pensar
Revista de Ciências Jurídicas
e-ISSN:2317-2150
DOI: 10.5020/2317-2150.2018.8447

Derecho fundamental al Internet: contenido esencial

Direito fundamental à internet: conteúdo essencial

Fundamental right to the Internet: essential content

César Landa Arroyo*

Resumen

La interconectividad va creciendo año a año, gracias al uso de las nuevas tecnologías de la comunicación, como el internet, que está modificando no solo el goce y ejercicio de los derechos fundamentales, particularmente los 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. El internet es el fundamento principal para construir la nueva identidad de los derechos fundamentales. La protección del libre acceso - informado y consentido - al 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 inter conexión entre las personas. Por eso, el Estado debe asegurar el intercambio libre, abierto, equitativo y sin discriminación de la comunicación e información mediante una regulación sin privilegios personales u obstáculos por razón de contenidos políticos, económicos, culturales o sociales.

Palabras Claves: Internet y derechos fundamentales. Libertad del internet. Controle de la vigilancia electrónica.

Resumo

A interconectividade está crescendo ano a ano, graças ao uso de novas tecnologias de comunicação, como a internet, que está mudando não só o gozo e exercício dos direitos fundamentais, em particular aqueles relacionados à liberdade de expressão e ao direito à intimidade, mas também tem sido um repensar do modelo de organização social, cultural e econômico do Estado e os cidadãos. A internet é o principal alicerce para construir a nova identidade dos direitos fundamentais. A proteção de acesso livre - e consentimento informado - a internet exige, pois, neutralidade para garantir a pluralidade e a diversidade do fluxo de informação. Portanto, o Estado deve assegurar a comunicação e a troca de informação de maneira livre, aberta, equitativa e não discriminatória mediante regulação sem privilégios pessoais ou obstáculos por causa do conteúdo político, econômico, cultural ou social.

Palavras-chave: *Internet e direitos fundamentais. Liberdade da internet. Controle da vigilância eletrônica.*

Abstract

Interconnectivity is growing year after year, thanks to the use of new communication technologies, such as the Internet, which is modifying not only the enjoyment and exercise of fundamental rights, particularly those related to freedom of expression and the right to privacy, but also has involved a rethinking of the model of social, cultural and economic organization of the State and citizens. The internet is the main foundation to build the new identity of fundamental rights. The protection of free access - informed and consented - to the internet, therefore, requires neutrality to guarantee the plurality and diversity of the information flow; inasmuch as, the internet is a good of public domain that allows the interconnection between people. Therefore, the State must ensure the free, open, equitable and non-discriminatory exchange of communication and information through regulation without personal privileges or obstacles due to political, economic, cultural or social content.

Keywords: *Internet and fundamental rights. Freedom of the internet. Control of electronic surveillance.*

* Ex-Presidente del Tribunal Constitucional. Coordinador del Área de Derecho Constitucional en la Pontificia Universidad católica del Perú. Profesor de Derecho Constitucional en la Pontificia Universidad católica del Perú y en la Universidad Nacional Mayor de San Marcos. Lima- Peru. E-mail: clanda@pucp.edu.pe.

1 Introducción

En el Perú la mitad de la población de 30 millones de habitantes está conectada al Facebook, y, existe alrededor de 31 millones de teléfonos celulares, a través de los cuales millones de personas se conectan al internet. Asimismo, el Perú es el octavo país latinoamericano con mayor cantidad de usuarios en Facebook y el número 24 a nivel mundial.

Es que el Perú no está ajeno al cambio de los paradigmas mundiales de la economía y la política; acontecido con 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. Este orden estuvo basado en la tensión entre el capital y el trabajo, que ordenó a los países bajo la órbita de los Estados Unidos con los valores de la libertad y el mercado, y, de la otrora Unión Soviética, con los valores del trabajo y el Estado.

Dicho cambio fue muy importante, debido a que se cerró el modelo de confrontación de la guerra fría, entre los dos sistemas ideológicos mundiales, y; se transformó hacia una sociedad global de la comunicación y la tecnología. En ese escenario, el internet es un producto del desarrollo científico al servicio de la sociedad, y; por tanto, permiten el acceso a la información, su almacenaje, procesamiento y transmisión de datos, que se viene incrementado exponencialmente en la actual "era digital".[1]

Esta sociedad de la información promovida por los países desarrollados en la era post industrial, constituye una oportunidad estratégica para las sociedades en vías de desarrollo para contribuir a superar su situación de retraso económico y social; así como, para potenciar la protección y desarrollo de los viejos y nuevos derechos fundamentales, a través del internet y las nuevas tecnologías; en la medida que la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado, según dispone el artículo 1 de la Constitución Política (CP).

Así, en el Perú la convergencia de las tecnologías de la informática –equipos y softwares, las telecomunicaciones –televisión y radio- y la comunicación digital –telefonía móvil-, están generando aceleradas transformaciones de índole social, económica y política. En esta era digital, el internet se viene 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; pero, también está sirviendo para expandir el control del Estado y las corporaciones sobre la vida privada de las personas.

Por ello, nos interesa analizar el internet, como un nuevo derecho en sí mismo, a raíz del impacto en todos los ámbitos de la vida humana, particularmente perfilando su naturaleza y contenido esencial como un nuevo derecho fundamental; así como, analizar la escasa jurisprudencia administrativa sobre la materia que muestra el control de los excesos de las empresas y también usuarios de las relaciones digitales; todo lo cual pone en evidencia la necesidad de regular los alcances y los límites del internet, en un balance con los derechos fundamentales.

2 Internet y derechos fundamentales

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.

En el marco del nuevo paradigma de la sociedad de la información y del conocimiento, el internet se convierte en un derecho (GARCÍA MEXÍA, 2016, p. 17-39); en la medida que, faculta a todas las personas a

1 Al respecto, 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.

través de las nuevas tecnologías, ampliar sus posibilidades de goce y ejercicio de los derechos fundamentales; aunque, directamente potencializa los referidos a la libertad de expresión y el libre acceso a la información (CONSEJO DE LA UNIÓN EUROPEA, 2014, p. 6-8).

Más aún, en la medida que los derechos fundamentales son universales, interdependientes e indivisibles, 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. Lo cual demanda que los Estados cumplan con sus compromisos internacionales de garantizar y promover los derechos humanos, en esta nueva 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 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.

3 Contenido esencial del derecho al internet

Como todo derecho fundamental el derecho al internet debe contar con un contenido esencial constitucionalmente protegido, que se deriva de la articulación de 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 (artículo 2°- 4 CP); 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 (artículo 2°- 5 CP); a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (artículo 2°- 6 CP), y; al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias (artículo 2°-7 CP).

En ese sentido, como el internet entrelaza directamente a 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 al internet, mediante un conjunto de atributos en su contenido constitucionalmente protegido:

3.1 Acceso al internet

El acceso informado y consentido a internet es una condición indispensable para poder gozar no solo de las libertades comunicativas, sino todos los demás derechos fundamentales. Pero, como el internet consiste en un sistema de grandes redes interconectadas, ello supone dos condiciones: Primero, que las personas cuenten con un equipo –*hardware*- y un programa –*software*-, que les permita acceder al internet. Segundo, 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.[2]

Pero, como el acceso público al internet tiene un costo, en algunos países de la región su acceso es gratuito dada las políticas de Estado para mejorar la educación pública básica e incluso la integración social de los jubilados. (URUGUAY, 2016). La inclusión digital para determinados grupos humanos vulnerables –particularmente de las zonas rurales- es importante; sin perjuicio de poner el 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.

2 Cfr. Los programas nacionales de aprovechamiento de nuevas tecnologías de información y comunicación, para la educación pública del Ministerio de Educación del Perú. (PERU, 2016).

Para asegurar dicho acceso al internet, informado y consentido, se deben 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 los *hardware* y *software*: para lo cual, se debe asegurar el acceso universal, mediante la interconectividad de los protocolos e infraestructuras de comunicación; esto es lo que se ha venido a establecer como el "principio de neutralidad". (PROYECTO…, 2015).

Al Estado también le compete regular el acceso al 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; sin perjuicio de establecer políticas de acciones afirmativas para facilitar el acceso al internet a personas en situación de discapacidad y a comunidades marginadas, especialmente. Promoviendo que las corporaciones privadas no establezcan barreras arbitrarias o desproporcionadas de acceso al internet, sino por el contrario amigables para todas las personas, dado su carácter de universal.

En ese entendido, la protección del libre acceso - informado y consentido - al 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 inter conexión entre las personas. Por eso, el Estado debe asegurar el intercambio libre, abierto, equitativo y sin discriminación de la comunicación e información (TÉLLEZ VALDÉS, 2015, p. 252-253), 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 porque así lo exige la naturaleza de las cosas, pero no por la diferencia entre las personas, como dispone el artículo 103 de la Constitución.

3.2 Libertad del internet

Toda persona tiene derecho a la libertad personal en el marco de su libre desarrollo y bienestar, en la medida que nadie está obligado a hacer lo que la ley no manda, ni impedido de hacer lo que ella no prohíbe (artículo 2°-24-A CP); pero, también, debe gozar de la protección de su libertad frente a los peligros de una actuación desproporcionada o arbitraria 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,[3] también es un medio de acceso para el robo de la identidad digital, el intrusismo, el uso indebido de datos por terceros, o, el ciber-acoso; así como, toda forma de delito que se cometa utilizando el internet. Por eso, el Estado requiere tomar medidas especiales desde las políticas de educación, campañas de prevención y el combate delictivo nacional e internacional.[4]

Sin perjuicio de los delitos informáticos, también se cometen abusos en el uso o administración del internet que configuran conflictos de derechos o potestades entre los usuarios y los proveedores.[5] De allí que, sea constitucional que el Estado regule la resolución de los conflictos y señale las ulteriores responsabilidades, con criterios de legitimidad y ponderación en el ámbito de los derechos digitales.

Sobre todo porque, en los últimos años se han planteado desafíos y conflictos entre el entorno digital y la libertad de expresión, libertad de información, acceso a la información pública, derecho a la

---

[3] Cfr. Comisión Interamericana de Derechos Humanos. *Libertad de expresión e internet.* OEA, 2013. Ver: <http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf. p. 17>.

[4] Cfr. Ortego Ruiz (2015, p. 174); Villavicencio (2016).

[5] Cfr. Ministerio de Justicia y Derechos Humanos – Dirección General de Protección de Datos Personales. Resolución Directoral N° 026.2016-JUS/DGPDP del 11 marzo 2016, mediante la cual multó a la empresa Google Perú S. R. L. o Google Inc., por no retirar los datos personales de un ciudadano peruano que había tenido un proceso penal, pero del cual ya había sido absuelto. Asimismo, revisar la decisión del Tribunal Europeo de Derechos Humanos. C: 2014: 317, del 13 de mayo de 2014, donde se consagra 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".

autodeterminación informativa, a la privacidad, al honor público, derechos de autor, así como, el interés superior de niñas, niños y adolescentes (ORIZAGA; CABRERA, 2015, p. 185-196). Casos en los cuales debe garantizarse la protección de contenidos mínimos, regulando los alcances del derecho al internet.

Ahora bien, los requisitos que debe cumplir cualquier regulación o restricción de los derechos digitales a los proveedores y/o usuarios son: 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 exigidas gubernamentalmente 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 debería ser admisibles cuando contengan o son usados con fines ilícitos. Tarea que corresponde determinar al Estado, y, aplicar a las empresas en tanto violen los términos contractuales y/o de uso establecidos, de conformidad con la ley y los principios constitucionales.

Pero, ante el vertiginoso avance de las nuevas tecnologías la regulación estatal se encuentra rezagada, desprotegiendo muchas veces al usuario frente a las empresas proveedoras de servicio de internet (PSI), de alojamiento de sitios web, plataformas de redes sociales y los motores de búsqueda. Las cuales permiten o también 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. Con lo cual 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 (artículo 65° CP).

Todo ello sobre la base de asumir que el negocio del internet es global, en la medida que brindan servicios de acceso e interconexión al internet con programas, sitios web, motores de búsqueda y redes sociales. Escenario donde también se producen pugnas entre las empresas de telecomunicaciones y/o las empresas informáticas; procurando unas y otras monopolios o posiciones dominantes del mercado, poniendo a veces en peligro la libertad de acceso en igualdad de condiciones a todos los servicios de internet – principio de neutralidad.[6]

3.3 Seguridad del internet

Con el vertiginoso desarrollo de las nuevas tecnologías la seguridad de los internautas se ha puesto en peligro; no solo por la acción de la delincuencia informática que se acrecienta, sino también por los excesos comerciales de las empresas proveedoras del derecho al internet y por la intrusión del Estado no solo nacional en las llamadas actividades sospechosas de los internautas. Lo cual, entonces, demanda establecer medidas de seguridad que al suponer restricciones a la libertad del internet, deben estar basadas en los principios básicos de legalidad, necesidad y proporcionalidad.

La llamada "ciberseguridad" abarca desde la infraestructura y las redes a través de las cuales se provee el servicio de internet. Para lo cual, también se requiere que los titulares disfruten de conexiones seguras en internet y cautelen la reserva de sus claves de acceso y evitar la acción ilícita de los *hackers* y *crackers*.[7]

A efecto de proveer seguridad sin afectar el contenido esencial del derecho al acceso y a la libertad e igualdad del internet es importante delimitar el alcance de la ciberseguridad, debido a que desde una concepción amplia de la misma se podría afectar desproporcionadamente esferas de la integridad de las

---

[6] Cfr. Las empresas Verizon y AT&T de los Estados Unidos afirman 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 el mercado del internet. Por el contrario, Twitter, Netflix, Yelp, consideran que es necesario asegurar que los proveedores de Internet eviten acuerdos que puedan favorecer un servicio y bloquear el de la competencia. En: <https://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>. Consultado el: 8 sept. 2016.

[7] Cfr. Varela (2016). Asimismo, Yahoo sufrió el mayor ciberataque el 2014, cuando los *hackers* robaron 500 millones de credenciales de sus usuarios. MySpace admitió en junio que le habían robado 360 millones de cuentas y, Linkedin sufrió el robo de 100 millones de claves (NIETTO, 2016).

redes e infraestructura de internet, ó, la integridad y confidencialidad de la información que portan los cibernautas. Pero, desde una concepción estrecha 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.

Ello en la medida que, se debe otorgar una posición jurídica preferente al ejercicio de la libertad de expresión, acceso a la información y difusión del pensamiento, las que aun pudiendo ejercerse con abuso del derecho, desviación o exceso de poder, o, con una posición dominante en el mercado, *prima facie* no merecen su rechazo penal. Por cuanto dichos actos o medidas provienen de usuarios, proveedores y autoridades del Estado que también constituyen una garantía institucional de las sociedades democráticas, pluralistas y tolerantes, para contribuir al mayor tráfico de ideas y críticas, a partir de establecer el derecho al internet con libertad, igualdad y seguridad para todos los internautas.

El ese entendido, las políticas y regulaciones legales deben ser proporcionales a los riesgos que se enfrenta la sociedad digital, ponderando el ejercicio de los derechos fundamentales y la seguridad ciudadana; asimismo, deben hacer público los acuerdos establecidos con los intermediarios privados, así como, las medidas de seguridad que implementan los proveedores de servicios.

3.4 Privacidad e internet

Si bien 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 se encuentra inserta en diversas bases de datos de los sistemas informáticos públicos y privados, para poder gozar y ejercer derechos fundamentales. No obstante, toda persona tiene derecho a mantener un espacio individual y familiar privado, ajeno al Estado y a terceros; en ese ámbito desarrollar su proyecto personal de vida; mantener en secreto los datos que se generen en ese espacio que considere necesario, y; proteger el derecho a su propia imagen de terceros (CÓRDOBA; DÍEZ-PICAZO, 2016).

La privacidad no es incompatible con la libertad de expresión y derecho a la información, pero, supone cuando menos dos políticas muy claras: una, la protección de datos personales, y, dos, la protección del discurso anónimo.

La protección de datos personales mediante el derecho a la autodeterminación informativa requiere que el Estado regule el almacenamiento, procesamiento, uso y transferencia de los mismos;[8] esto, es que se debe prohibir el uso de datos que violen derechos fundamentales, vinculados especialmente a la intimidad personal y familiar, así como, asegurar el derecho del titular al acceso a dichos datos, la corrección o supresión razonablemente de los mismos de las intromisiones indebidas.

Para tal efecto, el habeas data es el proceso constitucional reconocido en la Constitución[9] y desarrollado en el Código Procesal Constitucional,[10] que tutela no solo el derecho a la autodeterminación informativa, sino también derecho de acceso a la información pública.

La participación en el debate público a través de la redes sociales y el internet sin revelar la identidad del emisor es una garantía de las democracias modernas (SANJURJO, 2015, p. 540); dado que así protegen

---

8 Constitución Política. "Artículo 2º.- Toda persona tiene derecho: […]. 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."

9 Constitución Política. "Artículo 200º.- Son garantías constitucionales: […]. 3. La Acción de Hábeas data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos da que se refiere el artículo 2º, incisos 5 y 6 de la Constitución".

10 Código Procesal Constitucional. "Título IV. Proceso de Hábeas Data. Artículo 61.- El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética, o que obre en cualquier otro tipo de soporte material. Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica, o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicios o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privados que afecten derechos constitucionales".

a los usuarios que podrían sufrir represalias por la difusión de sus opiniones y críticas a los poderes públicos o privados; que en algunos casos ha supuesto llamar a movilizaciones ciudadanas, sobre todo a los jóvenes, para manifestarse u organizarse políticamente para cuestionar medidas arbitrarias en el Perú como "la repartija" o la llamada "Ley Pulpin" (CISNEROS, 2015), o, contra autoridades dictatoriales y/o corruptas en el mundo como ha sucedido en Egipto, Libia o Marruecos (CORTES, 2012).

Como toda regla existen excepciones, así el anonimato no protege de cualquier información del acceso o difusión de cualquier información, sobre todo si se trafica con pornografía infantil, se hace propaganda a la guerra o apología al odio racial, sexual, o, al genocidio. De modo que, la autoridad competente tendría la legitimidad para develar la identidad del emisor y tomar las medidas administrativas y/o judiciales correspondientes.

Desde luego que los registros informáticos de las entidades públicas o privadas que lo requieran, así como, en las transacciones comerciales o de interacciones sensibles, la identificación y autenticación de los usuarios en línea es una garantía de la seguridad jurídica de la transacción; pero, siempre conforme al principio de proporcionalidad en función del tipo de riesgo alto o intermedio que exista; pero, si este riesgo es bajo el anonimato debe ser la regla a aplicar.

3.5 Derecho al olvido digital

El desarrollo del internet ha traído consigo nuevas amenazas a los derechos fundamentales, en la medida que el internet se constituye como un registro permanente de los datos que se suben a la red de redes. De ahí que registros o noticias sobre antecedentes penales o fotografías y vídeos en 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 cancelar o suprimir los 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.

En la doctrina, se discute sus alcances, ya que de un lado se señala que este derecho al olvido puede ser entendido como un derecho a cancelar o anonimizar los datos referidos a los antecedentes judiciales de las personas, especialmente penales, que obran en bases de datos o repertorios jurisprudenciales disponibles en internet; también como un derecho nuevo que deriva de las facultades de cancelación de los datos y la oposición a su tratamiento y divulgación que forman parte del contenido del derecho a la protección de datos personales y que tienen regulación legal expresa en las leyes de protección de datos; y en estricto el derecho al olvido como un derecho a que se eliminen los datos de una persona alojados en internet, tanto de las web fuentes como de los motores de búsqueda (DE TERWANGNE, 2012).

Desde la perspectiva jurisprudencial, bajo los lineamientos de la decisión del Tribunal de Justicia de la Unión Europea, en el caso Google Inc. y Google Spain v. Agencia Española de Protección de Datos y Mario Costeja González, se ha considerado que el derecho al olvido debería ser entendido como un derecho del interesado a solicitar que la información de que se trate sobre su persona ya no se ponga a disposición del público en general mediante su inclusión en la red (CORRAL TALCIANI, 2017).

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, sobretodo, si a partir de los principios democrático 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.

También se ha vinculado el derecho al olvido con el derecho a la identidad, antes que con la privacidad. Se señala que el derecho a la privacidad faculta a la persona a mantener alejado del conocimiento del

público ciertos datos o informaciones atinentes a su intimidad personal. En buena cuenta, este derecho presupone que la información no sale de la esfera íntima. En cambio la información que obra en la red ha sido puesta ahí por su propio titular o este, en principio, ha consentido su tratamiento y alojamiento en la red por terceros. De ahí que, ya no haya privacidad o intimidad cuando la información se sube a la nube. Por ello, se sostiene que el derecho al olvido se fundamentaría en el derecho a la identidad, en la medida que el control que se ejerce mediante el olvido, que conlleva la cancelación o eliminación de datos y registros que obran en la red, facilita el ejercicio de la identidad, en la medida que se elimina la identidad del pasado para construir una nueva (ANDRADE, 2012, p. 74-75).

Las posiciones doctrinales, las sentencias reseñadas y la legislación comparada solo son un indicativo de que hay muchos aspectos que son constantemente discutidos en torno al concepto y alcances del derecho al olvido, como un contenido esencial del derecho fundamental al internet, dado el vertiginoso desarrollo del entorno digital.

3.6 "Seudonimización"

Como el derecho al internet no solo permite el acceso a base de datos y a la interconectividad, sino también a ejercer la libertad expresión, el acceso al internet debe permitírsele a todo usuario identificado o identificable, de acuerdo a los requerimientos que no infrinjan la ley o los contratos. Los usuarios son todas las personas que gozan de derechos fundamentales para el amplio acceso y uso eficiente del internet, como el seudonimización o anonimato, en el acceso a la información pública; dado que les permite garantizar tres derechos fundamentales siguientes (ARROYO, 2016):

Libertad de expresión. Bajo el anonimato no solo se potencializa las denuncias pública y privadas, permitiendo que los grandes poderes queden al descubierto de ciertas prácticas contrarias al orden pública o a la opinión pública; pero, también, el anonimato viene siendo usado para producir información falsa, pornografía de menores, discursos de odio, acoso y hostilización sobre determinadas personas. En este contexto, el agresor y/o emisor anónimo resultan ser un problema poder identificarlo.

Estas situaciones de agresiones, violaciones y manipulación de la opinión pública debe ser una preocupación para el Estado, con junta razón, a fin de regular el anonimato; pero, no para controlar todos los contenidos en internet. Por cuanto, la esencia del internet se basa en la libre interconectividad entre los usuarios; esto es, trasladar información sin restricción, propio de los derechos de acceso a la información, libertad de información, libertad de opinión y expresión.

Privacidad. Los datos personales seudonimizados –*nickname*-, que cabría atribuir a una persona física constituye un derecho a fin de proteger esta esfera de la intimidad, ante las distintas formas de intrusiones y violaciones, tanto de particulares como de agentes el Estado, de las esferas de la intimidad y/o privacidad personal y familiar. Lo que no es óbice para que una persona física sea identificable, directa o indirectamente, por razones objetivas derivadas de infracciones a deberes públicos u obligaciones privadas, previstas en la ley, que demanden su identificación rápida y oportuna.

Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima de forma absoluta, salvo a la información que no guarda relación con la infracción de bienes públicos y derechos privados imputable a la persona física "anonimazada", ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo.

Seguridad personal. El anonimato protege a los usuarios en las redes, en la medida que no es pasible o hace complicado que alguien atente contra un usuario anónimo. Como no recordar a la "primavera árabe", que simbolizó cómo las redes sociales cambiaron el curso de años de gobiernos autoritarios, a partir de una simple foto subida al internet y viralizada por "otros más"; asimismo, el anonimato en la campaña para las elecciones presidenciales a través del twitter y facebook han jugado un rol a veces determinante. (UNA…, 2018). Debido que el uso del internet a través del anonimato ha permitido que voces no escuchadas salgan a la luz pública y ello dentro de un modelo democrático es lo deseable.

No obstante, al igual que en el ejercicio derechos comunicativos el Estado pueda establecer regulaciones sobre el anonimato en el internet, en situaciones muy excepcionales y avaladas por los instrumentos internacionales como lo prevé la Convención Americana de Derechos Humanos en el Artículo 13 inciso 4.

En consecuencia, se debe de considerar a la al anonimato o seudonimización como un contenido esencial del acceso y uso del internet; en virtud del cual, el Estado debería regularlos en el tratamiento de datos personales; el mismo que no debe excluir al responsable del almacenamiento, tratamiento y transmisión de datos, para que adopte las medidas técnicas y organizativas necesarias para garantizar que se aplique razonablemente el anonimato en el marco de la protección datos personales. En esa media la seudonimización o anonimato debe ser concebido como parte del contenido constitucionalmente protegido del derecho fundamental al internet.

3.7 Control de la vigilancia electrónica

Las amenazas del terrorismo, el narcotráfico, la trata de personas, entre otras modalidades delictivas de alcance nacional y/o internacional, ha llevado a los Estados a establecer estándares de prevención y persecución de los delitos, mediante acuerdos internacionales, para desarrollar políticas y leyes nacionales armonizadas para combatir la delincuencia internacional y nacional.[11]

Para lo cual, el uso de programas o sistemas de vigilancia electrónica de las comunicaciones privadas de acuerdo a ley, resulta ser una medida adecuada y necesaria cuando se la use de forma estrictamente proporcional a los fines legítimos perseguidos por las autoridades. Por eso, la Corte Interamericana de Derechos Humanos ha planteado los límites de la apelación de algunos Estados a la doctrina de la seguridad nacional,[12] cuando se vaya a usar como argumento para vigilar la correspondencia y los datos personales, por su discrecionalidad y excesos.

El desarrollo de las nuevas tecnologías permiten a las industrias de las tele comunicaciones e informática desarrollar cada vez más sofisticados sistemas, programas y aparatos de vigilancia electrónica; que demandan de nuevos estándares de protección de los derechos fundamentales, para no cometer excesos que afecten a terceros o a los investigados, sino en lo estrictamente necesario. Y si se cometen, existan mecanismos de control no solo del Estado sobre los privados, sino también de la ciudadanía y/o sus representantes sobre el Estado. Por cuanto, la interceptación y el almacenamiento de datos de las comunicaciones privadas en la era digital, constituye un grave peligro para los ciudadanos e incluso autoridades.

Por eso, los paladines mundiales de la libertad de la información por internet y del derecho a la privacidad como Edward Snowden han contribuido al mundo con las revelaciones del espionaje gubernamental de los Estados Unidos – programa *PRISM-,*[13] Julian Asange ha aportado la difusión de documentos oficiales filtrados sobre asuntos de interés público mantenido en secreto por los gobiernos –*Wikileaks*-,[14] o, el Consorcio Internacional de Investigación Periodística (ICIJ) ha difundido las actividades empresariales no éticas o ilegales de personajes públicos de fama internacional -*The Panama Papers*.[15]

Como los derechos fundamentales tienen límites, 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; pero, ello, no significa que el interés

---

11 Cfr. Convenio sobre la ciberdelincuencia – Budapest, 23-11-2001. Es el primer tratado internacional con el cual los Estados tratan de enfrentar a los delitos informáticos y a los delitos en Internet, a través de procurar la homogenización de leyes nacionales, la mejora de las técnicas de investigación y la cooperación policial entre los países. (CONVENIO SOBRE LA CIBERDELINCUENCIA, 2001).

12 Corte IDH. *Molina Theissen vs. Guatemala.* Sentencia de 4 de mayo de 1004 (Fondo). Párrafo 40.2.

13 *PRISM* es un programa mundial de espionaje de la Agencia de Seguridad Nacional del Gobierno de los Estados Unidos, en base a la Ley de Vigilancia de la Inteligencia Extranjera, que se reforzó con la Ley Patriótica, después del derribo a las torres gemelas de Nueva York, caracterizado por capturar los datos de las comunicaciones electrónicas privadas de compañías como Google, Apple, Microsoft o Facebook. Cfr. FACTS… (2013).

14 Cfr. EL PENTÁGONO… (2016). Como respuesta el Congreso de los Estados Unidos aprueba la Ley *SHIELD* (*Securing Human Intelligence and Enforcing Lawful Dissemination*), prohibiendo la publicación de información clasificada sobre secretos internacionales de inteligencia.

15 Cfr. The International Consortium of Investigative Journalists. “Los papeles de Panamá” que aporta a la opinión pública información sobre la elusión y defraudación fiscal de empresas y personajes públicos –jefes de Estado, políticos, artistas, deportistas, etc.-, que alcanza a más de 11,5 millones de documentos del bufete de abogados panameños Mossak Fonseca.

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 sobre las propias actividades ilícitas de los aparatos de seguridad del Estado en materia de vigilancia electrónica, como de las empresas y personajes defraudadores del Estado.

4 Jurisprudencia administrativa sobre internet y derechos fundamentales

Realizado el planteamiento de la naturaleza del internet como un derecho, con todas las ventajas y dilemas que presenta sobre 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 año 2011 el Congreso de la República dictó la Ley 29733, Ley de Protección de Datos Personales (LPDP), creando la Autoridad Nacional de Protección de Datos Personales, radicada en la Dirección General de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, la misma que conoce 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 LPDP, que se inicia de oficio o denuncia de parte.

b) Procedimiento trilateral de tutela para la protección de los derechos reconocidos en la LPDP a 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 el año 2014 ha resuelto casos vinculados a ambos tipos de procedimientos. En dicho sentido, a la fecha en los casos resueltos se pueden observar lo siguiente:

Tipo de procedimiento	Número de casos resueltos
Procedimientos administrativos sancionadores	42[1*] (*)
Procedimientos trilaterales de tutela	39[2**] (**)
Total	91

Fuente: PERÚ. Minjus (2016).

* 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 el 2013 se resolvieron 3 casos, en el 2014 fueron 17 y en el 2015 se han resuelto 19 casos.

Elaboración: Propia

Se han revisado todos los casos publicados en el portal institucional de la DGPDP de los cuales se han seleccionado 5 casos de procedimientos sancionadores y 6 casos de procedimientos trilaterales de tutela (3 del 2014 y 2 del 2015). La selección ha tenido como criterio el que el caso se vincule 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 datos personales (procedimiento trilateral).

4.1 Casos sobre procedimientos sancionadores[16]

A. Caso Clínica San Felipe

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

Al respecto, en su descargo, 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 que la información recabada podía ser ubicada en otras bases de datos de acceso público como guías telefónicas, registros del RENIEC y guías profesionales en el caso de los correos electrónicos, por ello, sostenía, que no sería información que afectase su esfera íntima. La Clínica también señaló que la información recaba 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, siendo controvertible únicamente 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, que de acuerdo a lo establecido en el artículo 5 de la LPDP, el tratamiento de datos personales requiere el consentimiento de su titular. Sin embargo, según el artículo 14.5 de la misma LPDP 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.

En virtud al parámetro legal citado, el tratamiento de datos personales de los clientes de la Clínica, quienes mantenían una relación contractual, se efectuaba 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", es un tratamiento adicional de datos personales que sí requería el consentimiento de su titular, siendo más evidente ello 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 (numeral 10.8 de la Resolución).

En esa misma dirección, se señaló que no resultaba de aplicación la excepción al consentimiento del titular, prevista en el artículo 14.2 de la LPDP, que establece que no se requiere el consentimiento para el tratamiento de datos obtenidos de fuentes accesibles al público, en la medida 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 de su página web, con lo que se requería su consentimiento (numeral 10.11 de la Resolución).

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, 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

[16] Para identificar a los casos se ha utilizado el nombre del administrado sujeto al procedimiento sancionador. Asimismo, se debe precisar que se ha tomado aquellos aspectos de los casos que vinculan el tratamiento de los datos personales con el uso del internet.

el consentimiento (numeral 10.16). No era previo, pues la recopilación de los datos se daba con la sola navegación en la web. Tampoco era expreso e inequívoco, pues por sus propias características, con la sola navegación en web la Clínica presumía el consentimiento del usuario. Tampoco era informado pues de acuerdo a la propia información de la Política no se sabía a quién debería dirigirse la revocación para el tratamiento de los datos y cuál era la finalidad específica de su tratamiento (numerales 10.15 a 10.19 de la Resolución).

Por las razones expuestas se sancionó a Clínica San Felipe con cinco Unidades Impositivas Tributarias por usar formas de consentimiento inválidas para el tratamiento de datos personales. Asimismo, cabe precisar que esta decisión fue declarada firme mediante Resolución Directoral 028-2015-JUS/DGPDP de fecha 21 de setiembre de 2015, que rechazó el recurso de apelación de Clínica San Felipe 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 no solo del conocimiento del usuario sino también de su consentimiento para poder asegurar su derecho de acceso al internet, libre e informado. Para lo cual las fórmulas del 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, dado que el proveedor del servicio es el único que al ofrecer un producto lo conoce 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, protege en particular la salud y la seguridad de las personas, señala el artículo 65 de la Constitución.

B. Caso SENTINEL PERU SA

SENTINEL PERU SA es una empresa dedicada al rubro de centrales privadas 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 los montos, estado, calificación crediticia y situación de morosidad). En el mismo contexto, el director comercial de la empresa en diversos medios de comunicación difundió 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, de fecha 11 de noviembre de 2015, SENTINEL PERU SA fue sancionada con 42 UIT por efectuar tratamiento de datos personales con infracción de los principios de finalidad y proporcionalidad de la LPDP,[17] decisión que fue confirmada mediante Resolución Directoral 0006-2016-JUS/DGPD de fecha 22 de enero de 2016.

En primera instancia, la empresa sancionada alegó como sustento de su defensa los siguientes argumentos: a) 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 dedicas al rubro a efectuar tratamiento de datos crediticios para evaluar la solvencia económica de una persona; b) difundir 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), no puede constituir tratamiento de datos sobre convicciones políticas; c) el campo de acción de las centrales privadas de información de riesgo no se circunscribiría solo al mercado financiero sino también el denominado “mercado electoral”; d) la difusión de información a través de la herramienta “Conoce a tu candidato” no constituyó una estrategia publicitaria o de marketing, dado

[17] Ley de Protección de Datos Personales: “Artículo 6. Principio de finalidad Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización. Artículo 7. Principio de proporcionalidad Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados”.

que como central de riesgo también puede realizar fines sociales, lo que se hizo con el acceso gratuito a información crediticia de los candidatos a través de la herramienta citada; e) 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, por lo que no estaría bajo el ámbito de protección del derecho a la intimidad y la LPDP.

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

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 SA había efectuado un tratamiento adicional de datos personales no razonable a su finalidad autorizada como central de riesgos. Asimismo, se concluyó que la empresa se convirtió en un "actor electoral" dado que proporcionaba información para que la ciudadanía decidiera su voto, siendo esta una finalidad ajena a la que como central de riesgos se encontraba autorizada por la Ley de Centrales de Riesgo, cual es entregar un reporte de crédito para evaluar la solvencia económica de una persona, lo cual 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 central de riesgos sí estaba autorizada (numeral 17.2 de la Resolución de primera instancia).

De otro lado, también se concluyó que este accionar constituía una forma de publicidad en beneficio de SENTINEL PERU SA, 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; y que, en todo caso, como toda empresa SENTINEL PERU SA puede efectuar la publicidad que le convenga, pero lo cuestionable es que lo haga difundiendo masivamente datos personales (numeral 18.5 de la Resolución de primera instancia).

Por último, se concluyó que hubo lesión al derecho a la protección de datos personales ya que este no exige 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 SA se encontraba autorizada como central de riesgos (numeral 18.2 de la resolución de primera instancia).

Al apelar la decisión de primera instancia SENTINEL PERU SA sostuvo como argumentos los siguientes: a) la información electoral se encontraría bajo los alcances de la Ley de Transparencia y Acceso a la Información Pública, por lo que al ser información pública era viable que la misma pueda ser objeto de difusión por cualquier privado sin restricciones; b) 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 incurriría 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) considera que el concepto de mercado no solo debería circunscribirse al financiero sino también que 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.

Al respecto, la decisión de segunda instancia que confirmo la multa impuesta a SENTINEL PERU SA, sostuvo que: a) 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 a través de su difusión se

requiere recabar el consentimiento libre, previo, expreso e inequívoco e informado, de lo contrario estamos, como en el presente caso, frente a una infracción al derecho a la protección de datos personales, 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 (numeral 3.2.3 de la Resolución de Segunda instancia); b) 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 (numeral 3.2.2 de la Resolución de segunda instancia); c) 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 esa 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 si se evidencia que el mismo ha tenido fines publicitarios, por lo que es errado sostener que SENTINEL PERU SA que el deber de información de riesgos en el mercado comprende información electoral, pues dicha finalidad no está establecida de forma clara, expresa e inequívoca en la Ley de Centrales de Riego (numeral 3.2.4 de la Resolución de segunda instancia).

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 (DE LA CUEVA, 1993). Así, el derecho a la autodeterminación informativa permite el control de los servicios informáticos, computarizados o no, públicos o privados, a que no suministren informaciones que afecten la intimidad personal y familiar, según el artículo 2, inciso 6 de la Constitución.

A partir de lo cual, se ha producido una vis expansiva de dicho derecho a la autodeterminación informativa, en la medida que: por un lado, la prohibición señalada no se ha reducido a proteger el clásico derecho a la intimidad, sino también a la intimidad patrimonial; así como, se ha establecido una interpretación restrictiva de la Ley de Centrales de Riesgo para la recopilación de datos personales inclusive que se hallen en bancos de datos públicos, que está acotada a registrar y transmitir información para el mercado –económico-, pero, no información para el "mercado electoral".

C. Casos Cooperativa de Servicios Educacionales San Felipe (San Felipe), Institución Educativa Teresa González de Fanning (Teresa González), CEP Isabel Flores de Oliva (Isabel Flores).

Se ha citado todos los casos de manera conjunta en tanto a todas las instituciones educativas sancionadas se les atribuye una misma infracción el tratamiento de datos personales sin haber recabado el consentimiento de sus titulares, el hecho específico, consiste en publicitar en su página web institucional fotografías de sus estudiantes sin acreditar haber recabado el consentimiento de sus padres o tutores legales.

En dicho sentido, el colegio San Felipe señaló que las fotografías publicadas en su portal web correspondían a una sesión de fotos del verano del año 2011 para la campaña promocional de la admisión de dicho año, que en aquella ocasión todos los padres asistieron y prestaron su consentimiento, que a la fecha de descargo no todos los padres continuaban en el colegio, sin embargo, presentaron el consentimiento firmado por los que aún permanecían con sus hijos en el colegio. Por su parte, Teresa González sostuvo que las imágenes no serían datos personales, sino imágenes de actividades que se realizan en el colegio, pues han sido tomadas en sus instalaciones. Por último, Isabel Flores indicó, como argumento de defensa, que las imágenes de su página web corresponden a ex alumnos del colegio.

Al respecto, la Dirección de Sanciones sostuvo respecto de todos los casos que no se había acreditado que las instituciones educativas hayan obtenido el consentimiento previo y expreso para el tratamiento de los datos personales (imágenes de alumnos o ex alumnos) a través de su página web, que se procedía a sancionar a cada una de las instituciones educativas con las Resoluciones Directorales 117-2015-JUS/DGPDP-DS del 18 de diciembre de 2015 a 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 a Teresa González, y 025-2016-JUS/DGPDP-DS Isabel Flores del 18 de enero de 2016, cabe añadir que estas dos

últimas resoluciones no fueron impugnadas por las instituciones educativas sancionadas por lo que quedaron consentidas en primera instancia.

La propia imagen es un derecho fundamental que la Constitución reconoce a toda persona en su artículo 2, inciso 7 *in fine*; el derecho a la propia imagen de toda persona tiene una doble vertiente, como derecho a su figura humana, y, el derecho a que no se haga uso de su imagen sin su consentimiento. En virtud del cual cualquier utilización de nuestra imagen sin nuestro consentimiento constituye una vulneración de dicho derecho fundamental (ALEGRE MARTÍNEZ, 1997, p. 77-83).

No obstante, que las imágenes captadas de los alumnos y alumnas de las instituciones educativas fueron realizadas en sus locales y en el marco de sus actividades de formación, hizo bien la Autoridad en establecer un escrutino estricto para controlar el registro de los datos personales, en la medida que se requiere el consentimiento expreso de la voluntad de cada persona para ceder su propia imagen, en tanto derecho fundamental indisponible por terceros (PASCUAL MEDRANO, 2003, p. 44-55).

4.2 Casos sobre procedimientos trilaterales[18]

A. Caso “El Comercio”

El denunciante[19] cuestionaba 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) que 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 ex presidente Alejandro Toledo. En la web de *El Comercio* se mostraba la información a modo de nota periodística con la opinión del ex Presidente Toledo respecto del referido audio. El denunciante consideró al seguir dicha publicación activa al año 2014 se afectada sus derechos a la intimidad, el honor y buena reputación, en tanto ya no actúa en la vida política del país. Por su parte *El Comercio* en su defensa señaló que la publicación se derivó de las declaraciones del ex Presidente brindadas a la prensa en general, por lo que se contenido se ajustó a la labor periodística que cumple como tal; 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” (numeral 10).

Por ello, señaló la Autoridad, 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 ex Presidente Toledo, por lo que existe un interés público en las informaciones vinculadas a la actuación de un ex funcionario público; b) si bien la noticia se difundió en el 2011, al 2014 el interés público no ha dejado de existir, más si en ella está involucrado un ex presidente que sigue vinculado a la vida política del país; c) la noticia se publicó en virtud a las declaraciones del ex Presidente Toledo en el marco de una actividad proselitista siendo 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 y que fueron motivo de la denuncia.

---

[18] Para denominar a los casos se ha empleado el nombre de los denunciados.

[19] En la resolución de la DGPDP se ha tachado el nombre del denunciante para mantener en reserva su identidad y así respetar su derecho al olvido.

Esta decisión fue objeto de un recurso de reconsideración el que fue declarado infundado mediante Resolución 070-2014-JUS/DGPDP de fecha 3 de octubre de 2014. El reclamante como argumentos sostiene, por un lado, que, si bien comparte el criterio de que es legítimo el interés de conocer sobre los cargos y acciones de quienes han sido funcionarios públicos, tales informaciones no deberían haber sido obtenidas por medios ilegales como en el caso en el que se vulnera el derecho a la intimidad personal del reclamante al haberse interceptado una comunicación telefónica, de otro lado, que la relevancia pública de la información ya no se mantendría pues el audio difundido fue interceptado en el año 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 haya sido interceptado de manera ilegal por *El Comercio* y que, en todo caso, el denunciante había optado por la vía penal para cuestionar la ilegal interceptación telefónica. Finalmente, consideró que, a pesar de la cancelación por parte de *El Comercio* de la información sobre el reclamante, la difusión de la noticia y del audio que se hizo en su momento revestía un notorio interés público que el reclamante no había podido desvirtuar.

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

El derecho al olvido o cancelación de datos en internet 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 trata de la exposición de información privada – sobre asuntos de interés político - de cualquier persona, sino de un ex Ministro de Estado.

De modo que, el derecho al olvido no debería ser absoluto, en la medida que se trate de un personaje público; porque, una sobreprotección de sus datos podría afectar la libertad de expresión, que incluye el derecho a la información ciudadana. En un mundo donde cada vez la política se desprestigia por quienes asumen dichas responsabilidades, incluso de elección popular, para medrar de los cargos públicos; parece razonable que la presunción sea más bien el de la publicidad y la excepción sea el derecho al olvido digital (ÁLVAREZ CARO, 2015, p. 107-125).

B. Caso “datosperu.org”

Mediante Resoluciones Directorales 074-2014-JUS/DGPDP de fecha 24 de octubre de 2014 y 075-2014-JUS/DGPDP de fecha 24 de octubre de 2014 se declaró fundada 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 ex funcionario 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 con los datos de los reclamantes 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 donde 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, es una manifestación del principio de transparencia, propio de las sociedades democráticas. Por eso, 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, señala el artículo 2, inciso 5 de la Constitución.

Más aún la Ley de Transparencia y Acceso a la Información Pública, Ley N° 27806, ampara el derecho fundamental a conocer los asuntos públicos, ciertamente solicitando su 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 captadas y difundidas por internet; sino que estas para que estén protegidas deben ser verdaderas en el tiempo, es decir deber ser actualizadas, salvo que se señale su carácter sucedáneo en un momento determinado.

C. Caso del blog “Defensa de los derechos humanos laborales”

El blog citado 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, 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 referido a aspectos sensibles de la personalidad del reclamante y que no era necesario recabar el consentimiento del titular pues la información era de acceso público.

En la Resolución Directoral 030-2015-JUS/DGPDP de fecha 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 esta, no se encuentra protegida por la LPDP. En el 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 que constituye en estricto información en torno a 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 este 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, la LPDP autoriza el acceso sin consentimiento de los datos personales a dichas fuentes, pero no autoriza a su archivo o difusión sin mediar 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 de fecha 24 de noviembre de 2015. De esta 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 el interés público en la difusión de la información.

Respecto del primer aspecto, se concluyó que el blog reclamado en la entrada cuestionada contiene datos personales del reclamante que exceden la identificación del reclamante como representante de la persona jurídica que son tratados 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, más no cuando son 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 que ha reconocido ciertos derechos fundamentales a las personas jurídicas, como el de la autodeterminación informativa[20]; motivo, por el cual podría ser justiciable mediante el proceso constitucional de amparo.

D. Caso "Google"

En el presente caso una persona intentó infructuosamente que *Google Perú SRL* y Google Inc. Cancelen sus datos que aparecen a través del motor de búsqueda *Google Search* que lo vinculan 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 webs que difundían la información cuestionada.

A nivel del procedimiento de tutela, tanto *Google Perú SRL* 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 que se reclama; y 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 considera que el motor de búsqueda *Google Search* (a través del sitio web "http://www.google.com.pe") constituye un 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, esto constituye una clasificación de información que permite luego su acceso a terceros; y, b) porque brinda servicios de búsqueda por internet empleando nombres y apellidos de las personas afectándose con ello su privacidad.

De otro lado, en el análisis se ha concluido que *Google Perú SRL* y *Google Inc.* están vinculados indisolublemente por el tratamiento de la publicidad y las operaciones efectuadas a través de la web http://www.google.com.pe/ estuvieron ubicadas en territorio peruano, por lo que estaban sujetos a la LPDP y su Reglamento y además afectan la privacidad del reclamante.

Asimismo, se ha considerado que al permitirse a los robots de búsqueda vincular y hipervisibilizar los datos personales (nombres y apellidos) del reclamante con la información que se pide cancelar, porque

[20] Tribunal Constitucional. Expediente N° 4972-2006-PA/TC. FJ 14, e.

no se ajusta a los nuevos hechos, dado que 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 ha ordenado 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 han empleado básicamente los argumentos ya reseñados en los párrafos precedentes.

Como el internet es un almacén de información a la que se accede desde cualquier lugar, que se multiplica exponencialmente, la obtención, consulta, y difusión a través de las redes sociales es una tarea muy simple, poniendo en tensión derechos de los usuarios y las empresa prestadoras de servicios de internet. Por eso, parece tan necesario la protección de datos personales, como asegurar los intereses legítimos de los operadores económicos y de los usuarios del internet, en el marco de una interpretación sobre la base del principio de proporcionalidad (RALLO, 2014, p. 257).

5 Conclusiones

El nuevo paradigma de la sociedad de la información y del conocimiento permiten que con el desarrollo del internet y las nuevas tecnologías se potencialice no solo cuantitativamente los derechos fundamentales, sino que también 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 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 del internet; con lo cual, las regulaciones normativas no existen o no prevén el impacto del goce y ejercicio del derecho frente a terceros y bienes constitucionalmente protegidos.

Desde luego, que el internet se está convirtiendo en un nuevo derecho fundamental de las personas; pero, cuya titularidad reposa no solo en el ciudadano sino también en los proveedores –privados y estatales donde fuera- de los insumos estructurales para el uso de esta red de comunicación.

Desde la perspectiva de los derechos fundamentales el internet debe gozar de un contenido esencial, constitucionalmente protegido; debido a que es un bien de dominio público. En virtud del cual el Estado debe asegurar su acceso para todos, la libertad de uso del mismo, la seguridad y privacidad de los datos y comunicaciones, así como, el control de 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 y el internet, como medio de registro y difusión de información, es innegable, dado que todos los días en ella se aloja información que atañe a aspectos personales de los ciudadanos; protegidos por la el derecho a la autodeterminación informativa, del artículo 2, inciso 6 de la Constitución.

Los pocos casos resueltos por la Autoridad Nacional de Protección de Datos Personales demuestran que se está empezando a sentar una línea de protección del derecho a la protección de datos personales, que en todo caso, aún resulta insuficiente. Al respecto podemos ver como se ha sancionado a todas las páginas webs de instituciones educativas, empresas y entidades públicas que emplean imágenes de sus miembros para publicitar sus funciones o servicios sin haber requerido de manera previa el consentimiento de sus titulares (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 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 del internet (casos El Comercio, La República, Blog Defensa de los derechos humanos laborales).

En esa misma dirección ha resultado interesante advertir el análisis que se ha hecho de la difusión de información crediticia de candidatos, en el marco de un proceso electoral, por medio de una empresa del rubro de las centrales de riesgo que no se encontraba autorizada para vincular dicha información económica con la de tipo político.

Todo ello demuestra que quienes son objeto de control son las instituciones y corporaciones privadas que gracias al internet han hecho un uso mercantil de los derechos ciudadanos; pero, que la Autoridad pública ha iniciado una línea de protección de los derechos fundamentales personales.

Pero, constituye un gran desafío 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 Estado. Ello será posible a partir de comprender que todo Estado constitucional tiene como fundamento proteger tanto los nuevos derechos y libertades ciudadanas, como limitar los excesos de los poderes públicos y ahora también privados.

Referencias

ALEGRE MARTÍNEZ, Miguel Ángel. **El derecho a la propia imagen**. Madrid: Tecnos, 1997.

ÁLVAREZ CARO, María. **Derecho al olvido en internet**: el nuevo paradigma de la privacidad en la era digital. Madrid: Reus, 2015.

ANDRADE, Norberto Nuno Gomes de. El olvido: el derecho a ser diferente… de uno mismo. Una reconsideración del derecho a ser olvidado. **IDP.** Revista de Internet, Derecho y Política, Catalunya, n. 13, p. 74-75, 2012. Disponible en: <http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-andrade_esp/n13-andrade_esp>. Consultado el: 29 mayo 2018.

ARROYO, Verónica. El poder del anonimato en la libertad de expresión online. In: JORNADA NACIONAL DE DERECHOS FUNDAMENTALES, I., 2016, Lima. **Anais...** Lima: Pontificia Universidad Católica del Perú, 2016.

CISNEROS, Claudia. El uso de las redes facilita la confluencia alrededor de un tema específico. Entrevista. **#Código-Abierto_CC**, 2015. Entrevistada por Bernardo. Disponible en: <http://codigo-abierto.cc/claudia-cisneros-el-uso-de-redes-facilita-la-confluencia-alrededor-de-un-tema-especifico/>. Consultado el: 12 sept. 2016.

CONVENIO SOBRE LA CIBERDELINCUENCIA. Budapest, 23 nov. 2001. Disponible en: <https://rm.coe.int/CoERMPublicCommonSearchServices /DisplayDCTMContent?document Id=09000016802fa41c>. Consultado el: 12 sept. 2016.

CONSEJO DE LA UNIÓN EUROPEA. **Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet y fuera de Internet**. 9647/14. Bruselas, 2014, p. 6-8.

CORRAL TALCIANI, Hernán. El derecho al olvido en internet: antecedentes y bases para su configuración jurídica. **Revista Jurídica Digital UANDES**, Santiago, v. 1, p. 57-58, 2017.

CÓRDOBA, Diego; DÍEZ-PICAZO, Ignacio. Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico. En: JORNADAS DE LA ASOCIACIÓN DE LETRADOS DEL TRIBUNAL CONSTITUCIONAL, 20, 2016, Madrid. **Anais...** Madrid: CEPC, 2016. p. 99-110.

DE TERWANGNE, Cécile. Privacidad en internet y el derecho a ser olvidado / derecho al olvido. **IDP**. Revista de Internet, Derecho y Política, Catalunya, n. 13, p. 55-63, 2012. Disponible en: <http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_esp>. Consultado el: 29 mayo 2018.

DE LA CUEVA, Pablo Lucas Murillo. **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: CEC, 1993. p. 15-36.

EL PENTÁGONO: Wikileaks sería irresponsable si publica los documentos. **Europa press**. Disponible en: <http://www.europapress.es/internacional/noticia-pentagono-wikileaks-seria-irresponsable-si-publica documentos-20100813085329.html>. Consultado el: 11 sept. 2016.

FACTS on the collection of intelligence pursuant to section 702 of the foreign intelligence surveillance act. Office of the Director of National Intelligence. **Newsroom**, June 8, 2013. Disponible en: <https:// www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-onthe-collection-of-intelligence-pursuant-to-section702-of-the-foreign-intelligence-surveillance-act>. Consultado el: 11 sept. 2016.

FERNÁNDEZ RODRÍGUEZ, José Julio. **Lo público y lo privado en internet**. Intimidad y libertad de expresión en la Red. México: Instituto de Investigaciones Jurídicas – Universidad Nacional Autónoma de México, 2004.

GARCÍA MEXÍA, Pablo. El derecho de internet. En: PÉREZ BES, F. (Coord.). **El derecho de Internet**. Barcelona: Atelier, 2016. p. 17-39.

LAS REDES sociales como núcleo de las movilizaciones ciudadanas a nivel mundial. **Sisgecom**, Bogotá, 14 mar. 2012. Disponible en: <https://sisgecom.com/2012/03/14/las-redes-sociales-como-nucleo-de-las-movilizaciones-ciudadanas -a-nivel -mundial/>. Consultado el: 11 sept. 2016.

LUCAS MURILLO DE LA CUEVA, Pablo. **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: CEC, 1993. p. 15-36.

NIETO, Marya G. ¿Quién está detrás del ataque a Yahoo? **El país**, Madrid, 30 sept. 2016. Disponible en: < https://elpais.com/tecnologia/2016/09/26/actualidad/1474891005_071895.html>. Consultado el: 30 sept. 2016.

ORIZAGA, Isabel; CABRERA, Karen. Sexting y redes sociales: diversas relaciones y consecuencias jurídicas. En: BUENO DE MATA, F. (Coord.). **Fodertics 3.0** - Estudios sobre nuevas tecnologías y justicia. Granada: Comares, 2015. p. 185-196.

ORTEGO RUIZ, Miguel. **Prestadores de servicios de internet y alojamientos de contenidos ilícitos**. Madrid: Reus, 2015.

PASCUAL MEDRANO, Amelia. **El derecho fundamental a la propia imagen**. Fundamento, contenido, titularidad y límites. Navarra: Thomson – Aranzadi, 2003.

RALLO, Artami. **El derecho al olvido en Internet** - Google versus España. Madrid: CEPC, 2014.

SANJURJO REBOLLO, Beatriz. **Manual de internet y redes sociales**. Madrid: Dykinson, 2015.

SARLET, Ingo. Note on the co-called right to be forgotten un Brazil and its acknowlegdment and implementation by the superior courts. En: LANDA, César (Ed.). **Minutes of the Inter-American Conference of Fundamental Rights**. London: PSB, 2018. p. 101-114.

TÉLLEZ VALDÉS, Julio. Libertad de expresión en internet y redes sociales. En: BUENO DE MATA, F. (Coord.). **Fodertics 3.0** - Estudios sobre nuevas tecnologías y justicia. Granada: Comares, 2015. p. 252-253.

VARELA ADSUARA, Borja. ¿Quién responde si me roban mis datos o archivos en Internet? **El pais,** Madrid. 5 set. 2016. Disponible en: < https://elpais.com/tecnologia/2016/09/05/ actualidad/1473063219_596119.html>. Consultado el: 7 sept. 2016.

VILLAVICENCIO, Felipe. **Delitos informáticos en la ley 30096 y la modificación de la Ley 30071**. Disponible en: <http://www.derecho.usmp.edu.pe/cedp/revista/articulos/Felipe_ Villavicencio_Terreros_ Delitos_Informaticos_Ley30096_su_modificacion.pdf>. Consultado el: 3 sept. 2016.

PERÚ. Ministerio de Educación del Perú. **Programas nacionales de aprovechamiento de nuevas tecnologías de información y comunicación, para la educación pública**. Disponible en: <http:// educaciontic.perueduca.pe/?p= 253>. Consultado el: 30 ago. 2016.

PERÚ. Ministerio de Educación del Perú. **Plan Ceibal y Plan Ibirapitá**. 2013. Disponible en: <http://pulsoslp.com.mx/2013/10/25/gobierno-uruguayo-entrega-tabletas-a-escolares-de-4-a-6-anos-deedad/> Consultado el: 30 ago. 2016.

PERÚ. Ministerio de Justicia y Derechos Humanos. **Procedimientos administrativos sancionadores.** 2011. Disponible en: <http://www.minjus.gob.pe/procedimientos-administrativos-sancionadores>. Consultado el: 22 sept. 2016.

PERÚ. Ministerio de Justicia y Derechos Humanos. **Procedimientos trilaterales de tutela.** 2011. Disponible en: <http://www.minjus.gob.pe/ptt-dgpdp>. Consultado el: 22 sept. 2016.

THE INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS. **Los papeles de Panamá**. Disponible en: <https://offshoreleaks.icij.org>. Consultado el: 13 sept. 2016.

UNA consultora que trabajó para Trump robó a Facebook datos de 50 millones de usuarios para influir en las elecciones. **Diario ABC**, Madrid. 2018. Disponible en: <http://www.abc.es/internacional/abci-trump-robo-facebook-datos-50-millones-usuarios-para-influir-elecciones-201803172343_noticia.html>. Consultado el: 2 mayo 2018.

URUGUAY. **Gobierno de Uruguay entrega tabletas gratis a jubilados**. Disponible en: <http://www.scidev.net/america-latina/desarrollo-de-capacidades/noticias/gobierno-deuruguay-entrega-tabletas-gratis-a-jubilados.html>. Consultado el: 30 ago. 2016.

Recebido em: 28/09/2018
Aprovado em: 10/11/2018