 1981, p. 592). Asimismo, es un facilitador del delito dado que los ciberdelincuentes aprovechan la alta dificultad de rastreo para cometer fraudes masivos, ataques de denegación de servicio distribuido (en inglés, *distributed denial of service*), virus informáticos, robo de identidad y acoso, operando con rapidez y desapareciendo sin dejar rastro (Davenport, 2002, p. 34). A esta conducta se le ha llamado desinhibición tóxica, pues propicia discursos de odio, *trolling* y hostigamiento en línea (Suler, 2004, pp. 321-326).

Si el anonimato fuera absoluto, los riesgos del internet se agravarían desde la misma difusión de información. En el estudio realizado por Lim, Zo y Lee, estos lograron identificar cuatro reglas sociales que caracterizan las conductas de los agentes digitales (2011, pp. 455-457):

- a) **Una persona que utiliza su nombre real difundirá únicamente opiniones de las que está convencido, mientras que un agente anónimo difundirá tanto opiniones de las que está convencido como aquellas de las que no lo está. La regla se explica por dos fenómenos psicológicos.** Primero, la ansiedad social y la autopresentación: quienes usan su nombre real temen dañar su reputación al difundir opiniones en las que no creen, por lo que evitarán compartirlas. En cambio, los anónimos carecen de ese temor al no ser identificables. Segundo, el efecto de desinhibición, particularmente la anonimidad disociativa, hace que las personas anónimas revelen o compartan con más libertad

incluso opiniones no firmemente sostenidas, al sentirse libres de consecuencias personales (2011, p. 455).

- b) **Una persona que use su nombre real goza de mayor credibilidad que uno anónimo, por lo que los receptores tienden a confiar más en la información proveniente de usuarias con nombre real.** La regla se explica por la dificultad del rastreo de la persona anónima que engaña. Existe una presunción de que quien no comparte su nombre real puede difundir información falsa, por lo que se disminuye la confianza en él. Siguiendo la idea de Corritore, Kracher y Wiedenbeck (citado en Lim, Zo & Lee), distinguen cuatro dimensiones de la credibilidad: honestidad, pericia, predictibilidad y reputación. La honestidad y la pericia pueden juzgarse a partir del propio contenido de la opinión. Sin embargo, la predictibilidad y la reputación –que dependen de conocer al emisor y su historial– no son mensurables en agentes anónimos, lo que también contribuye a que su credibilidad sea percibida como baja (2011, pp. 455-456).
- c) **Las convicciones de una persona pueden cambiarse mediante interacciones con otras personas.** Las opiniones en las que se está convencido rara vez pasan a ser no convencidas, y las opiniones no convencidas cambian con facilidad a ser convencidas. La regla explica que el paso de una opinión a otra se comporta como una transición de fase: las opiniones en las que aún no se está plenamente convencido son las que pueden cambiarse con mayor facilidad, mientras que las convictas también pueden invertirse, pero de forma mucho menos frecuente (2011, p. 456).
- d) **La similitud entre personas influirá en la interacción entre ellos. Las personas solo se relacionarán con aquellos cuya semejanza supere un determinado umbral.** Además, la similitud percibida entre usuarios anónimos suele ser mayor de lo que realmente es. Se sustenta en la teoría de la disonancia cognitiva: cuanto mayor es la diferencia entre las opiniones de dos interlocutores, más incómoda se vuelve la interacción y la persona buscará reducir ese malestar, bien adaptándose al punto de vista ajeno o despreciándolo por completo, según el grado de discrepancia (2011, p. 457).

En el contexto peruano, no existe una regulación específica sobre el anonimato digital, pero consi-

deramos que su reconocimiento se deriva de los principios constitucionales que amparan la intimidad y la protección de datos personales. No obstante, el ejercicio del anonimato debe equilibrarse con otros derechos fundamentales, como la libertad de expresión y el acceso a la información. Por ejemplo, en situaciones donde el anonimato pueda ser utilizado para difamar o incitar al odio, las autoridades pueden intervenir para preservar el orden público y los derechos de terceros; para lo cual se podrá levantar el secreto de las comunicaciones para poder identificar el autor de dicha conducta antijurídica. Para tales efectos, se requerirá de una orden emitida por el sujeto legitimado por la Constitución para levantar el secreto de las comunicaciones.

Esto último va de la mano con el derecho al domicilio digital que, así como en el plano físico, es el lugar en donde una persona reside digitalmente, utiliza las herramientas para acceder al ciberespacio y, por lo mismo, goza de inviolabilidad y del secreto de las comunicaciones. Esto incluye tanto a la propia computadora como a las cuentas de redes sociales, videojuegos, aplicaciones, etc. Sobre el particular, existe ya jurisprudencia internacional. El Tribunal Constitucional de Chile, en el 2011, emitió la Sentencia Rol 1894-2011-CPR al pronunciarse sobre un proyecto de ley que buscaba obligar a llevar un registro de los usuarios de cibercafé:

Que, naturalmente, cualquiera entiende –aun sin ser jurisperito– que está a salvo en su legítima discreción para circular anónima e indistinguiblemente de los demás, sin chequeos o registros, a menos que a juicio de una autoridad competente hubiera causas probables que inciten a pensar que se están perpetrando ilícitos concretos y verosímiles. De suerte que, esto sentado, dicha intimidad resultaría usurpada en caso de seguimientos o monitoreos sistemáticos, constantes y focalizados para husmear a qué lugares asiste alguien, por pertenecer a una categoría a priori sospechable de ciudadanos; por dónde –vías, caminos o canales– se desplaza en particular; cuál es el número de los sitios que visita y de las direcciones contactadas, precisamente; con quién, o con cuánta duración y frecuencia se producen las conexiones realizadas. Más todavía cuando, a partir de estos datos, hoy es factible ir de hurones e inferir historiales o perfiles individuales, que incluyen hábitos y patrones de conducta humana, hasta poder revelar las preferencias políticas, opciones comerciales e inclinaciones sociales de las personas. (2011)

Tanto el anonimato como el domicilio digital constituyen herramientas fundamentales para preser-

var la esfera íntima de las personas en el entorno virtual. Mientras el anonimato permite al usuario interactuar, informarse y denunciar sin temor a represalias; el domicilio digital asegura un espacio de seguridad equiparable a la privacidad del hogar físico, protegido frente a registros y seguimientos arbitrarios. La jurisprudencia comparada subraya que cualquier intervención en estos ámbitos solo puede justificarse ante causas probables debidamente acreditadas y bajo la autoridad competente, bajo pena de vulnerar derechos fundamentales e incurrir en responsabilidades.

Este doble resguardo –la capacidad de permanecer anónimo y la inviolabilidad de nuestro espacio de conexión– impone al Estado y a los proveedores de servicios digitales la obligación de establecer normas, protocolos y salvaguardas técnicas que garanticen el respeto irrestricto al secreto de las comunicaciones y procedimientos claros y bajo la dirección de los sujetos legitimados constitucionalmente para la desanonimización o el acceso a domicilios digitales; procurando la conservación de la prueba digital (Núñez & Núñez, 2024).

F. El derecho a la paz en el ciberespacio

El derecho a la paz en el ciberespacio es la facultad de toda persona –sea natural o jurídica– a desenvolverse en un entorno digital libre de hostilidades, ataques y agresiones informáticas, con garantías de estabilidad y seguridad que permitan el ejercicio pleno de sus derechos en línea. Este derecho incluye la protección frente a ciberataques (*malware, phishing, distributed denial of service*), la prohibición de guerra informática, la prevención de campañas masivas de desinformación y la obligación de los Estados y operadores de infraestructuras críticas de responder con diligencia ante incidentes que pongan en riesgo la continuidad de servicios esenciales.

La paz tiene un sinnúmero de definiciones, pero consideramos que la más abierta y plástica es la que fija la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) al sostener que la paz no significa solamente ausencia de conflictos armados, sino también la ausencia de violaciones a derechos humanos en la medida que el contenido de la paz es la exigencia de justicia entre las sociedades y el reconocimiento de la igualdad y la dignidad de todos los pueblos y las culturas (Arango, 2007, p. 15).

La paz en el ciberespacio será, *mutatis mutandis*, la misma que en el espacio físico: la ausencia de perturbaciones, alteraciones, ataques y, en general, cualquier tipo de molestia injustificada e irra-

zonable que atente contra la tranquilidad del usuario digital. Este derecho ha sido ya reconocido por nuestra Constitución en el artículo 2.22²¹ en donde se reconoce el derecho a la paz, a la tranquilidad, al disfrute del tiempo libre y al descanso, así como a gozar de un ambiente equilibrado y adecuado para el desarrollo de la vida (1993).

Si bien el desarrollo jurisprudencial del Tribunal Constitucional apunta a reconocer la paz y el ambiente equilibrado y adecuado para el desarrollo de la vida, ligándolo al medioambiente²², ya esa noción deviene en anacrónica y estéril. La correcta interpretación de ese derecho fundamental tiene que ser más amplia y en son a las nuevas libertades digitales bajo el amparo del principio *pro libertatis*, el cual garantiza como principio interpretativo de los derechos fundamentales que, ante la concurrencia de interpretaciones, se debe optar por la más favorable para la satisfacción de un derecho constitucional. Citamos, por todas, dos sentencias del Tribunal Constitucional que desarrollan este principio:

[...] al ser favorable este hecho al actor, en aplicación de los principios *pro homine* y *pro libertatis* de la interpretación constitucional, según los cuales, ante eventuales y diferentes interpretaciones de un dispositivo legal, se debe optar por aquel que conduzca a una mejor protección de los derechos fundamentales. (Expediente 080-2002-AA/TC, fundamento jurídico 5)

[...] la interpretación de la recurrida no resulta acorde con los principios *pro homine* y *pro libertatis*, según las cuales, ante diferentes interpretaciones de un dispositivo legal, se debe optar por aquella que conduzca a una mejor protección de los derechos fundamentales, descartando así las que restrinjan o limiten su ejercicio. Vale decir, el principio *pro homine* impone que, en lugar de asumirse la interpretación restrictiva, e impedir el derecho [...], se opte por aquella que posibilite a los recurrentes el ejercicio de dicho derecho. (Expediente 0075-2004-AA/TC, fundamento jurídico 6)

La regla objetiva que ha fijado el Tribunal Constitucional es que, ante la presencia de distintas interpretaciones sobre un dispositivo legal, se debe optar por aquella que garantice de mejor manera un derecho fundamental, descartando las

que limiten el derecho. Claramente, y siguiendo la concepción del ciberespacio como el 'quinto dominio', se debe de considerar que la Constitución también garantiza que en todo lugar en donde interactúe una persona –plano físico o virtual– el derecho debe asegurar que las condiciones sean pacíficas para que pueda ejercer sus libertades con tranquilidad y sin ataques a su fuero interno ni demás derechos.

En este contexto, la protección de la paz en el ciberespacio no se limita a la defensa frente a molestias cotidianas, sino que también exige garantizar la integridad funcional de los entornos donde se ejercen los derechos fundamentales, se prestan servicios públicos esenciales o se resguardan vidas humanas. Por ello, es necesario identificar aquellos sistemas digitales cuya vulneración comprometería gravemente la seguridad, la continuidad institucional o la vida misma. Desde un enfoque de gestión de riesgos, se distinguen tres tipos de sistemas que, por su sensibilidad, deben ser priorizados:

- a) **Sistemas críticos para la misión:** son los sistemas que hacen funcionar los ámbitos más importantes de una organización. Si estos fallan, la organización no puede seguir funcionando.
- b) **Sistemas críticos para el negocio:** ayudan a la organización a brindar sus servicios, pero no son esenciales para que la organización siga funcionando en su totalidad. Si fallan, habrá problemas y pérdidas de dinero, pero la empresa puede seguir operando parcialmente.
- c) **Sistemas críticos para la seguridad:** protegen a las personas y el entorno de peligros físicos. Si fallan, pueden poner en riesgo la vida de las personas o causar daños al medio ambiente.

Incluso, desde una perspectiva práctica, la necesidad de proteger la paz en el ciberespacio exige no solo identificar los sistemas más sensibles y críticos para la misión, el negocio o la seguridad; sino comprender también cómo ciertas actividades digitales pueden perturbar ese entorno y comprometer derechos fundamentales. En esa línea, resulta útil trasladar al plano virtual las categorías

²¹ Artículo 2.- Toda persona tiene derecho: [...] 22. A la paz, a la tranquilidad, al disfrute del tiempo libre y al descanso, así como a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida (1993).

²² Véase las sentencias del Tribunal Constitucional recaídas en el Expediente 00004-2010-PI/TC (fundamentos 10, 12 y 15); Expediente 6204-2006-PHC/TC (fundamento 20); Expediente 0018-2001-AI/TC (fundamento 6); Expediente 00001-2012-PI/TC (fundamento 27); y Expediente 0260-2001-AA/TC (fundamento 1).

de actividades lesivas que el Tribunal Constitucional ha desarrollado para el ambiente físico, adaptándolas a la lógica del entorno digital como nuevo espacio de convivencia humana que, sin dudas, merece tutela constitucional.

En el fundamento jurídico 6 de la sentencia del Expediente 0018-2001-AI/TC, el Tribunal Constitucional distinguió entre actividades molestas, insalubres, nocivas y peligrosas como formas de afectación al derecho a un ambiente equilibrado y adecuado para el desarrollo de la vida. Esta clasificación puede aplicarse, *mutatis mutandis*, al ciberespacio, entendiendo que este también constituye un entorno en el que las personas desarrollan su existencia, ejercen derechos y despliegan relaciones sociales, políticas, económicas y culturales. Así, el ambiente digital debe entenderse como una extensión del ambiente vital protegido por el artículo 2.22 de la Constitución. Veamos:

- a) **Actividades molestas:** en el espacio físico, se refiere a ruidos o vibraciones; en el digital, equivalen a todo tipo de perturbaciones no solicitadas que degradan la experiencia de navegación o interacción. De manera enunciativa, estas son el *spam*, las ventanas emergentes agresivas, las notificaciones intempestivas, los contenidos publicitarios intrusivos, comunicaciones indeseadas. Aunque no destruyan sistemas, estos flujos constantes de información irrelevante generan molestia, distracción y fatiga cognitiva, mermando la calidad de nuestro entorno virtual.
- b) **Actividades insalubres:** así como en el mundo real se vierten contaminantes que perjudican la salud, en la red las amenazas a la integridad digital y mental –*malware*, *phishing*, enlaces a páginas maliciosas o contenido tóxico y adictivo– actúan como una lacra invisible. Estos agentes pueden infiltrarse en dispositivos, robar o cifrar datos personales (*ransomware*), y atacar la estabilidad psicológica de los usuarios mediante campañas de acoso o desinformación que provocan estrés, ansiedad y conductas de riesgo.
- c) **Actividades nocivas:** en el ámbito agropecuario se entiende como daño a la riqueza productiva; en el ciberespacio, son aquellas intrusiones o manipulaciones que lesionan los activos digitales y el capital reputacional de personas y organizaciones. Los ataques de *ransomware* que cifran bases de datos, las campañas de desinformación que arruinan la confianza en una marca (*astroturfing*), o las violaciones de propiedad intelectual

–como la piratería de *software* o el robo de código fuente– se traducen en pérdidas económicas y deterioro de la riqueza tecnológica de un país.

- d) **Actividades peligrosas:** equivalen a explosiones o radiaciones en el mundo físico. En el ciberespacio son las amenazas de alto impacto que ponen en riesgo la vida, la seguridad pública o la integridad de infraestructuras críticas. Un ataque a los sistemas de control de un hospital, la desconfiguración de redes eléctricas, el infiltramiento a un sistema de Supervisory Control and Data Acquisition o la manipulación de semáforos inteligentes pueden derivar en consecuencias letales. Asimismo, la propagación de *malware* industrial o la interrupción de los controladores de tráfico aéreo, configuran verdaderos peligros digitales con efectos devastadores en el mundo real que pueden terminar con la pérdida de vidas humanas y daños reputacionales inconmensurables (2002).

El reconocimiento del derecho a la paz en el ciberespacio, en tanto extensión lógica y necesaria de los derechos fundamentales previstos en el artículo 2.22 de la Constitución, supone una reinterpretación evolutiva del contenido de dicho precepto a la luz de las nuevas realidades digitales. El ciberespacio, como quinto dominio de interacción humana, no puede permanecer ajeno a las garantías propias de un entorno equilibrado y adecuado para el desarrollo de la vida, en donde toda persona pueda ejercer sus derechos en condiciones de seguridad, estabilidad y dignidad.

La proyección del principio *pro libertatis* impone, además, una obligación hermenéutica a favor de la interpretación más favorable al goce efectivo de los derechos constitucionales, lo que exige ampliar la noción de ambiente a todo lugar donde exista interacción humana sostenida. En ese sentido, la concepción de paz en el ciberespacio debe comprender tanto la prevención de agresiones informáticas como la reparación oportuna del equilibrio perturbado.

Desde una perspectiva funcional, el derecho a la paz comporta no solo una garantía negativa frente a interferencias y perturbaciones indeseadas e irrazonables; sino también una dimensión positiva que obliga al Estado a crear y mantener condiciones equitativas, implementar políticas públicas eficaces, y ejercer una fiscalización adecuada para preservar la armonía del entorno digital. Cuando dichas condiciones se vean vulneradas, se impone el deber de restaurar activamente ese equilibrio mediante el uso legítimo del poder público.

G. El derecho a la ciberseguridad

En el marco de la cláusula abierta de derechos reconocida por el artículo 3²³ de la Constitución, la ciberseguridad puede y debe ser entendida como un derecho fundamental emergente, cuya función no se agota en la dimensión técnica, sino que incide directamente en las condiciones estructurales que hacen posible el ejercicio efectivo de los derechos fundamentales en el ciberespacio. En un entorno digital caracterizado por la interconectividad permanente, la automatización de procesos y la concentración masiva de datos, la ausencia de estándares mínimos de protección y seguridad no solo incrementa los riesgos tecnológicos, sino que vacía de contenido real a los derechos que se ejercen en dicho entorno.

En efecto, sin niveles adecuados de ciberseguridad no resulta posible garantizar plenamente derechos fundamentales como la privacidad y la protección de datos personales, en la medida en que las fallas de seguridad facilitan la filtración, exfiltración o manipulación de información sensible. Del mismo modo, el ejercicio de la libertad de expresión y el acceso a la información en internet se ven seriamente comprometidos cuando los entornos digitales son vulnerables a ataques de censura indirecta, sabotaje informático o manipulación coordinada de contenidos. Incluso derechos como la tutela jurisdiccional efectiva o la participación ciudadana adquieren una dimensión precaria si las plataformas que los soportan carecen de garantías mínimas de integridad, disponibilidad y autenticidad.

Desde esta perspectiva, la ciberseguridad no puede ser concebida únicamente como un conjunto de medidas técnicas accesorias, sino como un mecanismo constitucionalmente relevante que preserva el contenido esencial de múltiples derechos fundamentales. Su función es, ante todo, habilitante: asegura que el entorno digital –hoy convertido en un espacio central de interacción social, económica y política– opere de manera fiable, previsible y segura. Sin dicha garantía, la declaración formal de los derechos fundamentales en el ciberespacio deviene meramente ilusoria, al quedar expuesta a interferencias sistemáticas que erosionan su ejercicio real.

Esta incidencia constitucional se manifiesta de manera concreta a través de, al menos, tres dimen-

siones complementarias. En primer lugar, la ciberseguridad protege materialmente bienes jurídicos constitucionalmente tutelados, como la confidencialidad de los datos médicos, financieros o personales; directamente vinculados con los derechos a la intimidad, la salud y la autodeterminación informativa. En segundo lugar, asegura la continuidad y disponibilidad de los sistemas y plataformas digitales que permiten el ejercicio efectivo de derechos fundamentales, tales como los servicios públicos electrónicos, los expedientes judiciales digitales o los mecanismos de participación ciudadana en línea. Finalmente, garantiza la integridad, autenticidad y trazabilidad de la información digital, elementos indispensables para la prueba electrónica y, con ello, para la tutela jurisdiccional efectiva en el entorno digital.

En este sentido, el derecho a la ciberseguridad se configura como una categoría autónoma, aunque estrechamente vinculada a otros derechos fundamentales, cuyo reconocimiento se justifica no solo por la proyección de garantías clásicas, sino por la aparición de riesgos estructurales propios del ciberespacio que no pueden ser adecuadamente afrontados mediante una lectura tradicional del catálogo constitucional. La cláusula abierta del artículo 3 de la Constitución habilita, precisamente, esta evolución, evitando una autorrestricción interpretativa que limitaría la protección constitucional a escenarios concebidos al margen de la realidad digital contemporánea.

Esta comprensión constitucional del derecho a la ciberseguridad encuentra ya una primera concreción en el ordenamiento jurídico peruano. A nivel legislativo, el Decreto de Urgencia 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, define la ciberseguridad en su artículo 3, inciso h), y establece obligaciones orientadas a la gestión de riesgos, la protección de infraestructuras críticas y la respuesta frente a incidentes de seguridad digital. Si bien dicha norma no agota el contenido constitucional del derecho, sí constituye un ejemplo claro de cómo el mandato constitucional de protección de la dignidad y seguridad de la persona se traduce en estándares técnicos, organizativos y normativos destinados a preservar el ejercicio efectivo de los derechos fundamentales en el ciberespacio, en los siguientes términos:

²³ Artículo 118.- Corresponde al presidente de la República:

[...]

14. Presidir el Sistema de Defensa Nacional; y organizar, distribuir y disponer el empleo de las Fuerzas Armadas y de la Policía Nacional.

[...]

16. Declarar la guerra y firmar la paz, con autorización del Congreso (1993).

Ciberseguridad.- Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país. (2020)

Si bien esta definición se formula desde una lógica predominantemente funcional y administrativa, su relevancia constitucional es indiscutible. En primer lugar, porque reconoce de manera expresa que la protección del ciberentorno no se agota en soluciones técnicas aisladas, sino que exige un enfoque integral que combine normas, procesos, responsabilidades y tecnologías. En segundo lugar, porque evidencia que el Estado ha asumido, aunque todavía de forma incipiente, que la ciberseguridad constituye un presupuesto necesario para la protección de los usuarios y, por tanto, para el ejercicio efectivo de derechos fundamentales en entornos digitales.

Desde una perspectiva constitucional, esta regulación no puede entenderse como un mero desarrollo sectorial desvinculado del sistema de derechos fundamentales. Por el contrario, el Decreto de Urgencia 007-2020 debe leerse como una concreción normativa inicial de la cláusula abierta de derechos prevista en el artículo 3 de la Constitución en la medida en que busca preservar condiciones estructurales indispensables para la vigencia de la dignidad humana, la libertad y la seguridad jurídica en el ciberespacio. En ese sentido, no se trata de un simple marco técnico de gestión pública, sino de una manifestación del deber estatal de garantizar, mediante normas de configuración legal, el contenido esencial de los derechos fundamentales cuando estos se ejercen en contextos tecnológicos complejos.

Ahora bien, precisamente por su ubicación normativa y por su enfoque operativo, esta definición legal resulta insuficiente si se la interpreta de manera restrictiva o reduccionista. La ciberseguridad, más que un conjunto de técnicas aisladas —como parece entenderlo nuestro Gobierno—, debe comprenderse como una garantía constitucional de carácter estructural, orientada a asegurar que el entorno digital sea un espacio confiable para el desarrollo de la vida personal, social, económica y política. Ello exige abandonar cualquier lógica de autorrestricción interpretativa que limite la ciberseguridad a un problema meramente técnico o de eficiencia administrativa, y asumirla, en cambio, como un componente inherente al estatuto constitucional de la persona en la era digital.

En esta línea, la ciberseguridad debe entenderse como la articulación sistémica de políticas,

controles y prácticas —inspiradas en estándares internacionales como la familia ISO/IEC 27000— destinadas a garantizar de manera concurrente la confidencialidad, la integridad y la disponibilidad de los sistemas de información y de los datos personales. Solo cuando estas tres dimensiones —la conocida CIA *Triad*— se encuentran adecuadamente protegidas es posible ofrecer un entorno digital estable y confiable, capaz de servir como soporte real para el ejercicio efectivo de los derechos fundamentales, tanto clásicos como emergentes, en el ciberespacio.

Sin un nivel mínimo de garantías en la protección de la información, cualquier pretensión de tutelar la privacidad en línea, la libertad de expresión o incluso la paz digital queda condenada al fracaso: las brechas de seguridad no solo permiten la filtración masiva de datos, sino que abren las puertas al sabotaje de infraestructuras críticas y a la manipulación de la opinión pública, erosionando con ello la confianza social y la legitimidad del propio Estado. Precisamente esa visión de derechos como instituciones vivas y adaptables se ve ratificada en la exposición de motivos del, ya mencionado, Decreto de Urgencia 007-2020, que subraya con claridad la dimensión estructural de la ciberseguridad para nuestra sociedad:

b. El impacto de los ciberataques afecta la credibilidad y confianza en el país, impacta la competitividad, la productividad, las condiciones para hacer negocios en el país, la productividad en las regiones y la seguridad de las personas. De igual manera, los delincuentes comunes utilizan las redes y el Internet para facilitar sus delitos: acosan a sus víctimas por redes sociales, ingresan a cámaras de vigilancia y a cualquier dispositivo de los hogares, hacen seguimiento a las víctimas rastreando maliciosamente. Por ello, existe la urgencia de establecer un marco regulatorio con el fin primario de salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital, especialmente en materia de intimidad personal, familiar y seguridad, así como también atender el deber constitucional del Estado peruano de proteger a la población de las amenazas contra su seguridad, incluyendo aquellas que provienen por agentes perjudiciales en el referido entorno digital. Si bien, la aprobación de la Ley de Gobierno Digital constituye un gran paso para este objetivo, el gobierno digital solo implica acciones al interior del Estado, lo cual resulta insuficiente. Revertir esta situación es urgente. Para ello debe garantizarse la articulación público privada y que el Estado emita lineamientos para los servicios y plataformas digitales públicas y privadas que se implementen para lograr estos objetivos. (2020, pp. 13-14)

Resulta particularmente revelador que el propio Gobierno, en la exposición de motivos del Decreto de Urgencia citado, reconozca de forma expresa que los derechos fundamentales no son instituciones estáticas ni cerradas, sino normas institucionales de naturaleza fenoménica, cuya legitimidad y contenido deben repensarse a la luz de los cambios sociales, tecnológicos y culturales. Este reconocimiento no es menor: implica asumir que la arquitectura constitucional no puede permanecer ajena a las transformaciones que alteran radicalmente los escenarios donde los derechos se ejercen y en donde el ser humano interactúa.

La interconectividad global, el acceso masivo e irrestricto al internet y la digitalización acelerada de todas las esferas de la vida son hechos normativamente relevantes que imponen al Estado la obligación de actualizar sus mecanismos de protección. Negarse a ello equivaldría a renunciar al compromiso constitucional de garantizar la dignidad humana, abandonando al ciudadano a un entorno digital donde las amenazas no solo se multiplican, sino que adquieren una capacidad de daño sin precedentes.

El Estado, como titular del monopolio legítimo de la fuerza y garante último del orden constitucional, no puede limitar su actuación a los espacios físicos tradicionales. Su deber de protección —que constituye la base del principio de juridicidad y legitima el pacto social— exige una intervención activa en el ciberespacio, allí donde hoy se despliegan no solo las nuevas formas de violencia, sino también los proyectos de vida, las identidades, los vínculos afectivos y las actividades económicas de millones de personas. La omisión de medidas jurídicas y técnicas adecuadas de ciberseguridad equivale, por tanto, a una abdicación institucional frente a su rol más esencial: garantizar un entorno seguro en el que los derechos fundamentales puedan ejercerse plenamente, sin interferencias ni amenazas arbitrarias.

Este deber de protección en el ciberespacio no puede limitarse a reacciones puntuales frente a incidentes aislados. Por el contrario, exige la construcción de un auténtico orden jurídico de la ciberseguridad, capaz de abarcar no solo los aspectos preventivos y reactivos frente a ataques, sino tam-

bién las estructuras normativas, institucionales y técnicas que aseguren la solidez del ecosistema digital. En efecto, la protección de los derechos fundamentales en la era digital requiere de un tratamiento normativo integral que reconozca la multiplicidad de riesgos y la complejidad de los activos involucrados. Ahora, la ciberseguridad debe ser abordada como una dimensión transversal del derecho público, con implicancias claras en materia de soberanía, regulación de la actividad privada y responsabilidad estatal.

El derecho fundamental a la ciberseguridad tiene muchísimas manifestaciones y ello es así, dado que protege todo tipo de activo cibernético. En ese sentido, no solo la seguridad física de los activos digitales y el intangible (*software*) será objeto de protección, sino todas las relaciones a la tecnología que puedan presentarse respecto a la información que contiene, al usuario que la usa, entre otros. El Estado será el responsable de ello, debiendo sancionar a aquellos integrantes de la sociedad que no garanticen tales parámetros de seguridad; o haciéndose responsable por inobservar tal garantía.

Sobre el particular, no hay dudas. La Constitución en su artículo 44²⁴ establece que son deberes primordiales del Estado:

[...] defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos; proteger a la población de las amenazas contra su seguridad; y, promover el bienestar general que se fundamenta en la justicia y el desarrollo integral y equilibrado de la Nación. (1993)

Del mismo modo, el artículo 163 establece que:

El Estado garantiza la seguridad de la Nación mediante el Sistema de Defensa Nacional. La Defensa Nacional es integral y permanente. Se desarrolla en los ámbitos interno y externo. Toda persona, natural o jurídica, está obligada a participar en la Defensa Nacional, de conformidad con la ley. (1993)

En tal sentido, la defensa nacional debe comprender todos los ámbitos, incluidos los nuevos escenarios tecnológicos: el ciberespacio, que hoy es reconocido como el quinto dominio y cuya protec-

²⁴ Artículo 44.-

Son deberes primordiales del Estado: defender la soberanía nacional; garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

Asimismo, es deber del Estado establecer y ejecutar la política de fronteras y promover la integración, particularmente latinoamericana, así como el desarrollo y la cohesión de las zonas fronterizas, en concordancia con la política exterior. (1993)

ción resulta inherente al mandato constitucional. Dicho mandato obliga al Ejecutivo a incorporar al ciberespacio en la esfera de la defensa nacional y las políticas públicas de seguridad.

Comentando el artículo 44 de la Constitución, el Tribunal Constitucional ha sentenciado en el Expediente 1363-2002-AA/TC, fundamento jurídico 1, lo siguiente:

El artículo 44 de la Constitución establece como deberes primordiales del Estado la defensa de la soberanía nacional, garantizar la plena vigencia de los derechos humanos, la protección de la población ante amenazas contra su seguridad y la promoción del bienestar general fundamentado en la justicia y en el desarrollo integral y equilibrado de la nación. Para el cumplimiento de tales deberes, el Estado se encuentra dotado de poder, el que, por su propia naturaleza, es uno solo, y cuyo ejercicio se manifiesta a través de las distintas actividades que realiza. En un Estado constitucional de derecho, como se precia de serlo el nuestro, la fuente de dicho poder se encuentra en el pueblo que lo legitima, y emana de la Constitución. (2003)

Como monopolizador del poder de coacción, el Estado se encuentra en la obligación de brindar todas las condiciones necesarias para asegurar el bienestar de su población, siendo que debe adecuar las medidas de seguridad y defensa que emplea y desarrolla para las nuevas amenazas. No por nada el supremo intérprete de la Constitución afirma categóricamente que el “[...] Estado está comprometido a invertir los recursos indispensables para desarrollar las tareas necesarias que le permitan cumplir con el encargo social de garantizar el derecho a la vida, la libertad, la seguridad y la propiedad privada” (Expediente 2945-2003-AA/TC, fundamento jurídico 26).

Este marco adquiere especial relevancia cuando se considera que el ciberespacio constituye una nueva dimensión de soberanía estatal (el quinto dominio). Ello supone que el presidente de la República, como jefe supremo de las Fuerzas Armadas y de la Policía Nacional según mandato constitucional (artículo 167²⁵ de la carta de 1993), así como los numerales 14 al 16 del artículo 118 de la Constitución, preside el Sistema de Defensa Nacional y adopta medidas para proteger la soberanía, la integridad del territorio y la defensa de la República. Estas normas facultan al Ejecutivo para la organización, mando y conducción de la defensa nacional,

lo que abarca por extensión la protección del ciberespacio como nuevo ámbito de soberanía estatal.

Bajo este esquema, el presidente está legitimado y obligado constitucionalmente a formular y ejecutar políticas de ciberdefensa y ciberseguridad. No obstante, la efectividad de dicha conducción depende también de la infraestructura institucional y técnica del Estado. Y es precisamente aquí donde advertimos una importante brecha: mientras el marco normativo permite la acción, la capacidad estatal para implementarla en la práctica sigue siendo limitada.

Claramente, las amenazas cibernéticas no son riesgos que deban ser tomados a la ligera por el potencial daño catastrófico que suponen. En el Perú, a la fecha, recién estamos tomando conciencia de este tema, siendo que, de acuerdo con la exposición de motivos del Decreto Supremo 017-2024-PCM, se reconoce que en el Perú se han perdido USD 4728 millones en ataques cibernéticos solo en el año 2017. A pesar de ello, debemos dejar de manifestar que el Estado peruano, recién en el año 2020, comienza a definir como política institucional lo que es la ciberseguridad, lo cual demuestra, a todas luces, el grave rezago en dicha materia.

De hecho, recién en el año 2021, mediante la Resolución Ministerial 0355-202-DE, la cual constituye el ‘Equipo de Respuestas ante Incidentes de Seguridad Digital’ –*Computer Security Incident Response Team*– (en adelante, CSIRT), del Ministerio de Defensa; se ha empezado a tomar en serio la labor del Estado en proteger los activos digitales críticos y en desarrollar un marco de ciberdefensa. Lo mismo ocurre con la Resolución Ministerial 00292-2022-PRODUCE, que conforma el CSIRT del Ministerio de la Producción. Sin embargo, advertimos que, para integrar este nivel de equipos, se requiere de personal altamente capacitado en respuesta de incidentes con certificaciones de avanzado nivel y un amplio bagaje de experiencia; profesionales que son escasos en el país por el mismo hecho de que no se fomenta esta materia ni es remunerada adecuadamente.

Esta situación de rezago normativo e institucional no implica, sin embargo, la inexistencia de facultades de respuesta ni la ausencia de deberes públicos. Por el contrario, la falta de preparación estructural refuerza la necesidad de un liderazgo político claro y activo en materia de ciberdefensa. En este escenario, el presidente de la República, como jefe supremo de las Fuerzas Armadas y conductor de la política general del gobierno, se convierte en una

²⁵ Artículo 167.- El presidente de la República es el jefe Supremo de las Fuerzas Armadas y de la Policía Nacional (1993).

pieza clave para suplir –mediante directivas, coordinación interinstitucional y decisiones ejecutivas– las brechas que aún persisten en el aparato estatal. El hecho de que existan pocos CSIRT sectoriales o escaso personal técnico calificado no disminuye el riesgo; lo agrava. Y cuanto más urgente sea la amenaza, más indispensable se vuelve la conducción desde la más alta instancia del Poder Ejecutivo.

La doctrina comparada enfatiza igualmente el papel ejecutivo en la defensa digital. Estudios como el de Matthew Waxman destacan que los ciberataques rara vez constituyen por sí solos ejercicios de facultades de guerra constitucional –una manifestación moderna del *ius ad bellum* (Schmitt *et al.*, 2017, p. 4)– y que suelen encuadrarse mejor en poderes ejecutivos de defensa, asuntos exteriores o inteligencia (2020). Este enfoque admite un amplio margen de maniobra presidencial para responder a amenazas cibernéticas, sujeto a control legislativo. De hecho, el artículo 8 de la Ley 30999, Ley de Ciberdefensa, ratifica dicha tesis:

La planificación y ejecución de las operaciones de ciberdefensa a cargo del Comando Conjunto de las Fuerzas Armadas responde al mandato conferido en la Constitución Política del Perú, así como al cumplimiento de las responsabilidades asignadas en las leyes que regulan su naturaleza jurídica, competencias, funciones y estructura orgánica, las disposiciones contenidas en la presente ley, y los tratados y acuerdos internacionales de los que el Perú es parte y resulten aplicables. (2019)

Estas facultades constitucionales tienen como finalidad proteger y garantizar el pleno ejercicio y goce de los derechos fundamentales. En efecto, el artículo 44 de la Constitución asocia la defensa de la soberanía con la garantía de la plena vigencia de los derechos humanos, lo que implica que las amenazas cibernéticas que pueden afectar derechos como la intimidad, la integridad de datos y la libertad de información, deben ser neutralizadas por el Estado. Por ello, asegurar el ciberespacio es, a la vez, preservar libertades y protecciones constitucionales. Así, la actuación presidencial en ciberseguridad cumple una función tutelar: salvaguardar el normal ejercicio de derechos de orden fundamental, contribuyendo así a la realización efectiva de la Constitución en el ciberespacio.

En esta línea, la ciberseguridad se erige como la piedra angular para garantizar el ejercicio pleno de los derechos digitales. No puede hablarse de privacidad, acceso a la información, libertad de expresión o protección de datos personales si el entorno digital en el que estos derechos se ejercen carece de garantías técnicas mínimas. La protección de la

infraestructura digital –incluyendo bases de datos públicas, plataformas gubernamentales y sistemas críticos– no es un fin en sí mismo, sino un medio esencial para preservar los derechos de los ciudadanos en la era digital.

Casos como el ciberataque masivo al sistema de salud del Reino Unido (National Audit Office, 2018) en 2017, mediante el *ransomware* WannaCry, evidencian que la falta de medidas preventivas puede comprometer no solo la información personal sensible, sino incluso el acceso a servicios esenciales y el derecho a la salud. Incluso en el Perú, el ciberataque sufrido por Interbank en 2022, que comprometió información sensible de un sinnúmero de clientes, reflejó la vulnerabilidad del entorno digital frente a agentes maliciosos y la necesidad urgente de protocolos robustos de ciberseguridad.

Estos eventos demuestran que la ciberseguridad no es un mero aspecto técnico, sino una condición estructural indispensable para garantizar el ejercicio pleno de los derechos digitales. Solo mediante entornos digitales seguros se puede proteger el derecho a la privacidad, la integridad de los datos personales, la libertad de información y el acceso equitativo a servicios públicos esenciales. Por tanto, más que una política sectorial, la ciberseguridad debe ser concebida como una pieza angular del Estado Constitucional de derecho en la era digital, sin la cual los derechos fundamentales en línea no pueden realizarse de manera efectiva ni sostenible.

IV. CONCLUSIONES

Los derechos fundamentales no son instituciones estáticas; por el contrario, están diseñadas para evolucionar conforme a las necesidades sociales y los contextos históricos de cada época. En la actualidad, esta evolución se manifiesta con fuerza en el ámbito tecnológico, donde el avance de las tecnologías de la información y la comunicación ha transformado radicalmente la forma en que interactuamos, trabajamos y ejercemos nuestras libertades. La interconectividad global, a través del acceso permanente a internet, ha creado un nuevo escenario de interacción social: el ciberespacio, considerado como un quinto dominio de soberanía estatal.

Este espacio digital no es un mero complemento, sino un lugar central en la vida cotidiana donde se desarrollan relaciones sociales, económicas, políticas y culturales. En consecuencia, los derechos fundamentales deben poder ejercerse plenamente en este ámbito, y para ello es imprescindible contar con condiciones que garanticen la seguridad y protección frente a las amenazas y riesgos

cibernéticos que hoy en día tienen un alcance global y un impacto potencialmente catastrófico.

Así, la ciberseguridad se erige como la pieza angular para asegurar el ejercicio efectivo de los derechos digitales. Sin ella, el acceso libre y seguro a la información, la privacidad, la integridad de los datos y la libertad de expresión pueden verse seriamente comprometidos. Para ilustrar este punto, podemos hacer una analogía clara: imaginar una vida sin policías que protejan a los ciudadanos, o un sistema de tránsito sin semáforos que ordenen y regulen el flujo vehicular, revela la anarquía y el peligro al que estaríamos expuestos. De forma similar, sin un sistema robusto de ciberseguridad, el ciberespacio se convertiría en un entorno hostil e inseguro, donde los derechos digitales quedarían vulnerables ante ataques, fraudes, desinformación y otros riesgos.

Por tanto, la consolidación de políticas públicas, marcos normativos y capacidades técnicas de ciberseguridad no solo protege los activos digitales críticos del Estado y la sociedad, sino que garantiza la vigencia y eficacia de los derechos fundamentales en esta nueva dimensión social. El Perú, enfrentando aún importantes desafíos para alcanzar un nivel adecuado de protección digital, debe continuar fortaleciendo su institucionalidad y adoptar una visión integral que incluya tanto la defensa nacional como la promoción y protección de derechos humanos en el ciberespacio.

Finalmente, esta adaptación debe ser equilibrada y respetar los controles democráticos, asegurando que el ejercicio de las facultades ejecutivas en materia de ciberdefensa sea transparente, legítimo y orientado a la protección real de la ciudadanía. Solo así el Estado podrá garantizar que el ciberespacio sea un entorno seguro y confiable para el desarrollo pleno de la vida social y democrática en la era digital. 🏠

CONFLICTO DE INTERESES

El autor declara expresamente que no existen conflictos de intereses que hayan influido en la elaboración, evaluación ni publicación del presente artículo.

FUENTES DE FINANCIACIÓN

El autor declara que no ha recibido financiamiento externo para la realización de la presente investigación.

ESTÁNDARES ÉTICOS

El autor manifiesta que esta investigación ha sido desarrollada conforme con los principios y estándares éticos aplicables a la labor académica e investigativa.

REFERENCIAS

- Abelson, H., Lessing, L., Covell, P., Gordon, S., Hochberger, A., Kovacs, J., Krikorian, R. & M. Schneck (1998). *Digital Identity in Cyberspace*. (White Paper Submitted for 6.805/Law of Cyberspace: Social Protocols).
- Agrawal, H., & Bhattar, N. (2022). Cyberbullying in India: A Hindrance to Peacebuilding and Gender Equality en Garrido (Ed.), *Mapping online gender-based violence* (1era ed., pp. 141-155). University for Peace.
- Arango, V. (2007). *Paz social y cultura de paz*. Ediciones Panamá.
- Atta, M. (2022). The Role of Civil Society in Combating Online Gender-Based Violence en Garrido (Ed.), *Mapping online gender-based violence* (1era ed., pp. 93-109). University for Peace.
- BBC News Mundo. (25 de noviembre de 2019). Goo Hara, la estrella de 28 años de K-Pop encontrada muerta en su casa. *BBC News Mundo*.
- BBC. (18 de julio de 2018). Roblox blames 'gang rape' on hacker adding code to game. Obtenido de <https://www.bbc.com/news/technology-44875920>
- Browning, K. (2020). Return of the King: Ninja, a Video Game Star, Goes Back to Twitch. *The New York Times*. <https://www.nytimes.com/2020/09/10/business/ninja-stream-twitch.html>
- Burgess, J., Jahr, M., Keljo, J., Schroeder, J., & Sweitzer, W. A Rape in Cyberspace. N/A, N/A, N/A. <https://cs.stanford.edu/people/eroberts/cs181/projects/controlling-the-virtual-world/history/rape.html>
- Bustamante Donas, J. (2001). Hacia la cuarta generación de Derechos Humanos: repensando la sociedad tecnológica. *CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación*, (1).
- Corritore, C., Kracher, B., & Wiedenbeck, S. (2003). On-line Trust: Concepts, Evolving Themes, a model. *International Journal of Human-Computer Studies*, 58, 737-758.
- Davenport, D. (2002). Anonymity on the Internet: Why the Price Be Too High. *Communications of the ACM*, 45, 33-35. <https://dl.acm.org/doi/epdf/10.1145/505248.505267>

- Decreto de Urgencia 007-2020, Exposición de motivos, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, Diario Oficial *El Peruano*, 9 de enero de 2020 (Perú), p. 13. https://www.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/du_interregno_2020/du-007-2020.pdf
- Dunn, S. (2020). *Technology-Facilitated Gender-Based Violence: An Overview*. Centre for International Governance Innovation. <https://www.jstor.org/stable/resrep27513>
- Escobar de la Serna, L. (1998). *Derecho a la Información*. Editorial Dykinson S.L.
- European Union Agency for Network and Information Security [ENISA] & Cybersecurity Coordination Group [CSCG]. (2015). *Definition of cybersecurity: gaps and overlaps in standardisation*. https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf
- Falco, G. y Rosenbach, E. (2022). *Confronting cyber risk: An embedded endurance strategy for cybersecurity: gaps and overlaps in standardisation*. Oxford University Press.
- Federal Communications Commission [FCC]. (2024). *The Infrastructure Investment and Jobs Act: Prevention and Elimination of Digital Discrimination*. Federal Register. https://www.federalregister.gov/documents/2024/01/22/2023-28835/the-infrastructure-investment-and-jobs-act-prevention-and-elimination-of-digital-discrimination?utm_source=chatgpt.com
- Fequiere, R. (25 de octubre de 2024). *The Remarkable Life of Ibelin Is an Emotional Ode to Connection and Gaming*. TUDUM. <https://www.netflix.com/tudum/articles/ibelin-release-date-trailer-news>
- Flores Dapkevicius, R. (2021). *Tratado de Derecho Constitucional* (tomo I, 2da ed.). La Ley Uruguay.
- Freixes Sanjuán, T. (1992). *Constitución y derechos fundamentales: Estructura jurídica y función consitucional de los derechos*. Barcelona: PPU.
- GATOYRATÓN, Soluciones para el acoso escolar. (2015). *La despedida de Amanda Todd, un golpe de realidad para entender que el #bullying no es un juego* [video]. <https://www.youtube.com/watch?v=L1bTlq7o1EE&rc=1>
- Hainsworth, J. (17 de abril de 2014). Dutch man's case linked to Amanda Todd. *MSN News*. <https://web.archive.org/web/20140421074026/http://news.msn.com/crime-justice/dutch-mans-case-linked-to-amanda-todd>
- Hubbard, D. y Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Wiley. https://duikt.edu.ua/uploads/l_2077_77796609.pdf
- Landa Arroyo, C. R. (2002). Teorías de los Derechos Fundamentales. *Cuestiones Constitucionales. Revista Mexicana De Derecho Constitucional*, 1(6) [49-71].
- (2017). *Los Derechos Fundamentales*. Lima: Fondo Editorial PUCP.
- Lanier, L. (5 de julio de 2018). Video Game 'Roblox' Showed a 7-Year-Old Girl's Avatar Being Raped. (Variety, Ed.) <https://variety.com/2018/gaming/news/roblox-little-girl-avatar-raped-1202865698/>
- Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.
- Lim, D., Zo, H., & Lee, D. (5-6 de mayo de 2011). *The Value of Anonymity on the Internet*. [Conferencia]. Conference: Service-Oriented Perspectives in Design Science Research - 6th International Conference. Milwaukee: Estados Unidos.
- Lin, J., & Latoschik, M. (2022). Digital body, identity and privacy in social virtual reality: A systematic review. *Journal Frontiers in Virtual Reality*, 1-25.
- Loewenstein, K. (2018). *Teoría de la Constitución*. Barcelona: Editorial Ariel.
- Mann, L. (1981). The Baiting Crowd in Episodes of Threatened Suicide. *Journal of Personality and Social Psychology*, 41(4), 703-709.
- Martineau, M., Spiridon, E., & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sci*, 3(3), 452-477.
- McClellan, J. (2000). *Liberty, Order, and Justice: An Introduction to the Constitutional Principles of American Government* (Tercera ed.). Liberty Fund.
- Monereo Pérez, J. L. (2023). Sociología crítica del derecho y teoría jurídica en Hans Kelsen. *Re-*

vista de Estudios Jurídico Laborales y de Seguridad Social, (6) [327-349].

National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS* (HC 414 Session 2017–2019). <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>

Núñez Robinson, R. (2021). Informe jurídico de la demanda de inconstitucionalidad recaída en el Expediente 00009-2014-AI/TC para optar por el grade de abogado. Lima: Pontificia Universidad Católica del Perú. <https://tesis.pucp.edu.pe/items/6d4e50e9-12dd-4e93-a00e-72aec47f2f0a>

Núñez, R. (5 de septiembre de 2024). Una introducción al derecho de la ciberseguridad. *Ius 360*. <https://ius360.com/una-introduccion-al-derecho-de-la-ciberseguridad-rodolfo-nunez-robinson/>

Núñez Robinson, R. (2025). El fenómeno de la interconectividad y la ciberseguridad: una introducción al objeto del derecho de la ciberseguridad. *Análisis Jurídico-Político*, 7(13), [15-43]. <https://portal.amelica.org/ameli/journal/702/7025402001/7025402001.pdf>

Núñez Robinson, R., & Núñez Robinson, D. (3 de octubre de 2024). La admisibilidad y procedencia de la evidencia cibernética: un enfoque técnico-jurídico desde la lex mercatoria. *Ius360*. <https://ius360.com/la-admisibilidad-y-procedencia-de-la-evidencia-cibernetica-un-enfoque-tecnico-juridico-desde-la-lex-mercatoria/>

O'Reilly, D. (17 de diciembre de 2007). Five ways to protect your privacy online. *CNET News*. <https://www.cnet.com/tech/services-and-software/five-ways-to-protect-your-privacy-online/>

Organización Internacional de Normalización / Comisión Electrotécnica Internacional. (2020). *Information technology –Cybersecurity– Overview and concepts* (ISO/IEC TS 27100:2020). <https://cdn.standards.iteh.ai/samples/72434/f9ad5982cca44476854567d778f7e579/ISO-IEC-TS-27100-2020.pdf>

Ortiz, S. M. (2020). Trolling as a Collective Form of Harassment: An Inductive Study of How Online Users Understand Trolling. *Social Media + Society*, 6(2), 1-9.

Pevac, M. (2022). Tertiary Victimization of Sexual Violence Victims Online: How the Internet

Needs to Become a Safer Space for Women en Garrido (Ed.), *Mapping online gender-based violence* (1era ed., pp. 53-70). University for Peace. <https://upeace.org/wp-content/uploads/2024/04/Garrido-Mapping-Online-Gender-based-Violence.pdf>

Phillips, T. (27 de febrero de 2019). “I do not condone child pornography, white supremacy, or racism”. *EUROGAMER*.

Ralston, W. (11 de noviembre de 2020). The untold story of a cyberattack, a hospital and a dying woman. *WIRED*. <https://www.wired.com/story/ransomware-hospital-death-germany/>

Ree, B. (Dirección). (2024). *The Remarkable Life of Ibelin* [Documental]. Netflix.

Riofrío Martínez-Villalba, J. C. (2014). La cuarta ola de derechos humanos: los derechos digitales. *Revista Latinoamericana de Derechos Humanos*, 25(1), 15-45. <https://www.revistas.una.ac.cr/index.php/derechoshumanos/article/view/6117>

Rubio Correa, M., Eguiguren Praeli, F., & Bernales Ballesteros, E. (2010). *Los Derechos Fundamentales en la jurisprudencia del Tribunal Constitucional: análisis de los artículos 1, 2 y 3 de la Constitución*. Lima: Fondo Editorial PUCP. <https://repositorio.pucp.edu.pe/items/c05d3e58-1543-42cc-823a-07d992fac75b>

Sales, N. J. (5 de enero de 2024). A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future? (T. Guardian, Ed.) Obtenido de <https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta>

Silva, A., & Pinheiro, R. (2021). Bens jurídicos lesados no crime de pornografia de vingança e sua efetiva tutela penal na lei Maria Da Penha. *Duc In Altum - Cadernos De Direito*, 12(28). <https://doi.org/10.22293/2179-507x.v12i28.1434>

Srinivasan, S., & Ni, L. K. (2023). *Ransomware attack at a Springhill Medical Center*. Harvard Business School Case No. 123-065. <https://www.hbs.edu/faculty/Pages/item.aspx?num=63611>

Stonehouse, R. (29 de mayo de 2019). Roblox: ‘I thought he was playing an innocent game’. (BBC, Ed.). <https://www.bbc.com/news/technology-48450604>

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7, 321-326.

<https://www.liebertpub.com/doi/10.1089/1094931041291295>

Syahriani Putri, G., & Rahmi Pratiwi, M. (2024). Instagram as A Digital Media to Build Self-Acceptance. *Scriptura*, 13(2), 129-141.

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. <https://www.onlinelibrary.iuhl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf>

Styczynski, J., & Beach-Westmoreland, N. (2019). *When the Lights Went Out: A Comprehensive Review of the Attacks on Ukrainian Critical Infrastructure*. Booz Allen Hamilton. <https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>

Tecnologías para la privacidad y la libertad de expresión: reglas sobre el anonimato y cifrado. Chile en el contexto latinoamericano. (2017). Derechos Digitales. <https://www.derechosdigitales.org/wp-content/uploads/anonimato-y-cifrado.pdf>

The Duc Tam, N. (2022). Fighting Against Gender-Based Abuse of Deepfakes Technology: Are We Only Tackling the Tip of the Iceberg? en Garrido (Ed.), *Mapping online gender-based violence* (1era ed., pp. 23-33). University for Peace. <https://upeace.org/wp-content/uploads/2024/04/Garrido-Mapping-Online-Gender-based-Violence.pdf>

United States Government Accountability Office. (2018). *Weapon systems cybersecurity*.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>

Waxman, M. (2020). *Cyberattacks and the Constitution*. [Ensayo académico, Stanford University]. Hoover Working Group on National Security, Technology, and Law. https://www.hoover.org/sites/default/files/research/docs/waxman_webready.pdf

Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 2, 140-175. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=2282&context=faculty_scholarship

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Constitución Política del Perú [Const.] (1993).

Corte de Apelaciones de Kentucky, 15 de noviembre de 1927, *Brents v. Morgan* (Estados Unidos)

Decreto Supremo 014-2013-MTC, Reglamento de la Ley 29904, Ley de promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica. Diario Oficial *El Peruano*, 4 de noviembre de 2013 (Perú).

Decreto de Urgencia 007-2020, Decreto de Urgencia que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento, Diario Oficial *El Peruano*, 9 de enero de 2020 (Perú).

Ley 29733, Ley de protección de datos personales. Diario Oficial *El Peruano*, 3 de julio de 2011 (Perú).

Ley 29904, Ley de promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica. Diario Oficial *El Peruano*, 24 de abril de 2015 (Perú).

Ley 31878, Ley de reforma constitucional que promueve el uso de las tecnologías de la información y la comunicación, y reconoce el derecho de acceso a internet libre en todo el país, Diario Oficial *El Peruano*, 23 de agosto de 2023 (Perú).

Ley 30999, Ley de ciberdefensa, Diario Oficial *El Peruano*, 27 de agosto de 2019 (Perú).

Resolución Ministerial 00292-2022-PRODUCE, 2 de septiembre de 2022 (Perú).

The Constitution of the United States [Const.] (1789).

Tribunal Constitucional [T.C.], 19 de agosto de 2002, sentencia recaída en el Expediente 0895-2001-AA/TC (Perú).

Tribunal Constitucional [T.C.], 24 de octubre de 2002, sentencia recaída en el Expediente 080-2002-AA/TC (Perú).

Tribunal Constitucional [T.C.], 6 de noviembre de 2002, sentencia recaída en el Expediente 0018-2001-AI/TC (Perú).

Tribunal Constitucional [T.C.], 6 de diciembre de 2002, sentencia recaída en el Expediente 1042-2002-AA/TC (Perú).

Tribunal Constitucional [T.C.], 2 de diciembre de 2003, sentencia recaída en el Expediente 1363-2002-AA/TC (Perú).

Tribunal Constitucional [T.C.], 20 de abril de 2004, sentencia recaída en el Expediente 2945-2003-AA/TC (Perú).

Tribunal Constitucional [T.C.], 5 de mayo de 2004, sentencia recaída en el Expediente 0075-2004-AA/TC (Perú).

Tribunal Constitucional [T.C.], 12 de julio de 2011, Sentencia Rol 1894-2011-CPR (Chile).

Tribunal Constitucional [T.C.], 6 de agosto de 2020, sentencia recaída en el Expediente 04138-2016-PA/TC (Perú).

Tribunal Constitucional [T.C.], 22 de agosto de 2022, sentencia recaída en el Expediente 02839-2021-PHD/TC (Perú).