LIBRO HOMENAJE DEL ÁREA DE DERECHO CONSTITUCIONAL POR LOS

100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú

César Landa (editor)

Capítulo 6

EPARTAMENTO
CADÉMICO DE
ERECHO

CENTRO DE
INVESTIGACIÓN,
CAPACITACIÓN Y
ASESORÍA JURÍDICA (CICAJ)

ET LUX IN TENEBRIS LUCET
MCMXVII
PUCP

LIBRO HOMENAJE DEL ÁREA DE DERECHO CONSTITUCIONAL POR LOS

100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú

LIBRO HOMENAJE DEL ÁREA DE DERECHO CONSTITUCIONAL POR LOS

100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú

DEPARTAMENTO ACADÉMICO DE **DERECHO**

CENTRO DE **INVESTIGACIÓN, CAPACITACIÓN Y ASESORÍA JURÍDICA (CICAJ)**

PUCP

Libro homenaje del Área de derecho constitucional por los 100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú
César Landa (editor)

Imagen de cubierta: Justicia/www.freepik.es
Primera edición: Octubre 2019
Tiraje: 500 ejemplares

Corrección de estilo: Thaïs Luksic y Mercedes Dioses

Impresión: Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156 - Breña
tareagrafica@tareagrafica.com
Teléf.: (51-1) 332-3229
Octubre 2019

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2019-16064
ISBN: 978-612-47151-6-7

Impreso en el Perú - Printed in Peru

CONTENIDO ESENCIAL DEL DERECHO FUNDAMENTAL A INTERNET: TEORÍA Y PRAXIS

César Landa[1]

En el Perú la mitad de la población –15 millones de habitantes– está conectada al Facebook, y existen alrededor de 35 millones de teléfonos celulares (El Comercio, 2016). La interconectividad crece año a año, gracias al uso de las nuevas tecnologías de la comunicación, como Internet, que está modificando no solo el goce y ejercicio de los derechos fundamentales, particularmente aquellos referidos a la libertad de expresión y el derecho a la intimidad, sino que también ha supuesto un replanteamiento del modelo de organización social, cultural y económica del Estado y los ciudadanos.

En ese sentido, el Perú no es ajeno al cambio de los paradigmas mundiales de la economía y la política acontecido tras el rápido proceso de la caída del Muro de Berlín, que fue la expresión del cambio del modelo político y económico universal hasta entonces vigente. Dicho orden estaba basado en la tensión entre el capital y el trabajo, tensión que ordenó a los países bajo la órbita de los Estados Unidos, con los valores de la libertad y el mercado, o de la otrora Unión Soviética, con los valores del trabajo y el Estado.

El cambio fue muy importante: se cerró el modelo de confrontación de la Guerra Fría entre los dos sistemas ideológicos mundiales, que se transformó en una sociedad global de la comunicación y la tecnología. En ese escenario, el Internet, en tanto un producto del desarrollo científico al servicio de la sociedad, permite el acceso a información, y su almacenaje, procesamiento y transmisión, que se viene incrementado exponencialmente en la actual "era digital". En relación con lo indicado, por ejemplo, un disco de almacenaje fijo o portátil de un terabyte puede guardar 300 horas de video o 3.6 millones de fotografías digitales estándar. Asimismo, un terabyte puede almacenar el equivalente a mil copias de la Enciclopedia Británica digital.

El contexto de una sociedad de la información, modelo de sociedad promovido por los países "desarrollados" en la era posindustrial, constituye una oportunidad estratégica para las sociedades en vías de desarrollo, que puede contribuir a superar su situación de retraso económico y social, así como a potenciar la protección y desarrollo de los viejos y nuevos derechos fundamentales, a través del Internet y las nuevas tecnologías, en la medida en que la defensa de la persona humana y el respeto de su dignidad es el fin supremo de la sociedad y del Estado, según dispone el artículo 1 de la *Constitución Política del Perú* (1993).

Así, en el Perú la convergencia de las tecnologías de la informática –equipos y software–, las telecomunicaciones –televisión y radio– y la comunicación digital –telefonía móvil– está generando aceleradas transformaciones de índole social, económica y política. En esta era

---

1 Expresidente del Tribunal Constitucional, profesor de Derecho Constitucional en la Pontificia Universidad Católica del Perú y en la Universidad Nacional Mayor de San Marcos

digital, el Internet se está convirtiendo en un nuevo *bien de dominio público* del siglo XXI, por cuanto su acceso alcanza progresivamente a casi todos los ciudadanos, interesados o no. Asimismo, esta tecnología también está permitiendo expandir el control del Estado y las corporaciones sobre la vida privada de las personas.

A la luz de los argumentos expuestos sobre la importancia del acceso al internet en la sociedad actual, el objetivo del presente texto es analizar el acceso a y el uso del Internet como un nuevo derecho fundamental en sí mismo, que tiene impacto en todos los ámbitos de la vida humana, particularmente perfilando su naturaleza y contenido esencial, así como analizando la escasa jurisprudencia administrativa sobre la materia que muestra el control de los excesos de las empresas y también de los usuarios de las relaciones digitales, lo cual pone en evidencia la necesidad de regular los alcances y los límites del Internet, en un balance con los derechos fundamentales.

Internet y Derechos Fundamentales

Como ya se ha expresado previamente,

> El Internet constituye el ícono de la sociedad de la información, en la medida que facilita la creación, el acceso, el almacenamiento, el procesamiento y la distribución de la información; jugando un papel esencial en las relaciones sociales, culturales y económicas entre las autoridades, las empresas y los ciudadanos, y, entre estos entre sí. En esta nueva etapa de transformación del Estado y la sociedad, el Internet es el fundamento principal para construir la nueva identidad de los derechos fundamentales. (Landa, 2016, p. 2)

En el marco del nuevo paradigma de la sociedad de la información y del conocimiento, el Internet se convierte en un derecho fundamental (García 2016; Fernández, 2004), en la medida en que faculta a todas las personas, a través de las nuevas tecnologías, a ampliar sus posibilidades de goce, y ejercicio de los derechos y libertades clásicos, especialmente potencializando directamente a aquellos referidos a la libertad de expresión y el libre acceso a la información (Consejo de la Unión Europea, 2014).

Es más, en la medida en que los derechos fundamentales son "universales, indivisibles e interdependientes" (Declaración y Programa de Acción de Viena, art. 5), el Internet los integra digitalmente y permite que trasciendan más allá de las fronteras de los Estados nacionales, no solo para el goce del mismo, sino también para su defensa y protección. Por ello, la Organización de las Naciones Unidas ha llegado a declarar el Internet como un derecho humano (Carballo, 2016), lo cual implica que los Estados deben cumplir con nuevos compromisos internacionales en esta era digital.

En ese entendido, el Internet constituye no solo un derecho fundamental, sino que también es una garantía institucional de la democracia, en la medida en que se constituye en una necesidad social para acceder, y gozar a plenitud los derechos y libertades reconocidos en la Constitución y los tratados internacionales de derechos humanos.

Contenido Esencial del Derecho al Internet

Como todo derecho fundamental, el derecho al Internet debe contar con un contenido esencial constitucionalmente protegido, que se derive de la articulación de los derechos referidos "a 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" ("Constitución Política del Perú" [CP], 1993, art. 2-4); "a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, exceptuando las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional" (CP, 1993, art. 2-5); "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" (CP, 1993, art. 2-6); y "al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias" (CP, 1993, art. 2-7), básicamente.

En ese sentido, ya que el Internet entrelaza directamente los derechos fundamentales mencionados, adquiere una naturaleza de bien de dominio público, que el Estado tiene la responsabilidad de asegurar a toda persona como un derecho autónomo, mediante un conjunto de atributos en su contenido constitucionalmente protegido, los cuales se desarrollan a continuación.

Acceso a Internet

El acceso informado y consentido a Internet es una condición indispensable para poder gozar no solo de las libertades comunicativas, sino de todos los demás derechos fundamentales. No obstante, como el Internet consiste en un sistema de grandes redes interconectadas, ello supone dos condiciones: en primer lugar, que las personas cuenten con un equipo –hardware– y un programa –software– que les permita acceder al Internet; en segundo lugar, que exista una infraestructura de comunicación –eléctrica, plataforma satelital y/o cableado dorsal de fibra óptica–, a cargo del Estado, las empresas y, particularmente, el sistema educativo. Al respecto, el Ministerio de Educación cuenta con una plataforma, Perú Educa. Sistema Digital para el Aprendizaje (http://www.perueduca.pe/) y su aula virtual (http://aulavirtual.perueduca.pe/), que aprovechan el Internet para ofrecer a los docentes, a nivel nacional, diversos cursos formativos y de complementación pedagógica, además de información de interés para el desempeño de su función educativa.

Sin embargo, en el Perú el acceso público a Internet tiene un costo, incluyendo los costos referidos al soporte necesario para el acceso, mientras que en algunos países de la región este es gratuito, gracias a las políticas de Estado orientadas a mejorar la educación pública básica e incluso la integración social de los jubilados. Tal es el caso de la República Oriental del Uruguay, que, con el objetivo de brindar el soporte necesario para el acceso al internet, ya ha entregado, a través del Plan Ceibal, un millón de computadoras portátiles a escolares de 4 a 6 años (Pulso, 2013); asimismo, en 2015 empezó a entregar tablets a los jubilados para posibilitar, en ambos casos, su acceso al entorno digital e integrarlos a la sociedad de la información (Emol, 2015).

La inclusión digital de determinados grupos humanos vulnerables –particularmente en las zonas rurales– es importante, así como poner el acceso a Internet al alcance de la ciudadanía

en espacios y recintos públicos como plazas, parques, bibliotecas, escuelas, universidades, centros comunitarios, hospitales, aeropuertos, instituciones públicas, y demás espacios de infraestructura y servicios públicos.

Para asegurar el acceso a Internet, informado y consentido, se debe ofrecer también equipos y servicios de calidad básica, que deben ir mejorando en función de los nuevos desarrollos tecnológicos, así como garantizar la libertad de elección del sistema, aplicación y uso de los programas, para evitar la concentración y/o las posiciones dominantes en el mercado de hardware y software, para lo cual, se debe asegurar el acceso universal, mediante la interconectividad de los protocolos e infraestructuras de comunicación. Es eso lo que se ha establecido como el *principio de neutralidad*, que en el Perú ha sido regulado mediante el *Reglamento de Neutralidad de Red aprobado* por Resolución del Consejo Directivo 165-2016-CD/OSIPTEL.

Al Estado también le compete regular el acceso a Internet en condiciones de igualdad, sin discriminación por razones de origen, sexo, raza, religión, opinión política, idioma, nacionalidad, condición económica o de cualquier otra índole, ello sin perjuicio del establecimiento de políticas de acción afirmativa para facilitar el acceso a personas en situación de discapacidad y a comunidades marginadas, especialmente. Debe promoverse que las corporaciones privadas no establezcan barreras arbitrarias o desproporcionadas para dicho acceso, sino más bien condiciones amigables para todas las personas.

En ese entendido, la protección del libre acceso –informado y consentido– a Internet requiere pues de neutralidad, para garantizar la pluralidad y la diversidad del flujo informativo, por cuanto el Internet es un bien de dominio público que permite la interconexión entre las personas. Por ello, el Estado debe asegurar el intercambio libre, abierto, equitativo y sin discriminación de la comunicación e información (Téllez 2015) mediante una regulación sin privilegios personales u obstáculos por razón de contenidos políticos, económicos, culturales o sociales, lo cual no se opone a que puedan expedirse leyes especiales requeridas por la naturaleza de las materias a ser reguladas, más no por la diferencia entre las personas, tal como dispone el artículo 103 de la Constitución.

Libertad del uso de Internet

Toda persona tiene derecho a la libertad personal en el marco de su libre desarrollo y bienestar, en la medida en que "nadie está obligado a hacer lo que la ley no manda, ni impedido de hacer lo que ella no prohíbe" (CP, 1993, art. 2-24-A). Sin embargo, todo sujeto también debe gozar de la protección de su libertad frente a los peligros de una actuación desproporcionada o arbitraria de parte de los poderes públicos y privados.

El "Internet debido a su naturaleza multidireccional e interactiva, su velocidad y alcance global a un relativo bajo costo y sus principios de diseño" abierto y descentralizado (Comisión Interamericana de Derechos Humanos, 2013, p. 17), también es un medio que posibilita el robo de la identidad digital, el intrusismo, el uso indebido de datos por terceros y el ciberacoso, entre otras formas de delito que se cometen utilizando dicha red. Por ello, es necesario que el Estado tome medidas especiales, tales como políticas de educación y campañas de prevención, y que combata los actos delictivos a nivel nacional e internacional (Ortego, 2015; Villavicencio, 2015).

Además de los delitos informáticos, también se cometen abusos en cuanto al uso o administración de Internet, los cuales configuran conflictos de derechos o potestades entre los

usuarios y los proveedores. En ese sentido, en el Perú, tal como sucedió antes en Europa, se ha sancionado a Google por no retirar los datos personales de un ciudadano peruano que atravesó un proceso penal del cual ya había sido absuelto (en la sección "Derecho al olvido digital" del presente trabajo se dan más detalles del caso). Respecto de ese tipo de casos, el Tribunal de Justicia de la Unión Europea ha reconocido el derecho a

> Solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. (2014, párr. 99).

Por lo tanto, es constitucional que el Estado busque garantizar la libertad del uso de Internet, aunque regulando la resolución de conflictos y señalando las ulteriores responsabilidades, con criterios de legitimidad y ponderación, en el ámbito de los derechos digitales.

Dicha labor es particularmente crucial debido a que durante los últimos años se han planteado desafíos y conflictos entre el entorno digital y la libertad de expresión; la libertad de información y acceso a la información pública; el derecho a la autodeterminación informativa, a la privacidad y al honor público; los derechos de autor; y el interés superior de niñas, niños y adolescentes (Orizaga & Cabrera 2015). En dichos casos debe garantizarse la protección de contenidos mínimos, regulando los alcances del derecho a Internet.

Ahora bien, cualquier regulación o restricción de los derechos digitales a los proveedores y/o usuarios debe cumplir una serie de requisitos: a) expedición de una ley; b) legitimidad constitucional de la finalidad restrictiva; c) necesidad, idoneidad y proporcionalidad de la medida restrictiva; d) garantías judiciales de control; y e) respeto al debido proceso.

No obstante, deben existir medidas obligatorias por parte del Estado, o de las propias empresas intermediarias, de filtrado, bloqueo o suspensión de portales web, direcciones IP, enlaces (links), datos, extensiones de nombre de dominio, puertos, protocoles de red y sitios web del servidor en los que están alojados, que solo deberían ser admisibles cuando contengan materiales ilícitos o sean usados con fines ilícitos. Esta tarea debe ser determinada por el Estado, y aplicarse a las empresas en tanto violen los términos contractuales y/o de uso establecidos, de conformidad con la ley y los principios constitucionales.

Lamentablemente, ante el vertiginoso avance de las nuevas tecnologías, la regulación estatal se encuentra rezagada, por lo que el usuario se encuentra la mayoría de veces desprotegido ante las empresas proveedoras de servicio de Internet (PSI) y de alojamiento de sitios web, las plataformas de redes sociales y los motores de búsqueda. Dichas empresas limitan o condicionan la conexión entre usuarios a través de plataformas de redes sociales, alojamiento de material publicado y búsquedas en la red, trasmisión, procesamiento y ordenación del tráfico, transacciones financieras, etc. Con ello se afecta el derecho del consumidor a elegir con información y opciones suficientes entre los distintos equipos, programas y servicios de Internet, derecho a la información que el Estado tiene la obligación de defender (CP, 1993, art. 65).

Esta concepción sobre los retos para asegurar el acceso al internet asume que el negocio del Internet es global, en la medida en que los proveedores de internet brindan servicios de acceso e interconexión al Internet que incluye el acceso a programas, sitios web, motores de búsqueda y redes sociales. En este escenario también se producen pugnas entre las empresas

de telecomunicaciones y/o las empresas informáticas por conformar monopolios u ocupar posiciones dominantes del mercado, lo cual pone a veces en peligro la libertad de acceso en igualdad de condiciones a todos los servicios de Internet –principio de neutralidad–. Así, por ejemplo, empresas como Verizon y AT&T en Estados Unidos sostienen que la regulación del Internet como un servicio público sometido al principio de neutralidad de la red restringe y desalienta la inversión que realizan en dicho rubro del mercado. Por el contrario, otras empresas, como Twitter, Netflix y Yelp, consideran que es necesario asegurar que los proveedores de Internet eviten acuerdos que puedan favorecer un servicio y bloquear el de la competencia (Associated Foreign Press, 2016).

Seguridad en Internet

Con el vertiginoso desarrollo de las nuevas tecnologías, la seguridad de los internautas se ha puesto en peligro, no solo debido al aumento de la delincuencia informática, sino también por los excesos cometidos por las empresas proveedoras de Internet y por la intrusión del Estado en las supuestas actividades sospechosas de los internautas. Esta situación demanda establecer medidas de seguridad que supongan restricciones a la libertad del Internet, las cuales deben plantearse sobre la base de los principios de legalidad, necesidad y proporcionalidad.

La llamada *ciberseguridad* abarca la infraestructura y las "redes a través de las cuales se provee el servicio de Internet" (OEA, 2013, fundamento 118). Para garantizar la ciberseguridad, se requiere que los titulares disfruten de conexiones seguras en Internet, cautelen la reserva de sus claves de acceso, y tomen precauciones contra la acción ilícita de los *hackers y crackers* (Varela, 2016; Nieto, 2016).

Para proveer seguridad sin afectar el contenido esencial del derecho al acceso a Internet, y a la libertad e igualdad al respecto, es importante delimitar el alcance de la ciberseguridad. Partir de una concepción demasiado amplia de la misma podría afectar desproporcionadamente "la integridad de las redes e infraestructura de Internet", así como la "integridad y confidencialidad de la información que contienen [los cibernautas]" (OEA 2013, fundamento 119). Sin embargo, desde una concepción más limitada, solo debería sancionarse actos y prácticas que puedan afectar el honor, la intimidad, la privacidad o, incluso, los derechos de autor, entre otros que no merecen una respuesta penal, sino civil o administrativa.

Esta postura se fundamenta en que se debe otorgar una posición jurídica preferente al ejercicio de la libertad de expresión, acceso a la información y difusión del pensamiento, facultades que, aun pudiendo ejercerse con abuso del derecho, desviación o exceso de poder, o desde una posición dominante en el mercado, *prima facie* no merecen rechazo penal, Dichos actos o medidas que provienen de usuarios, proveedores y autoridades del Estado constituyen una garantía institucional de las sociedades democráticas, pluralistas y tolerantes, orientada a contribuir al mayor tráfico de ideas y críticas a partir del establecimiento del derecho a Internet con libertad, igualdad y seguridad para todos los internautas.

En ese sentido, las políticas y regulaciones legales deben ser proporcionales a los riesgos a los que se enfrenta la sociedad digital; deben plantearse ponderando el ejercicio de los derechos fundamentales y la seguridad ciudadana. Asimismo deben hacerse públicos los acuerdos establecidos con los intermediarios privados, así como las medidas de seguridad que implementan los proveedores de servicios.

Privacidad e Internet

Si bien el derecho establece que nadie puede ser objeto de interferencias arbitrarias en su vida privada, su domicilio o su correspondencia, también es cierto que, en la sociedad de la información y del conocimiento, toda persona debe estar registrada en diversas bases de datos de sistemas informáticos, tanto públicos como privados, para poder gozar y ejercer de sus derechos fundamentales. No obstante, todo individuo también tiene derecho a mantener un espacio individual y familiar privado, ajeno al Estado y a terceros, y en ese ámbito desarrollar su proyecto personal de vida, manteniendo en secreto los datos que allí se generen según considere necesario, así como a ejercer el derecho a la propia imagen de terceros (Córdoba & Diez-Picazo, 2016) .

Al respecto, la protección de datos personales y la protección del discurso anónimo resultan esenciales para lograr la compatibilidad del derecho a la información y el derecho a la libertad de expresión con el derecho a la privacidad. La protección de datos personales, reconocida mediante el derecho a la autodeterminación informativa consagrada en el artículo 2.6 de la Constitución de 1993, requiere que el Estado regule el almacenamiento, procesamiento, uso y transferencia de los mismos. Es decir, debe prohibir el uso de datos que viole derechos fundamentales, especialmente información vinculada a la intimidad personal y familiar. Asimismo, le corresponde asegurar el derecho del titular al acceso a dichos datos, así como la razonable corrección o supresión de los mismos de las intromisiones indebidas.

Para tal efecto se aplica el hábeas data, el proceso constitucional reconocido en el artículo 200.3 de la Constitución, desarrollado en el artículo 61 del *Código Procesal Constitucional,* que tutela no solo el derecho a la autodeterminación informativa, sino también el derecho de acceso a la información pública.

La posibilidad de participar en el debate público a través de la redes sociales (Sanjurjo, 2015) sin revelar la propia identidad es una garantía de las democracias modernas. Así se protegen aquellos usuarios que podrían sufrir represalias por la difusión de sus opiniones críticas sobre los poderes públicos o privados. En algunos casos, por ejemplo, se ha convocado a movilizaciones ciudadanas, sobre todo entre los jóvenes, para manifestarse u organizarse políticamente para cuestionar medidas arbitrarias tomadas por el gobierno peruano, como la "Repartija"[2] o la llamada "Ley Pulpín[3]" (Cisneros, s. f.), tal como sucede en otras latitudes del mundo, para enfrentarse contra autoridades dictatoriales y/o corruptas, como en Egipto, Libia o Marruecos durante la Primavera Árabe (Cortes, 2012).

Sin embargo, el anonimato no protege de forma absoluta al usuario del acceso o difusión de su información. Por ejemplo, si se trafica con pornografía infantil, se hace propaganda a favor de la guerra, o se incurre en apología al odio racial o sexual, o al genocidio, la autoridad competente tendría la legitimidad para develar la identidad del emisor, y tomar las medidas administrativas y/o judiciales correspondientes.

Desde luego, los registros informáticos de las entidades públicas o privadas deben contar con las medidas de seguridad adecuadas en aquellos casos que lo requieran. Por ejemplo, en el caso de transacciones comerciales o interacciones sensibles, la identificación y autenticación

2 Se refiere a las negociaciones en el Congreso durante las elecciones para elegir nuevos integrantes del Tribunal Constitucional en el 2013 que se entendió que tenían como objetivo elegir personas que favorecieran determinados intereses.

3 Ley que promueve el acceso de Jóvenes al Mercado Laboral y a la Protección Social Ley Nº 30288, conocida como "Ley Pulpín" como referencia a los y las jóvenes ("pulpines") a quienes estaba dirigida la ley.

de los usuarios en línea es una garantía de la seguridad jurídica de la transacción, siempre conforme al principio de proporcionalidad en función del tipo de riesgo, alto o intermedio, que exista. Si el riesgo es bajo, el anonimato debe ser la regla a aplicar.

Derecho al uso del seudónimo

Ya que el derecho a Internet no solo implica el acceso a bases de datos y a la conectividad, sino que también permite expande el uso de la libertad expresión, este debe permitírsele a todo usuario identificado o identificable, de acuerdo con los requerimientos sociales que no infrinjan las normas legales y administrativas, y/o contratos jurídicos.

Los usuarios son todas aquellas personas que gozan de derechos fundamentales que permiten el amplio acceso y uso eficiente de Internet, como lo son el derecho a la *seudonimización* o anonimato –el empleo de un *nickname* o alias–, para el acceso a la información pública, lo que les permite garantizar tres derechos fundamentales (Arroyo, 2016).

Libertad de expresión. El anonimato permite que tengan lugar denuncias, públicas y privadas, que ponen al descubierto las prácticas contrarias al orden o la opinión pública en las que incurren grandes poderes. Sin embargo, cabe señalar que el anonimato también puede ser usado para producir y difundir información falsa –*fake news*–, pornografía infantil, y discursos de odio, acoso y hostilización contra determinadas personas. En dichos casos, la anonimia del agresor y/o emisor es una traba para poder identificarlo.

Estas situaciones de agresión, violación y manipulación de la opinión pública deben ser una preocupación para el Estado, que debería regular el anonimato, absteniéndose siempre de controlar el acceso a todos los contenidos que circulan en Internet, por cuanto la esencia de Internet es la libre interconectividad entre los usuarios, esto es, el traslado de información sin restricción, tal como se refleja en los derechos de acceso a la información, libertad de información, libertad de opinión y expresión.

Privacidad. La existencia de "los datos personales seudonimizados [*nickname*]– que cabría atribuir a una persona física" (Parlamento Europeo y el Consejo de la Unión Europea, 2016, cndo. 26) constituye un derecho que tiene la finalidad de proteger la esfera de la intimidad, ante las distintas formas intrusiones y violaciones, tanto de particulares como de agentes el Estado. Ello no es óbice para que una persona física sea identificable, directa o indirectamente, por razones objetivas derivadas de infracciones respecto a sus deberes públicos u obligaciones privadas previstas en la ley.

Es consecuencia, "los principios de protección de datos no deben aplicarse a la información anónima" de forma absoluta, salvo a aquella información que no guarda relación con la infracción de bienes públicos y derechos privados imputable a la persona física "anonimizada", "ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo" (Parlamento Europeo y el Consejo de la Unión Europea, 2016, cndo. 26).

Seguridad personal. El anonimato protege a los usuarios en las redes, en la medida en que no es posible o resulta más "complicado que alguien atente contra el usuario anónimo" (Arroyo, 2016, p. 2). Durante la Primavera Árabe, proceso en el cual el uso de redes sociales cambió el curso de años de gobiernos autoritarios, a partir de una simple foto subida a Internet

y viralizada por las redes sociales. Asimismo, el anonimato fue empleado en la campaña de las elecciones presidenciales de los Estado Unidos para favorecer al candidato Trump y atacar a su competidora, Clinton, a través de Twitter y Facebook, práctica que jugó un rol a veces determinante (Arroyo, 2016).

No obstante, al igual que en el ejercicio de los derechos comunicativos, el Estado debería establecer regulaciones sobre el anonimato en Internet, "en situaciones muy excepcionales y avaladas por los instrumentos internacionales como lo prevé la Convención Americana de Derechos Humanos en el Artículo 13" (Arroyo, 2016, p. 4, inc. 4). Si bien el uso de Internet bajo el anonimato ha "permitido que voces no escuchadas salgan a la luz y ello dentro de un modelo democrático es lo deseable" (Arroyo, 2016, p. 3), también ha hecho posible que se pueda manipular la voluntad popular en las democracias abiertas.

En consecuencia, se debe considerar el anonimato o seudonimización como un aspecto esencial del acceso a y uso de Internet, en virtud del cual el Estado debería regular el tratamiento de datos personales, el mismo que no debe excluir al responsable del almacenamiento, tratamiento y transmisión de datos, que debe adoptar las medidas técnicas y organizativas necesarias para garantizar que se aplique razonablemente el anonimato en el marco de la protección datos personales. En esa medida la seudonimización o anonimato deben ser concebidos como contenido constitucionalmente protegido por el derecho fundamental a Internet.

Derecho al olvido digital

El desarrollo de Internet ha traído consigo nuevas amenazas a los derechos fundamentales, en la medida que este se constituye como un registro permanente de los datos que allí se suben. De ahí que registros o noticias sobre antecedentes penales, o fotografías y vídeos de situaciones embarazosas almacenados en la red (especialmente en redes sociales) puedan, con el paso del tiempo, ser perjudiciales para la persona e incidir de modo negativo en su vida personal, familiar, social, académica, laboral o profesional.

Frente a dichas situaciones se ha ido construyendo un derecho al olvido o a ser olvidado (*right to oblivion o right to be forgotten*), cuya finalidad consiste, en último término, en la cancelación o supresión de datos de carácter personal (datos de identidad, fotografías, vídeos, noticias, publicaciones de redes sociales, etc.) que estando alojados en Internet puedan afectar a la persona. Según el *Reglamento de Protección de Datos Personales* de la Unión Europa (Reglamento UE), el derecho al olvido es la manifestación del derecho de supresión aplicado de forma concreta a los buscadores de internet (Parlamento Europeo y el Consejo de la Unión Europea, 2016, cnds. 65-66). En la misma línea, puede verse los artículos 4 y 93 de la *Ley Orgánica 3/2018, Ley de Protección de Datos Personas y Garantía de los Derechos Digitales del Reino de España.*

En la doctrina, se discute sus alcances. Por un lado, se señala que dicho derecho al olvido puede ser entendido como un derecho a cancelar o anonimizar los datos de origen legal o jurisprudencial referidos a los antecedentes judiciales o administrativos de las personas, especialmente los de carácter penal, que existen en bases de datos o repertorios disponibles en Internet, una vez que hayan dejado de ser de interés público, y resulten gravosos o el interesado desea que queden en el olvido. Por otro lado, el derecho al olvido también se concibe como el derecho a cancelar información agraviante o difamatoria divulgada mediante fotos, audios o vídeos privados que forman parte del contenido sujeto al derecho a la protección de datos

privados personales, en tanto afectan el honor, la intimidad, la privacidad o la propia imagen de una persona (Martínez, 2015). Así, el derecho al olvido sería el derecho a que se eliminen del Internet ciertos datos de una persona, tanto de las páginas web fuente como de los motores de búsqueda.

Desde la perspectiva jurisprudencial, según los lineamientos de la decisión del Supremo Tribunal de Justicia de la Unión Europea (STJUE), en el caso Google Inc. y Google Spain vs. Agencia Española de Protección de Datos y Mario Costeja González, se consideró que el derecho al olvido debió ser entendido como el derecho del interesado a solicitar que la información sobre su persona ya no se pusiera a disposición del público en general mediante su inclusión en la red, por haber perdido interés la publicación de una orden judicial de remate de sus inmuebles por falta de pago de las cotizaciones sociales al Estado, las cual ya había sido pagada.

El mencionado caso finalmente fue resuelto por el Tribunal de Luxemburgo, que estableció lo siguiente:

> La supresión de la información debía ser efectuada caso por caso en función de criterios muy precisos: naturaleza de la información, su grado de sensibilidad en relación a la vida privada de la persona afectada, y el interés para el público de tener acceso a esta información, noción que cobra importancia cuando la persona objeto del tratamiento de información es conocida públicamente. (Pérez, 2016, p. 182)

Si bien el derecho al olvido

> representa un mecanismo de garantía del derecho al buen nombre de la persona afectada por la difusión de la noticia, implica a la vez un sacrificio innecesario del principio de neutralidad de Internet y, con ello, de las libertades de expresión e información. (Corte Constitucional de Colombia, 2015, punto 9.8.2)

Ello especialmente, si a partir de los principios democráticos y constitucionales se sustenta el interés legítimo por mantener la memoria histórica, tanto general como particular. De hecho, se hace necesario realizar "una ponderación o una fórmula orientada a establecer un adecuado balance entre los derechos y/o bienes en conflicto" (Corte Constitucional de Colombia, 2015, punto 9.8.2).

Las posiciones doctrinales, la sentencia reseñada y la legislación comparada solo son un indicativo de que hay muchos aspectos en torno al concepto y alcances del derecho al olvido que son constantemente discutidos, en tanto un aspecto esencial del derecho fundamental a Internet, dado el vertiginoso desarrollo del entorno digital.

Control de la vigilancia electrónica

Amenazas como el terrorismo, el narcotráfico, la trata de personas y otras modalidades delictivas de alcance nacional y/o internacional han llevado a los Estados a establecer estándares de prevención y persecución de delitos, mediante acuerdos internacionales, que se emplean para desarrollar políticas y leyes nacionales armonizadas con el objetivo de combatir la delincuencia internacional y nacional. En ese sentido, el 23 de noviembre de 2001 el Consejo de Europa aprobó el *Convenio sobre la Ciberdelincuencia* de Budapest, el primer tratado internacional orientado a enfrentar a los delitos informáticos y en Internet, a través de procurar la homogenización de leyes nacionales, y de mejorar las técnicas de investigación y la cooperación policial entre países.

Para ello, el uso de programas o sistemas de vigilancia electrónica de las comunicaciones privadas de acuerdo a la ley resulta ser una medida adecuada y necesaria cuando se la usa de forma estrictamente proporcional a los fines legítimos perseguidos por las autoridades. Por eso la Corte Interamericana de Derechos Humanos (2004) ha planteado los límites de la apelación de algunos Estados a la doctrina de la seguridad nacional, cuando esta es empleada como argumento para vigilar la correspondencia y los datos personales, con el objetivo de evitar la discrecionalidad y excesos en su implementación.

El desarrollo de nuevas tecnologías permite a las industrias de las telecomunicaciones y la informática desarrollar cada vez más sofisticados sistemas, programas y aparatos de vigilancia electrónica, los cuales demandan nuevos estándares de protección de los derechos fundamentales, para evitar que se cometan excesos que afecten tanto a terceros como a los investigados, salvo en los casos en que sea estrictamente necesario. En el caso de que se cometan excesos, deben existir mecanismos de control sobre los privados, no únicamente estatales, sino también desde la ciudadanía y/o sus representantes en el Estado, por cuanto la interceptación y el almacenamiento de datos de las comunicaciones privadas en la era digital constituyen un grave peligro para los ciudadanos e incluso para las autoridades.

Por eso, los paladines mundiales de la libertad del flujo de información por Internet y del derecho a la privacidad como Edward Snowden, Julián Assange y el Consorcio Internacional de Investigación Periodística[4] (ICIJ, por sus siglas en inglés) han contribuido al mundo con distintas revelaciones. Snowden puso al descubierto la maquinaria de espionaje gubernamental de los Estados Unidos: *PRISM,* un programa mundial de espionaje de la Agencia de Seguridad Nacional que capturaba las comunicaciones electrónicas privadas de Google, Apple, Microsoft y Facebook (Director of National Intelligence, 2013). Por su parte Assange difundió –a través de Wikileaks– documentos oficiales filtrados sobre asuntos de interés público, que eran mantenidos en secreto por los gobiernos, suceso que tuvo como respuesta de parte del Congreso de los Estados Unidos la llamada Ley *SHIELD* (*Securing Human Intelligence and Enforcing Lawful Dissemination*), que prohibió la publicación de información clasificada sobre secretos internacionales de inteligencia (Europapress, 2010). Finalmente, el ICIJ difundió información (11.5 millones de documentos del bufete de abogados panameños Mossack Fonseca) sobre las actividades empresariales no éticas o ilegales (elusión y defraudación fiscal) de personajes públicos de fama internacional (los llamados *Panama Papers*), entre ellos jefes de Estado, políticos, artistas, deportistas, etc. (ICIJ, 2017).

Los derechos fundamentales tienen límites, y a su vez estos límites a su vez tienen límites; en este entendido, los derechos a la protección de datos, como el secreto de los documentos de Estado, y/o la privacidad empresarial o económica no son derechos absolutos. Sin embargo, ello no significa que el interés público siempre deba prevalecer frente al interés particular del Estado o de los particulares. En todo caso, es legítimo realizar y difundir responsablemente investigaciones periodísticas, pero también resulta necesario realizar investigaciones fiscales y judiciales, cuando sea el caso, tanto sobre las actividades ilícitas de los aparatos de seguridad del Estado en materia de vigilancia electrónica, como de las empresas y personajes defraudadores del Estado.

En general se puede señalar que el progresivo desarrollo del acceso y uso del derecho a Internet en las dimensiones esenciales identificadas –libre acceso, seguridad, privacidad,

4 International Consortium of Investigative Journalists

uso de seudónimo, olvido digital y control de la vigilancia electrónica–, requiere de una tutela institucional y jurisprudencial adecuada. No obstante, la jurisprudencia constitucional es inexistente aún; no obstante, la jurisprudencia sobre la materia emitida por el tribunal administrativo competente respecto de la protección de los datos personales es suficientemente relevante para dar cuenta de ella críticamente.

Jurisprudencia Administrativa sobre Internet y Derechos Fundamentales

Realizado el planteamiento de la naturaleza de Internet como un derecho, con todas las ventajas y dilemas que presenta respecto de los derechos fundamentales, dado su agresivo desarrollo tecnológico y/o comercial, corresponde analizar cómo ha respondido el Estado constitucional a este nuevo desafío de las sociedades de la comunicación y el conocimiento en la actual era digital. Al respecto, el Congreso de la República dictó en 2001 la *Ley 29733, Ley de Protección de Datos Personales* (LPDP), con lo que creó la Autoridad Nacional de Protección de Datos Personales (ANPDP), radicada en la Dirección General de Protección de Datos Personales (DGPDP) del Ministerio de Justicia y Derechos Humanos, la misma que tiene competencia para llevar a cabo dos tipos de procedimientos:

a) Procedimiento administrativo sancionador por infracciones a la LPDP y su Reglamento, de acuerdo a lo establecido en los artículos 37 a 40 de la misma ley, que se inicia de oficio o denuncia de parte.
b) Procedimiento trilateral de tutela para la protección de los derechos consignados en la LPDP para los titulares de los datos almacenados en bancos de datos personales, de acuerdo a lo establecido en el artículo 24 de la LPDP.

En atención a dichas facultades, la DGPD, desde el inicio de sus funciones en 2014, ha resuelto casos vinculados a ambos tipos de procedimientos:

Tabla 1. Número de casos por tipo de procedimiento

Tipo de procedimiento	**Número de casos resueltos**
Procedimientos administrativos sancionadores	42 (*)
Procedimientos trilaterales de tutela	39 (**)
Total	**91**

(*) Según la información de la página web de la DGPDP solo se ha publicado las decisiones recaídas en procedimientos sancionadores concluidos.

(**) Cabe añadir que de acuerdo a la información proporcionada por la página web de la DGPDP en 2013 se resolvieron 3 casos, en 2014 fueron 17 y en 2015 se han resuelto 19 casos.

Elaborado sobre la base de DGPDP, s/f-a y s/f-b.

Se han revisado todos los casos publicados en el portal institucional de la DGPDP, de entre los cuales se han seleccionado cinco casos de procedimientos sancionadores y de procedimientos trilaterales de tutela (3 de 2014 y 2 de 2015). El criterio de selección fue la vinculación con la protección de datos personales en Internet (bancos de datos o páginas web). Seguidamente se efectuará una presentación de los casos seleccionados poniendo énfasis en la argumentación empleada por la DGPDP, bien para sancionar a los titulares de banco de datos personales (procedimiento sancionador) o para proteger los derechos de los titulares de dichos datos (procedimiento trilateral).

Caso Clínica San Felipe

Según se señala en la *Resolución Directoral 043-2015-JUS/DGPDP-DS*, de fecha 15 de julio de 2015, la Clínica San Felipe fue sometida a procedimiento sancionador por utilizar datos personales sin consentimiento, al haberse detectado que obtenía consentimiento mediante prácticas inválidas, ya que mediante el link *Contáctanos* realizaba recopilación y almacenamiento de datos personales de clientes y de no clientes usuarios de su página web (nombres, apellidos, sexo, DNI, fecha de nacimiento y correo electrónico).

Al respecto, en su descargo, la Clínica San Felipe señaló que la información recabada de los usuarios no era información vinculada a datos sensibles dado que no estaban vinculados con su salud. Asimismo, argumentó que la información recabada podía ser ubicada en otras bases de datos de acceso público como guías telefónicas, el Registro Nacional de Identificación y Estado Civil, y guías profesionales en el caso de los correos electrónicos; por ello, sostenía, no se trataba de información que afectase su esfera íntima. La clínica también señaló que la información recabada y proporcionada por los usuarios tenía por objeto entablar una relación contractual vinculada a los servicios de salud que ofrece.

De igual manera, sostuvo que, a través de su *Política de Protección de Datos Personales* otorgaba a los usuarios de su página web información acerca del tratamiento que se brindaría a los datos que proporcionaban, por lo que únicamente sería controvertible la forma en que se obtenía el consentimiento (de manera tácita o presunta).

Ante los descargos, la Dirección de Sanciones de la DGPDP, primera instancia administrativa, sostuvo que la clínica había reconocido que realizaba tratamiento de datos personales, lo que de acuerdo a lo establecido en el artículo 5 de la LPDP (2001), requiere el consentimiento de su titular. Sin embargo, en la misma LPDP se establece que no se requiere dicho consentimiento "cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular sea parte" (2011, art. 14.5).

En virtud al parámetro legal citado, el tratamiento de datos personales de los clientes de la Clínica, quienes mantenían una relación contractual con esta, se efectúa a través del proceso denominado *admisión de pacientes;* por ello, se consideró que el tratamiento de datos a través de su página web, mediante el enlace *Contáctanos*, era un tratamiento adicional de datos personales que sí requería el consentimiento de su titular, lo cual era más evidente en el caso de los usuarios que no son clientes de la clínica, por lo que no resultaba aplicable el artículo 14.5 de la LPDP (DGPDP, 2015a, numeral 10.8).

Asimismo, se señaló que no resultaba de aplicación la excepción al consentimiento del titular, prevista en el artículo 14.2 de la LPDP (2001), que establece que no se requiere el consentimiento para el tratamiento de datos obtenidos de fuentes accesibles al público, en la

medida en que los datos recopilados y almacenados a través del mencionado enlace no fueron obtenidos de guías telefónicas o registros públicos, sino que fueron proporcionados por los mismos usuarios, por lo que se requería su consentimiento (DGPDP, 2015a, numeral 10.11).

De otro lado, sobre la *Política de Protección de Datos Personales*, se concluyó que, tal y como estaba redactada, no constituía una política de protección de datos sino cláusulas de consentimiento inválidas, pues no se ajustaba a los requisitos establecidos en el artículo 12 del Reglamento de la LPDP (2001), que establece que el consentimiento debe obtenerse de manera libre, previa, expresa e inequívoca, e informada.

El consentimiento no era libre en tanto el usuario no tenía la opción de otorgar o denegar el consentimiento, ya que según la propia política cualquier interacción web en sí misma implica que la clínica dé por otorgado el consentimiento (DGPDP, 2015a, numeral 10.16). Por lo tanto, no era previo, pues la recopilación de los datos se daba con la sola navegación en la web. Tampoco era expreso e inequívoco, pues ello bastaba para que la Clínica presuma el consentimiento del usuario. Tampoco era informado, pues de acuerdo a la propia información contenida en la política no estaba claro a quién debería dirigirse la revocación para el tratamiento de los datos y cuál era la finalidad específica de su tratamiento (DGPDP, 2015a, numerales 10.15 a 10.19).

Por las razones expuestas, se sancionó a la Clínica San Felipe con una multa de cinco Unidades Impositivas Tributarias (UIT). Asimismo, cabe precisar que esta decisión fue declarada firme mediante la *Resolución Directoral 028-2015-JUS/DGPDP,* de fecha 21 de setiembre de 2015, que rechazó el recurso de apelación de la institución, por haber sido interpuesto de manera extemporánea.

El acceso a una página web y a las bases de datos que en ella se alojan para navegar, requiere del conocimiento del usuario también para poder asegurar su derecho de acceso a Internet, libre e informado. Las fórmulas de consentimiento deben ser claras, sencillas y precisas, a fin de asegurar que la relación virtual establecida no sea perjudicial para la parte más débil, que es el usuario, y controlar a la parte fuerte de esta relación asimétrica, el proveedor del servicio, que es el único que conoce el producto en detalle.

Por eso, el Estado defiende el interés de los consumidores y usuarios; para tal efecto, debe garantizar el derecho a la información sobre los servicios y bienes que se encuentran a su disposición en el mercado; asimismo, debe proteger en particular la salud y la seguridad de las personas, tal como señala el artículo 65 de la Constitución.

Caso SENTINEL PERU S. A.

SENTINEL PERU S. A. es una central privada de información de riesgos (CEPIRS) que en el mes de setiembre de 2014 habilitó en su página web una herramienta denominada *Conoce a tu Candidato,* desde la cual se podía acceder de manera gratuita a toda la información crediticia de los candidatos de las elecciones regionales y municipales del año 2014 (deudas reportadas con detalle de montos, estado, calificación crediticia y situación de morosidad). En el mismo contexto, el director comercial de la empresa difundió en diversos medios de comunicación los alcances de dicha herramienta, señalando que con ello la empresa cumplía una función social para permitir a la ciudadanía el acceso a información que les permitiría elegir por quien votar en el referido proceso electoral.

Por estos hechos, mediante la *Resolución Directoral 085-2015-JUS/DGPDP-DS,* del 11 de noviembre de 2015, SENTINEL PERU S. A. fue sancionada con 42 UIT por efectuar

tratamiento de datos personales infringiendo los principios de finalidad y proporcionalidad reconocidos en los artículos 6 y 7 de la LPDP (2001), decisión que fue confirmada mediante *Resolución Directoral 0006-2016-JUS/DGPD* de fecha 22 de enero de 2016.

En primera instancia, la empresa sancionada presentó como sustento de su defensa los siguientes argumentos: a) que la difusión y publicación de la información crediticia de los candidatos se hallaría amparada por la *Ley 27489, Ley de Centrales de Riesgo,* que faculta a las empresas dedicadas al rubro a efectuar tratamiento de datos crediticios para evaluar la solvencia económica de una persona; b) que se trató de la difusión de información sobre la pertenencia de los candidatos a un partido político, información que se encuentra en fuentes de acceso público (bases de datos de ONPE y JNE) y por lo tanto no puede constituir tratamiento de datos sobre convicciones políticas; c) que el campo de acción de las CEPIRs no se circunscribe solo al mercado financiero, sino también el denominado *mercado electoral*; d) que la difusión de información a través de la herramienta *Conoce a tu Candidato* no constituyó una estrategia publicitaria o de márketing, dado que como central de riesgo también puede tener fines sociales, tal como el acceso gratuito a información crediticia de los candidatos; e) que la información proporcionada por la herramienta *Conoce a tu Candidato* no afectaba el bien jurídico protegido por la LPDP, dado que los propios candidatos difundieron su información electoral (pertenencia a un partido político) al presentarla ante la ONPE y hacerla pública en diversos medios de comunicación, por lo que la misma se convertiría en información de acceso público y no estaría bajo el ámbito de protección del derecho a la intimidad y la LPDP.

En relación con los argumentos de SENTINEL PERU S. A., en primera instancia la ANPDP sostuvo que de acuerdo al artículo 6 de la LPDP los datos personales deben ser recopilados para una finalidad específica. En ese sentido, la *Ley 27849, Ley de Centrales de Riesgo,* solo autoriza que las CEPIRS a efectuar tratamiento de datos vinculados a riesgos en el mercado, por lo que cualquier interpretación extensiva es contraria a dicha limitación.

Por ello, cuando se verificó que el uso de la herramienta *Conoce a tu Candidato* proporcionaba información que vinculaba los datos crediticios (información económica) del candidato con su afiliación al partido político que representaba y al cargo al que postulaba (información electoral), se concluyó que SENTINEL PERU S. A. había efectuado un tratamiento adicional de datos personales no razonable a su finalidad autorizada como CEPIR. Asimismo, la ANPDP que la empresa se convirtió en un *actor electoral*, dado que proporcionaba información para que la ciudadanía decidiera su voto, finalidad ajena a la que como CEPIR se le autoriza por la *Ley de Centrales de Riesgo*, entregar un reporte de crédito para evaluar la solvencia económica de una persona. Su proceder, además, suponía una infracción al principio de proporcionalidad, en tanto la información proporcionada sobre los candidatos no resulta imprescindible o relevante para cumplir con la finalidad para la que como CEPIR estaba autorizada (DGPDP, 2015d, numeral 17.2).

Por otro lado, también la ANPDP que este accionar constituyó una forma de publicidad en beneficio de SENTINEL PERU S. A., ya que la empresa difundió este servicio en medios de comunicación masiva a través de su director comercial, quien tiene por finalidad vender los servicios de la empresa, indicando que era la empresa más moderna del mercado en el rubro, además de publicitar sus tarifas y el alcance de sus servicios. Como toda empresa, SENTINEL PERU S. A. puede efectuar la publicidad que le convenga, pero lo cuestionable es que lo haya hecho mediante la difusión masiva de datos personales (DGPDP, 2015d, numeral 18.5).

Por último, la ANPDP concluyó que hubo lesión al derecho a la protección de datos personales, ya que este no exige que haya tenido lugar una lesión al derecho a la intimidad personal, puesto que lo discutido, tal y como ya se ha evidenciado, fue el uso de información económica de los candidatos no acorde con la finalidad para la cual SENTINEL PERU S.A. se encontraba autorizada como central de riesgos (DGPDP, 2015d, numeral 18.2).

SENTINEL PERU S.A. apeló a la decisión de primera instancia, y para ello empleó como argumentos los siguientes: a) que la información electoral se encontraba bajo los alcances de la *Ley de Transparencia y Acceso a la Información Pública,* por lo que esta podía ser difundida por cualquier privado, sin restricciones; b) que tanto los candidatos como la ONPE difundieron, en diversos medios, su pertenencia o afiliación a un partido político, por lo que hicieron de la misma información pública no amparable por la LPDP, por lo que la decisión impugnada incurría en un error al haber analizado el accionar de la empresa bajo el prisma del derecho a la protección de datos personales y no del derecho a la información pública, como correspondía; c) que el concepto de mercado no solo debería circunscribirse al financiero sino también debería extenderse al mercado electoral, donde existe una cruce de información entre una oferta (candidatos) y una demanda (ciudadanos) para la toma de decisiones que pueden afectar el rumbo del país, por lo que con su accionar cumplen una función social.

No obstante, en la decisión de segunda instancia que se confirmó la multa impuesta a SENTINEL PERU S. A., pues se sostuvo a) que el hecho de que la información de un ciudadano se encuentre en una fuente de acceso público no hace de dichos datos información pública, por lo que para su tratamiento y difusión se requiere recabar el consentimiento libre, previo, expreso e inequívoco e informado, pues de lo contrario se trata de una infracción al derecho a la protección de datos personales, y que en todo caso, si la ONPE o el JNE difundieron la misma, lo hicieron porque se encontraban autorizados de manera expresa por la ley, situación distinta a la de la empresa sancionada (DGPDP, 2016d, numeral 3.2.3); b) que la DGPDP es la autoridad nacional en materia de protección de datos personales, por lo que sostener que el caso debió enfocarse desde el derecho de acceso a la información pública es un error, ya que no es la autoridad competente en dicha materia y menos en materia electoral (DGPDP, 2016d, numeral 3.2.2); c) que la empresa sancionada es una CEPIR que de acuerdo a la ley de la materia solo está autorizada a brindar información para la evaluación de riesgos en el mercado, por lo que el uso de información para fines distintos a los autorizados por la *Ley de Centrales de Riesgos,* como lo es el uso electoral, constituye un tratamiento ajeno a su finalidad, más aún si se evidencia que el mismo tuvo fines publicitarios, finalidad que no está establecida de forma clara, expresa e inequívoca en la *Ley de Centrales de Riesgos* (DGPDP, 2016d, numeral 3.2.4).

En efecto, la protección de datos personales se funda en el derecho a la autodeterminación informativa que tiene toda persona, en tanto portadora y titular de información personal y/o familiar que no puede ser difundida o utilizada por terceros, salvo que medie consentimiento o se produzca por mandato de la ley (Lucas, 1993). Así, el derecho a la autodeterminación informativa permite el control de los servicios informáticos, computarizados o no, públicos o privados, para que no suministren información que afecte la intimidad personal y familiar, tal como figura en el artículo 2, inciso 6 de la Constitución.

A partir de ello, se ha producido una *vis expansiva* de dicho derecho a la autodeterminación informativa, en la medida en que, por un lado, la prohibición señalada no se reduce proteger el

clásico derecho a la intimidad, sino también a proteger la intimidad patrimonial; por otro, se ha establecido una interpretación restrictiva de la *Ley de Centrales de Riesgo* para la recopilación de datos personales, inclusive aquellas que se hallen en bancos de datos públicos, que está acotada al registro y transmisión de información para el mercado –económico–, pero para el mercado electoral.

Casos cooperativa de servicios educacionales San Felipe, institución educativa Teresa González de Fanning), Centro de Educación Primaria Isabel Flores de Oliva

Estos casos han sido agrupados en tanto a todas las instituciones educativas en cuestión se les atribuyó una misma infracción: el tratamiento de datos personales sin haber recabado el consentimiento de sus titulares, mediante el acto específico de emplear en su página web institucional fotografías de sus estudiantes sin acreditar haber recabado el consentimiento de sus padres o tutores legales.

Al respecto, la cooperativa de servicios educacionales San Felipe (colegio San Felipe) señaló que las fotografías publicadas en su portal web correspondían a una sesión de fotos del verano del año 2011, realizadas para la campaña promocional de admisión de dicho año, y que en aquella ocasión todos los padres asistieron y prestaron su consentimiento, especificando que a la fecha de descargo no todos los alumnos continuaban en el colegio, y presentando el consentimiento firmado por aquellos padres que aún mantenían a sus hijos en el colegio. Por su parte, la institución educativa Teresa González sostuvo que las imágenes no eran datos personales, sino imágenes de actividades que se realizan en el colegio, pues fueron tomadas en sus instalaciones. Por último, el CEP Isabel Flores de Oliva indicó, como argumento de defensa, que las imágenes de su página web muestran a exalumnos del colegio.

La Dirección de Sanciones sostuvo, respecto de todos los casos, que no se había acreditado que las instituciones educativas habían obtenido el consentimiento previo y expreso para el tratamiento de los datos personales (imágenes de alumnos o exalumnos) a través de su página web, por lo que se procedía a sancionar, mediante las *Resolución Directoral 117-2015-JUS/DGPDP-DS,* del 18 de diciembre de 2015 al colegio San Felipe (confirmada por la *Resolución Directoral 20-2016-JUS/DGPDP* de fecha 23 de febrero de 2016); *016-2016-JUS/DGPDP-DS,* del 18 de enero de 2016, al I. E. Teresa González; y *025-2016-JUS/DGPDP-DS.* del 18 de enero de 2016, al C. E. P. Isabel Flores. Cabe añadir que estas dos últimas resoluciones no fueron impugnadas por las instituciones educativas sancionadas, por lo que quedaron consentidas en primera instancia.

El derecho a la propia imagen es un derecho fundamental que está reconocido en el artículo dos, inciso *7 in fine* de la Constitución (1993). Este derecho tiene una doble vertiente, en tanto derecho a su figura humana y a que no se haga uso de su imagen sin su consentimiento. En virtud de este, cualquier utilización de la propia imagen sin consentimiento constituye una vulneración de dicho derecho fundamental (Alegre, 1997).

Si bien las imágenes de los alumnos y alumnas de las instituciones educativas fueron captadas en sus respectivos locales, en el marco de sus actividades de formación, la ANPDP hizo bien en realizar un escrutinio estricto para controlar el registro de los datos personales, en la medida que se requiere que cada persona ceda su imagen mediante consentimiento expreso de tak voluntad, en tanto derecho fundamental indisponible por terceros (Pascual, 2003).

Caso *El Comercio*

El denunciante, cuyo nombre ha sido tachado en la resolución de la DGPDP para proteger su identidad y respetar su derecho al olvido, cuestionó que el diario *El Comercio* no atendiera su solicitud de cancelación respecto del alojamiento, desde el año 2011, de un link en su página web (htpp://elcomercio.pe/archivo/2011-03-17), el cual enlazaba con una publicación de otra página web (http://whiskyleaksperu.blogspot.com/) en la que se alojaba un audio de una llamada telefónica sostenida entre el denunciante y el expresidente Alejandro Toledo. En la web del diario se mostraba la información a modo de nota periodística, junto con la opinión del expresidente Toledo respecto del referido audio. El denunciante consideró que el que dicha publicación siga activa en 2014 se afectaba sus derechos a la intimidad, el honor y la buena reputación, en tanto ya no era un actor en la vida política del país. Por su parte, *El Comercio*, en su defensa, señaló que la publicación se derivó de las declaraciones que el expresidente brindó a la prensa en general, por lo que dicho contenido se ajustaba a la labor periodística; asimismo, indicó que había retirado la publicación y que la misma ya no figuraba en su página web.

La denuncia fue declarada infundada mediante *Resolución 061-2014-JUS/DGPDP* de fecha 1 de agosto de 2014, porque si bien la libertad de información debe armonizarse con los principios de la protección de datos personales, en el caso debía evaluarse la

> importancia que conlleva mantener de forma permanente una absoluta accesibilidad a los datos personales contenidos en noticias, cuya relevancia informativa puede devenir en inexistente en el contexto actual. Asimismo, debe tener en cuenta los efectos sobre la privacidad de las personas que deriva de ello, considerando además si la persona involucrada desarrolla actividad de relevancia pública. (2014, num. 10)

Por ello, señaló la ANPDP, si bien en la nota periodística figuran datos personales del denunciante, en la difusión de la noticia existe un interés público en atención a la actividad pública del denunciante porque a) el reclamante fue ministro de Estado y congresista de la República durante el gobierno del expresidente Toledo, por lo que existe un interés público en las informaciones vinculadas a la actuación de un exfuncionario público; b) si bien la noticia se difundió en 2011, en 2014 el interés público no ha dejado de existir, más aún si en ella está involucrado un expresidente que sigue vinculado a la vida política del país; c) la noticia se publicó en virtud a las declaraciones del expresidente Toledo en el marco de una actividad proselitista, y fue este quien aludió al reclamante; y d) el audio no fue publicado por la web de *El Comercio,* que, además, a la fecha de emisión de la resolución, había bloqueado y luego cancelado los datos del reclamante cuya utilización indebida fue motivo de la denuncia.

Esta decisión fue objeto de un recurso de reconsideración, el cual fue declarado infundado mediante *Resolución 070-2014-JUS/DGPDP* el 3 de octubre de 2014. El reclamante sostuvo, por un lado, que si bien comparte el criterio de que es legítimo el interés por conocer sobre los cargos y acciones de quienes han sido funcionarios públicos, tales informaciones no deberían haber sido obtenidas por medios ilegales como la vulneración del derecho a la intimidad personal del reclamante al interceptar una comunicación telefónica; por otro lado, que la información ya no tiene relevancia pública, pues el audio difundido fue interceptado en 2004, es decir, hace más de 10 años.

Al respecto, la DGPDP sostuvo que en la reclamación no se había sostenido ni probado que el audio original difundido hubiese sido interceptado de manera ilegal por *El Comercio*, y que, en todo caso, el denunciante había optado por la vía penal para cuestionarla. Finalmente, consideró que, a pesar de la eliminación de la información sobre el reclamante por parte de *El Comercio,* la difusión de la noticia y del audio que se hizo en su momento revestía un notorio interés público, que el reclamante no pudo desvirtuar.

Cabe agregar que un caso sustancialmente igual, referido a la difusión del mismo audio, formulado por el mismo reclamante pero esta vez en la página web del diario *La República,* fue resuelta en términos similares mediante la *Resolución Directoral 062-2014-JUS/DGPDP,* de fecha 1 de agosto de 2014, confirmada mediante *Resolución Directoral 069-2014-JUS/DGPDP,* del 3 de octubre del mismo año, que declaró infundado el recurso de reconsideración del reclamante.

El derecho al olvido o cancelación de datos alojados en las páginas web de los periódicos se fundamenta en el derecho a la intimidad personal y familiar. Así, la protección de datos personales se extiende a las informaciones publicadas por los medios de comunicación digitales que obren en otras fuentes de Internet, como los blogs. No obstante, en este caso no se trató de la exposición de información privada –sobre asuntos de interés político– de cualquier persona, sino de un exministro de Estado.

Así, el derecho al olvido no debería ser absoluto, en la medida en que se trate de un personaje público. Una sobreprotección de sus datos podría afectar la libertad de expresión, que incluye el derecho a la información ciudadana. En un mundo en el cual la política se desprestigia cada vez más por causa de quienes asumen dichas responsabilidades, incluso mediante elección popular, parece razonable que la presunción sea más bien la intención de hacer publicidad y que la excepción sea el derecho al olvido digital (Álvarez, 2015).

Caso datosperu.org

Mediante *Resolución Directoral 074-2014-JUS/DGPDP,* de fecha 24 de octubre de 2014, y *075-2014-JUS/DGPDP,* de la misma fecha, se declaró fundadas dos solicitudes de tutela contra datosperu.org, debido a que esta página web difundía anuncios obtenidos de otros bancos de datos (diario oficial *El Peruano*) sin haber recabado el consentimiento de los titulares de los datos personales difundidos y sin haberla actualizado debidamente.

En relación el primer caso, se trataba del hecho de que en la dirección electrónica http://www.datosperu.org se encontraba alojada en formato portátil la resolución que autorizaba al procurador público de la Policía Nacional del Perú a impugnar judicialmente las resoluciones supremas de ascenso y posterior pase a retiro por causal de renovación del reclamante. En el segundo caso, se discutía el hecho de la publicación de la resolución que impuso sanción disciplinaria de destitución al reclamante en su condición de exfuncionario de la unidad de tesorería de una municipalidad.

En ambos casos los reclamantes acreditaron que datosperu.org no había recabado su consentimiento para realizar tratamiento automatizado de sus datos personales. También se constató que la referida página web no había anonimizado los datos de los reclamantes y que la información difundida no estaba debidamente actualizada, pues en el primer caso la resolución que autorizó al procurador a accionar judicialmente fue dejada sin efecto y en el segundo caso la resolución de destitución del reclamante fue declarada nula por la Corte Suprema, que

dispuso se realice un nuevo procedimiento administrativo en el cual fue absuelto por haberse declarado la prescripción.

Las funciones de los funcionarios públicos se encuentran regladas por la Constitución y las leyes. En esa medida, el acceso a la información pública es un derecho fundamental, una manifestación del principio de transparencia propio de las sociedades democráticas. Por ello, toda persona puede

> solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública en el plazo legal y con el costo que suponga el pedido; con excepción de las informaciones que afecten la intimidad personal y las que expresamente se excluyan por la ley o por razones de seguridad nacional. (1993, art. 2, inc. 5)

Más aún, la *Ley 27806, Ley de Transparencia y Acceso a la Información Pública,* ampara el derecho fundamental a conocer los asuntos públicos, ciertamente solicitando el acceso. Por tanto, no es de recibo que la información pública registrada en la base de datos del diario oficial, que da cuenta de las normas y resoluciones, sobre los funcionarios públicos, no puedan ser captada y difundida por Internet, sino que esta, para que esté protegida, debe ser verdaderas en el tiempo; es decir, debe ser actualizada salvo que se señale su carácter sucedáneo en un momento determinado.

Caso del blog *Defensa de los Derechos Humanos Laborales*

El blog *Defensa de Derechos Humanos* fue objeto de una reclamación por parte del gerente de una empresa que había sido sancionada por la autoridad de trabajo por la vulneración de los derechos de sus trabajadores. El reclamante sostenía que en el blog se había efectuado un tratamiento de datos –recopilación y difusión– relativos a su persona, específicamente su nombre, documento nacional de identidad (DNI) e imagen.

El blog reclamado adujo en su defensa que la información propalada era de acceso público, pues se encontraba alojada en fuentes accesibles para el público (Consulta RUC SUNAT, y web del Ministerio de Trabajo y Promoción del Empleo) y no estaba referida a aspectos sensibles de la personalidad del reclamante, por lo que no era necesario recabar el consentimiento del titular.

En la *Resolución Directoral 030-2015-JUS/DGPDP*, del 22 de octubre de 2015, que declaró fundado el reclamo, se consideró en primer lugar que la LPDP y su Reglamento protegen los datos personales de las personas naturales, más no de las personas jurídicas, lo que no quiere decir que los datos de estas no estén protegidas, sino que no se encuentran bajo el régimen legal de la LPDP y su Reglamento; por ello, la difusión de los datos de la empresa (razón social, RUC, giro de negocio) no constituye una infracción a la LPDP.

De otro lado, se sostuvo que el tratamiento de datos de las personas naturales que representan a las personas jurídicas, en tanto su uso esté vinculado con la actividad comercial de la empresa o como parte de los datos de la propia empresa, no se encuentra protegido por la LPDP. En este caso, se consideró contrario al principio de proporcionalidad el uso de datos personales del reclamante, tales como su DNI e imagen, para propalar la información vinculada a la lesión de derechos laborales por parte de la empresa, pues constituye en estricto información respecto de la propia actividad de la persona jurídica y no del reclamante.

Asimismo, se sostuvo que en el presente caso era necesario contar con el consentimiento del reclamante para difundir en el blog su DNI e imagen, debido a que los hechos

informados no eran de interés general o relevancia pública, debido a que el afectado no desarrolla actividad pública.

También se sostuvo que el blog realizaba tratamiento automatizado de datos personales que, si bien habían sido obtenidos de fuentes de acceso público a las cuales la LPDP autoriza el acceso sin consentimiento, no autoriza a su archivo o difusión sin que medie el consentimiento de su titular.

Finalmente, el hecho de que la información difundida se encuentre en fuentes de acceso público no conlleva que los datos personales se conviertan en información pública; el acceso se autoriza para fines de consulta y no de difusión.

Esta decisión fue confirmada en todos sus extremos por la *Resolución Directoral 035-2015-JS/DGPDP,* del 24 de noviembre de 2015. De dicha resolución cabe resaltar el análisis que se realiza del conflicto entre la libertad de información y el derecho a la protección de datos personales. Según la DGPD, se debe ponderar de un lado la naturaleza de la información publicada y del otro el interés público en la difusión de la información.

Respecto del primer aspecto, se concluyó que la entrada del blog en cuestión contenía datos personales del reclamante que exceden la identificación del reclamante en tanto representante de la persona jurídica y que fueron consignados sin su consentimiento. Es decir, el tratamiento de los datos del representante de una empresa debe limitarse a aquellos que sean necesarios para identificarlo como tal. Sobre el segundo elemento, se concluyó que no existe un interés público relevante en que terceros accedan a información personal del reclamante, pues la información publicada se centra en emitir opiniones en torno a la actividad comercial de la empresa de la cual el reclamante es representante, es de la persona jurídica mas no de la persona natural.

Resulta pertinente que se haya establecido que obtener información de bases de datos públicas sobre determinadas personas naturales no faculta a que un tercero las archive, procese y difunda en un blog, por cuanto se requiere del consentimiento del titular de la información personal, excepto cuando se trata de asuntos de interés público referidos a personas jurídicas, que no gozan del derecho de protección de datos personales.

No obstante, acertadamente se plantea la necesidad de realizar un test de razonabilidad y proporcionalidad entre la libertad de información por Internet y el derecho a la privacidad de la empresa denunciada, tarea que queda amparada por la jurisprudencia del Tribunal Constitucional, en la medida en que ha reconocido ciertos derechos fundamentales a las personas jurídicas, como el de la autodeterminación informativa (Tribunal Constitucional, 2006), motivo por el cual podría ser justiciable mediante el proceso constitucional de amparo.

Caso Google

En el presente caso una persona intentó infructuosamente que Google Perú S. R. L. y Google Inc. cancelen la aparición de sus datos a través del motor de búsqueda Google Search, información que lo vincula con un proceso penal del cual a la fecha de solicitud había sido sobreseído. Google Inc. le respondió que debía dirigirse directamente a los administradores de las páginas web que difundían la información cuestionada.

A nivel del procedimiento de tutela, tanto Google Perú S. R. L. como Google Inc. eludieron formular descargos bajo el argumento de que la segunda no operaba el motor de búsqueda y que no tiene la titularidad de la información cuya protección se reclamaba, mientras que la

segunda no se encontraba domiciliada en territorio peruano, por lo que las disposiciones de la LPDP y su Reglamento no le resultaban aplicables.

Mediante la *Resolución Directoral 045-2015-JUS/DGPDP*, de fecha 30 de diciembre de 2015, la DGPDP determinó que el motor de búsqueda Google Search (a través del sitio web http://www.google.com.pe) realiza tratamiento de datos personales por dos motivos: a) porque realiza una operación técnica automatizada que tiene por finalidad identificar, recopilar, sistematizar, almacenar y difundir información en sus servidores, lo cual constituye una clasificación de información que permite luego su acceso a terceros; y b) porque brinda servicios de búsqueda por Internet empleando los nombres y apellidos de las personas, con lo cual afecta su privacidad.

De otro lado, la ANPDP concluyó que Google Perú S. R. L. y Google Inc. están vinculados indisolublemente por el tratamiento de la publicidad, y que las operaciones efectuadas a través de la web http://www.google.com.pe/ tuvieron lugar en territorio peruano, por lo que estaban sujetas a la LPDP y su Reglamento.

Asimismo, se consideró que el permitir a los robots de búsqueda vincular e hipervisibilizar los datos personales del reclamante (nombres y apellidos) junto con la información que se solicitó cancelar, ya que esta no se ajusta a la actualidad de los hechos, dado que el demandante fue absuelto del delito por el que se le procesaba, supone una lesión a su derecho a la protección de datos personales y su difusión mediante el motor de búsqueda debe cesar. Finalmente, se ordenó que se excluya como criterio de búsqueda los nombres y apellidos del reclamante, lo que no impide que se pueda acceder a dicha información a través de otros criterios de búsqueda.

Esta decisión fue impugnada, habiéndose rechazado el recurso y confirmado la decisión antes citada, mediante la *Resolución Directoral 026-2016-JUS/DGPDP*, de fecha 11 marzo de 2016. En esta se emplearon básicamente los argumentos ya reseñados en los párrafos precedentes.

Como Internet es una especie de almacén de información al que se accede desde cualquier lugar, que multiplica exponencialmente la obtención, consulta, y difusión a través de las redes sociales de forma muy simple, lo cual pone en tensión derechos de los usuarios y las empresa prestadoras de servicios de Internet. Por ello resulta tan necesaria la protección de datos personales, así como asegurar los intereses legítimos de los operadores económicos y de los usuarios de Internet, en el marco de una interpretación sobre la base del principio de proporcionalidad (Rallo, 2014).

Conclusiones y Perspectivas

Los nuevos paradigmas de la sociedad de la información y del conocimiento promueven que con el desarrollo de Internet y de las nuevas tecnologías se potencialice no solo cuantitativamente los derechos fundamentales, sino también que estos adopten un grado artificial de desarrollo, propio de las sociedades de consumo de la información y la comunicación.

El Estado, como garante del interés general, debe "mejorar la tecnología [digital], ampliar los servicios diversos y baratos de banda ancha, alfabetizar digitalmente y cerrar la brecha tecnológica que existe entre ricos y pobres, entre jóvenes y viejos" (Trotti, 2011, párr. 11). Sin embargo, se encuentra a la zaga de los avances de las nuevas tecnologías, que amplían y masifican el consumo de instrumentos y medios de comunicación a través del uso de Internet:

no existen regulaciones normativas al respecto, o estas no prevén el impacto del goce y ejercicio del derecho frente a terceros y respecto de los bienes constitucionalmente protegidos.

Desde luego, el acceso a Internet se está convirtiendo en un nuevo derecho fundamental de las personas; sin embargo, su titularidad reposa no solo en el ciudadano sino también en los proveedores –privados y estatales, donde fuera– de los insumos estructurales necesarios para el uso de esta red de comunicación.

Desde la perspectiva de los derechos fundamentales, el derecho al internet debe poseer de un contenido esencial, constitucionalmente protegido, debido a que es un bien de dominio público. En virtud de ello, el Estado debe asegurar su acceso para todos, la libertad de uso del mismo, la seguridad y privacidad de los datos y comunicaciones, su uso anónimo y el derecho al olvido digital, así como, controlar la vigilancia electrónica, para evitar los excesos públicos y/o privados en la lucha contra la ciberdelincuencia.

En particular, la vinculación entre el derecho a la protección de datos personales e Internet, como medio de registro y difusión de información, es innegable, dado que todos los días se aloja información que atañe a aspectos personales de los ciudadanos en dicha red; datos protegidos por el derecho a la autodeterminación informativa, como figura en el artículo 2, inciso 6 de la Constitución (1993).

Los pocos casos resueltos por la ANPDP demuestran que se está empezando a sentar una línea respecto del derecho a la protección de datos personales, la cual, en todo caso, aún resulta insuficiente. Por ejemplo, se ha sancionado a páginas web de instituciones educativas, empresas y entidades públicas que han utilizado imágenes de sus miembros para publicitar sus funciones o servicios sin haber requerido de manera previa el consentimiento de estos (casos San Felipe, Teresa González e Isabel Flores).

De igual manera, resulta interesante advertir que la protección de los datos personales puede constituirse en un límite válido del ejercicio de la libertad de información, en vista de que se emplea el juicio de relevancia pública para determinar la legitimidad de la difusión de datos personales por parte de medios de comunicación social a través de Internet (casos El Comercio, La República, Blog Defensa de los derechos humanos laborales).

En ese sentido, también cabe advertir el análisis que se ha hecho respecto de la difusión de información crediticia de candidatos, en el marco de un proceso electoral, por parte de una empresa del rubro de las centrales de riesgo, que no se encontraba autorizada para información económica con otra de carácter político caso SENTINEL PERÚ S.A.).

Estos casos son prueba de que quienes son objeto de control son las instituciones y corporaciones privadas, las cuales gracias a Internet han hecho uso mercantil de los derechos ciudadanos, ante lo que la ANPDP ha iniciado una línea de protección de los derechos fundamentales personales.

No obstante, regular los ámbitos de desprotección del derecho ciudadano al Internet y de sus datos personales, no solo frente a los poderes privados sino también frente al propio Estado, constituye un gran desafío. Ello será posible solo a partir de comprender que todo Estado constitucional tiene como fundamento la protección tanto de los nuevos derechos y libertades ciudadanas, como el deber de limitar los excesos de los poderes públicos y privados.

REFERENCIAS

Associated Foreign Press. (2016). *Estados Unidos: Corte Federal ratifica que Internet es un servicio público, Verizon y AT&T apelarán para quitar regulaciones.* Recuperado de https://www.business-humanrights.org/es/estados-unidos-corte-federal-ratifica-que-Internet-es-un-servicio-p%C3%BAblico-verizon-y-att-apelar%C3%A1n-para-quitar-regulaciones.

Alegre Martínez, M. Á. (1997). *El derecho a la propia imagen.* Madrid, España: Tecnos.

Álvarez Caro, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital.* Madrid, España: Reus.

Arroyo, V. (2016, 29 de setiembre-1 de octubre). *El poder del anonimato en la libertad de expresión online.* Ponencia presentada a la mesa temática 2, Libertad de Expresión y Nuevas Tecnologías, de la I Jornada Nacional de Derechos Fundamentales. Pontificia Universidad Católica, Lima, Perú. del 29 de setiembre a 1 de octubre, 2016.

Carballo, J. (2016, 6 de julio). La ONU declara el acceso a Internet como un derecho humano. *Computer hoy*. Recuperado de https://computerhoy.com/noticias/Internet/onu-declara-acceso-Internet-como-derecho-humano-47674

Cisneros, C. (s. f.). El uso de las redes facilita la confluencia alrededor de un tema específico [Entrevista]. *#Código-Abierto_CC.* Recuperado de http://codigo-abierto.cc/claudia-cisneros-el-uso-de-redes-facilita-la-confluencia-alrededor-de-un-tema-especifico/

Clínica San Felipe. (s/f). Política de Protección de Datos Personales. Recuperado de https://www.clinicasanfelipe.com/politica-corporativa-proteccion-datos-personales. Comisión Interamericana de Derechos Humanos. (2013). *Libertad de expresión e Internet.* Recuperado de http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_web.pdf

Consejo de la Unión Europea. (2014). *Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet y fuera de Internet.* Bruselas, 9647/14. Recuperado de 14 de febrero de 2019 de http://data.consilium.europa.eu/doc/document/ST-9647-2014-INIT/es/pdf

Congreso de la República (2011, 3 de julio) Ley 29733, Ley de Protección de Datos Personales (LPDP). *El Peruano.*

Consorcio Internacional de Investigación Periodística. (2017). *An ICIJ investigation. The Panama Papers: exposing the rogue offshore finance industry.* Recuperado el 17

de febrero de 2019 de https://www.icij.org/investigations/panama-papers/#_ga=2.191555439.474570564.1550416993-831792236.1550416993

Córdoba, D. & Díez-Picazo, I. (2016). Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico. En Asociación de Letrados del Tribunal Constitucional, *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional* (pp. 99-110). Madrid, España: Centro de Estudios Políticos y Constitucionales.

Corte Constitucional de Colombia. (2015, 12 de mayo). *Sentencia T-277.* Sala Primera de Revisión.

Corte Interamericana de Derechos Humanos. (2004, 4 de mayo). *Sentencia de la Corte IDH* (Molina Theissen vs. Guatemala).

Cortes, N. (2012, 14 de marzo). Las redes sociales como núcleo de las movilizaciones ciudadanas a nivel mundial. *Sistemas para la Gestión de la Información y las Comunicaciones Estratégicas.* Recuperado de https://sisgecom.com/2012/03/14/las-redes-sociales-como-nucleo-de-las-movilizaciones-ciudadanas-a-nivel-mundial/

Declaración y Programa de Acción de Viena. (1993, 25 de junio). *Conferencia Mundial de Derechos Humanos.* Viena, Austria.

DGPDP. (s/f-a).Procedimientos administrativos sancionadores. Recuperado de http://www.minjus.gob.pe/procedimientos-administrativos-sancionadores/.

DGPDP. (s/f-b). Procedimientos trilaterales de tutela. Recuperado de http://www.minjus.gob.pe/ptt-dgpdp/

DGPDP. (2014a, 1 de agosto). Resolución Directoral 061-2014-JUS/DGPDP.

DGPDP. (2014b, 1 de agosto). Resolución Directoral 062-2014-JUS/DGPDP.

DGPDP. (2014c, 3 de octubre). Resolución Directoral 069-2014-JUS/DGPDP.

DGPDP. (2014d, 3 de octubre). Resolución Directoral 070-2014-JUS/DGPDP.

DGPDP. (2014e, 24 de octubre). Resolución Directoral 074-2014-JUS/DGPDP.

DGPDP. (2014f, 24 de octubre). Resolución Directoral 075-2014-JUS/DGPDP.

DGPDP. (2015a, 15 de julio). Resolución Directoral 043-2015-JUS/DGPDP-DS.

DGPDP. (2015b, 21 de setiembre). Resolución Directoral 028-2015-JUS/DGPDP.

DGPDP. (2015c, 22 de octubre). Resolución Directoral 030-2015-JUS/DGPDP.

DGPDP. (2015d, 11 de noviembre). Resolución Directoral 085-2015-JUS/DGPDP-DS.

DGPDP. (2015e, 24 de noviembre). Resolución Directoral 035-2015-JS/DGPDP.

DGPDP. (2015f, 18 de diciembre). Resolución Directoral 117-2015-JUS/DGPDP-DS.

DGPDP. (2015g, 30 de diciembre). Resolución Directoral 045-2015-JUS/DGPDP.

DGPDP. (2016a, 18 de enero). Resolución Directoral 016-2016-JUS/DGPDP-DS.

DGPDP. (2016b, 18 de enero). Resolución Directoral 025-2016-JUS/DGPDP-DS.

DGPDP. (2016c, 22 de enero). Resolución Directoral 0006-2016-JUS/DGPD.

DGPDP. (2016d, 23 de febrero). Resolución Directoral 20-2016-JUS/DGPDP.

DGPDP. (2016e, 11 de marzo). Resolución Directoral 026-2016-JUS/DGPDP.

Director of National Intelligence. (2013, 8 de junio). *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. Office.* Recuperado el 15 de febrero de 2019 de https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf

El Comercio (2016, 19 de noviembre). *El 55% de peruanos accede a Facebook cada mes.* Recuperado de https://archivo.elcomercio.pe/amp/apec/noticias/55-peruanos-accede-facebook-todos-meses-noticia-1947434

Emol. (2015, 3 de agosto). *Gobierno de Uruguay comienza entrega gratuita de tablets a jubilados.* Recuperado el 16 de febrero de 2019 de https://www.emol.com/noticias/Tecnologia/2015/08/03/743230/Gobierno-de-Uruguay-comienza-entrega-gratuita-de-tablets-a-jubilados.html

Europapress. (2010, 13 de agosto). *El Pentágono: Wikileaks sería irresponsable si publica los documentos.* Recuperado el 15 de febrero de 2019 de https://www.europapress.es/internacional/noticia-pentagono-wikileaks-seria-irresponsable-si-publica-documentos-20100813085329.html

Fernández Rodríguez, J. J. (2004). *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la Red.* Ciudad de México, México: Instituto de Investigaciones Jurídicas - Universidad Nacional Autónoma de México.

García Mexía, P. (2016). El derecho de Internet. En F. Pérez Bes (Coord.), *El derecho de Internet* (pp. 17-39). Barcelona, España: Atelier.

Landa, C. (2016). Derecho fundamental al Internet. En *Primeras Jornadas Nacionales de Derechos Fundamentales* (pp. 1-26). Recuperado de http://themis.pe/wp/wp-content/uploads/2016/07/Derecho-al-Internet-y-Libertad-de-Expresio%CC%81n.docx

Lucas Murillo de la Cueva, P. (1993). *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal).* Madrid, España: Centro de Estudios Constitucionales y Políticos.

Martínez Otero, J. M. (2015, mayo-agosto). Derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs. AEPD y Mario Costeja. *Revista de Derecho Político,* (93), 111-117.

Nieto, M. G. (2016, 30 de septiembre). ¿Quién está detrás del ataque a Yahoo? Los expertos creen que algunos piratas informáticos están respaldados por importantes grupos

de poder. *El País*. Recuperado de https://elpais.com/tecnologia/2016/09/26/actualidad/1474891005_071895.html

Orizaga, I. & Cabrera, K. (2015). Sexting y redes sociales: diversas relaciones y consecuencias jurídicas. En F. Bueno de Mata (Coord.), *Fodertics 3.0 (Estudios sobre nuevas tecnologías y justicia)* (pp. 2185-196). Granada, España: Comares.

Organización de los Estados Americanos. (2013). "Informe de la Relatoría Especial para la libertad de expresión". En Organización de los Estados Americanos, *Informe Anual de la Comisión Interamericana de Derechos Humanos 2013,* vol. II. Recuperado de http://www.oas.org/es/cidh/docs/anual/2013/informes/LE2013-esp.pdf

Ortego Ruiz, M. (2015). *Prestadores de servicios de Internet y alojamientos de contenidos ilícitos.* Madrid, España: Reus.

Parlamento Europeo y el Consejo de la Unión Europea (2016, 27 de abril) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea* (4 de mayo de 2016).

Pascual Medrano, A. (2003). *El derecho fundamental a la propia imagen. Fundamento, contenido, titularidad y límites.* Navarra, España: Thomson - Aranzadi.

Pérez Gómez, A. M. (2016, julio-diciembre). Cuando Google juega con la información privada… El derecho al olvido digital en Europa, una lucha de titanes. *La Propiedad Inmaterial,* (22), 173-186. Recuperado de http:// dx.doi.org /10.18601 /16571959.n22.09

Pulso, Diario de San Luis. (2013, 15 de octubre). *Gobierno uruguayo entrega tabletas a escolares de 4 a 6 años de edad.* Recuperado de https://pulsoslp.com.mx/2013/10/25/gobierno-uruguayo-entrega-tabletas-a-escolares-de-4-a-6-anos-de-edad/

Rallo, A. (2014). *El derecho al olvido en Internet. Google versus España.* Madrid, España: Centro de Estudios Constitucionales y Políticos.

Sanjurjo Rebollo, B. (2015). *Manual de Internet y redes sociales.* Madrid, España: Dykinson.

Téllez Valdés, J. (2015). Libertad de expresión en Internet y redes sociales. En F. Bueno de Mata (Coord.), Fodertics 3.0 (*Estudios sobre nuevas tecnologías y justicia*) (pp. 241-253). Granada, España: Comares.

Tribunal Constitucional. (2006, 4 de agosto). *Sentencia del TC.* Exp. 4972-2006-PA/TC.

Tribunal de Justicia de la Unión Europea. (2014, 13 de mayo). *Sentencia (de la Gran Sala) C:*

2014: 317 (Google Spain S. R. L. y Google Inc. vs. Agencia Española de Protección de Datos y Manuel Costeja González).

Trotti, R. (2011, 20 de diciembre). Internet, un nuevo derecho humano. *Vanguardia.* Recuperado de https://vanguardia.com.mx/columnas-Internetunnuevoderechohumano-1182879.html

Varela Adsuara, B. (2016, 5 de setiembre). ¿Quién responde si me roban mis datos o archivos en Internet?. *El País.* Recuperado el 16 de febrero de 2019 de https://elpais.com/tecnologia/2016/09/05/actualidad/1473063219_596119.html

Villavicencio, F. (2015). Delitos informáticos en la Ley 30096 y la modificación de la Ley 30071. *Revista Virtual del Centro de Estudios de Derecho Penal de la Facultad de Derecho de la Universidad de San Martín de Porres,* 2015, (2), 1-30. Recuperado el 16 de febrero de 2019 de http://www.derecho.usmp.edu.pe/cedp/revista/articulos/Felipe_Villavicencio_Terreros_Delitos_Informaticos_Ley30096_su_modificacion.pdf