El Internet, el *Big Data* y el tratamiento de datos personales

Laisha Mubarak Aguad

Abogada por la Universidad de Lima.
Miembro Asociado de ADV Editores – Revista ***ADVOCATUS***.
Máster en Derecho (LL.M.) por la Universidad de Alicante.

SUMARIO:

RESUMEN:

El internet y las redes sociales han producido una revolución en nuestras vidas, ocasionando una gran dependencia en el quehacer de la sociedad, generando cada vez más una mayor preocupación por la seguridad informática y el adecuado tratamiento de los datos personales en la red, toda vez que el mal uso de esta información podría afectar la privacidad e intimidad personal. No obstante, en la mayoría de los casos, las políticas de privacidad y protección de datos personales ofrecidas a los usuarios son unilaterales y de difícil comprensión, las cuales pocas veces son leídas. Por tanto, la autora, a continuación, nos planteará los nuevos retos para la aplicación de la normativa a estas tecnologías.

Palabras Clave: Protección de Datos Personales, Políticas de Privacidad, Redes Sociales, Internet, *Big Data*.

ABSTRACT:

The internet and social networks have revolutionized our lives, generating a greater dependence on social endeavors, generating a greater concern regarding cyber security and the proper treatment of personal data on the web, since that the misuse of this information could affect our personal privacy. However, in most cases, the privacy and personal data protection policies offered to users are unilateral and difficult to understand, and therefore are rarely read. On that account, the author will raise the new challenges for the application of the regulations to these technologies.

Keywords: Data Protection, Privacy Policies, Social Networks, Internet, Big Data.

I. INTRODUCCIÓN

La seguridad en el ser humano, como necesidad básica, ocupa un lugar importante. En dicho sentido —y trayendo a colación la teoría de las necesidades de Malinowski— la seguridad es una de las siete necesidades básicas a satisfacer por el ser humano[1]. Hoy en día, la seguridad puede analizarse desde ámbitos muy diversos. Hace algunos años, lo más importante para una persona y hasta para la sociedad en su conjunto era la seguridad física. Sin embargo, con el desarrollo del internet, también hemos comenzado a preocuparnos por la seguridad informática y el adecuado tratamiento de los datos personales en la red, toda vez que el mal uso de esta información podría afectar la privacidad e intimidad personal.

El internet y las redes sociales se han convertido en un símbolo característico de la cultura actual. En efecto, como ya lo señalaba Escribano hace algunos años:

> "(...) el *Internet ha supuesto tal revolución que hoy para sus usuarios, sería impensable la vida sin el mismo. Con Internet hacemos muchas actividades cotidianas, estudiar, trabajar, realizar compras, quedar con nuestros amigos o incluso buscar pareja. Las ventajas y utilidades que nos proporciona son innumerables, no podemos dudarlo, pero la facilidad con la que se accede al mismo, su uso a edades cada vez más tempranas, la rapidez con la que se difunde la información, y el escaso control que tenemos de nuestros datos, entre otros factores, hacen que Internet se configure como un marco idóneo para la lesión de nuestros derechos*"[2].

En este sentido, somos conscientes de que el internet y las redes sociales han producido una revolución en nuestras vidas, generando una gran dependencia en el quehacer de la sociedad. De la noche a la mañana formamos parte de un nuevo mundo tecnológico y digital que nos demanda mayor cuidado y atención en el manejo de nuestra información personal.

1. MALINOWSKI, Bronislaw. "*A scientific theory of culture and other essays*". California: The University of North Carolina Press, 1944.
2. ESCRIBANO TORTAJADA, Patricia. "*Algunas cuestiones sobre la problemática jurídica del derecho a la intimidad, al honor y a la propia imagen en internet y en las redes sociales".* En: FAYOS GARDÓ, Antonio y CONDE COLMENERO, Pilar (Coordinadores.). *Los derechos a la intimidad y a la privacidad en el Siglo XXI*. Madrid: 2014, Dykinson, p. 61.

Así, pues, las redes sociales constituyen "*servicios prestados a través de internet que permiten a los usuarios generar un perfil público, en el que plasman datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado*"[3].

La fácil accesibilidad para ser parte de ellas y, sobre todo, porque en su mayoría, son servicios gratuitos o, al menos, no hay una retribución económica por parte de los usuarios, hace pensar que los mismos están para brindar entretenimiento. Sin embargo, la real finalidad y ganancia del proveedor de servicios es la información que entregamos, ya que la misma tiene un valor en el mercado.

Como se puede apreciar, por la naturaleza misma que poseen las redes sociales, estas pueden llegar a tener una estrecha relación con los aspectos íntimos de la persona respecto de los cuales esta última quiera guardar cierto grado de privacidad.

En el ámbito nacional, a fin de resguardar nuestros derechos fundamentales a la privacidad e intimidad, la actual Constitución Política del Perú recoge en su artículo 2 numeral 6 que "*toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren aquella información que afecte la intimidad personal y familiar*".

Al respecto, podemos denotar que el citado artículo hace referencia únicamente al derecho que tiene toda persona de impedir el suministro de información:

> "*(…) omitiendo así componentes esenciales de este derecho, reconocidos en otras normas constitucionales o legales comparadas, como el poder acceder a la información personal contenida en los registros o bases de datos, conocer su contenido, tener la facultad de corregirla o actualizarla, o de hacer suprimir la información personal*"[4].

Es en dicho contexto que, frente a la carencia de una adecuada normativa de parte de nuestra Constitución en cuanto a la protección del citado derecho, que —*dentro de un contexto de "desarrollo tecnológico que se tradujo en la aparición y desarrollo de sistemas informáticos capaces de procesar, relacionar y transmitir información —libremente—*"[5]— se publica en el año 2011 la Ley 29733, Ley de Protección de Datos Personales —en adelante, "LPDP"— y su respectivo Reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales, el cual fue publicado el 22 de marzo de 2013 —en adelante, "el Reglamento"— y demás modificatorias. Dichos textos normativos buscan otorgar una protección más amplia del derecho a la privacidad dando cabida al derecho de la autodeterminación de la información de toda persona natural.

En este sentido, la LPDP amplía la protección de los datos personales, a fin de garantizar una serie de derechos a las personas titulares de estos, tales como el derecho a ser informado de cuándo y por qué se tratan sus datos personales, el derecho a acceder a ellos, el derecho a la rectificación o cancelación de los datos, o el derecho a la oposición al tratamiento de los mismos.

La contracara de este marco normativo constituye la consagración de diversos deberes, obligaciones, cargas y responsabilidades para las entidades públicas y privadas, los cuales tienen como finalidad asegurar que estas se sujeten al nuevo escenario de protección del

3. *Ibid.*, p. 69.

4. EGUIGUREN PRAELI, Francisco José. "*El derecho a la protección de los datos personales. Algunos temas relevantes de su protección en el Perú*". En: Themis N° 67. Lima: 2015, p. 132.

5. CASTRO CRUZATT, Karin. *"El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú".* En: Ius et veritas N° 37. Lima: 2008, p. 260.

derecho a la autodeterminación de la información personal relacionada con la privacidad e intimidad personal.

Esta materia ha sido objeto de discusión en diversos países. En el caso de la Unión Europea, recientemente, el 25 de mayo de 2018, ha entrado en vigencia el Reglamento 2016/679 del Parlamento y del Consejo, Reglamento Europeo de Datos Personales, como bien sabemos, el Derecho tiene que cambiar y estar en sintonía con la realidad, razones que parecen haber impulsado a la Unión Europea a realizar dicho cambio. En efecto, los avances tecnológicos y la globalización "*requieren de un marco más sólido y coherente para la protección de datos de la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior*"[6]. En este orden de ideas, se dictó el señalado Reglamento con el fin de proteger a los datos personales de las personas físicas y eliminar cualquier obstáculo de circulación de datos personales, así como para homogenizar el tratamiento de aplicación de dichas normas en todos los países de la Unión Europea.

II. ÁMBITO DE APLICACIÓN DE LA NORMATIVA

La LPDP es de aplicación cuando nos encontremos ante datos personales, incluyendo datos sensibles; se encuentren contenidos o destinados a ser contenidos en Bancos de Datos Personales, automatizados o no, independientemente del soporte, administrados por entidades públicas o privadas, cuyo tratamiento se realice dentro del territorio nacional —artículo 3—.

De acuerdo con el artículo 4 del Reglamento, no aplica la LPDP a los Datos Personales contenidos o destinados a ser contenidos en Bancos de Datos Personales creados por personas naturales para fines domésticos, personales o en el ámbito familiar. Tampoco aplica a los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito.

Asimismo, el Reglamento señala que el tratamiento se deberá efectuar en algunos de los siguientes escenarios: (i) en un establecimiento ubicado en territorio peruano correspondiente al titular del Banco de Datos Personales o de quien resulte responsable del tratamiento; (ii) sea efectuado por un encargado del tratamiento, con independencia de su ubicación, a nombre de un titular del banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento; (iii) el titular del Banco de Datos Personales o quien resulte responsable del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional; y (iv) el titular del Banco de Datos Personales o quien resulte responsable no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento —artículo 5—.

Cabe señalar que la Dirección de Datos Personales en la absolución a una consulta con Oficio N° 625-2015-JUS/DGPDP ha sugerido cuáles serían los medios que se utilizan únicamente con fines de tránsito de circulación de la información —y que, por ende, no impliquen un tratamiento de datos personales—. Así, pues, se refiere el Oficio en mención a las: "*redes de telecomunicaciones —ejes, centrales, cables— que forman parte del soporte de la plataforma de Internet, y por las cuales pasan los contenidos desde el punto de expedición hasta el punto de destino y que pueda incluir el paso por las instalaciones de un país que*

6. Considerando (7) del Reglamento Europeo de Datos Personales. 2016.

no es el del envío ni el del destino"[7]. Como se puede advertir, la norma se refiere sólo a supuestos de circulación temporal de la información sin el objeto de efectuar un tratamiento, entendiendo por tratamiento todas las acciones establecidas en la LPDP y su Reglamento.

III. AUTORIDAD COMPETENTE

La autoridad encargada es la Dirección de Datos Personales —en adelante, "la Autoridad"— que forma parte de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que depende jerárquicamente del Despacho Viceministerial de Justicia.

IV. EL TIPO DE INFORMACIÓN PROTEGIDA

Resulta de suma importancia, entonces, entender cuáles son los datos protegidos por la normativa peruana y definirlos adecuadamente. Al respecto, la LPDP define a los datos personales como toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados —artículo 2.4—. Complementando dicho concepto, el Reglamento señala que constituyen datos personales, aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales —artículo 2.4—.

De la misma forma, conceptualiza los datos sensibles como aquellos datos personales constituidos por lo datos biométricos que por sí mismo pueden identificar a un titular. Esto es, datos referidos al origen racial y étnico, a los ingresos económicos, a las opiniones o convicciones políticas, religiosas, filosóficas o morales, a la afiliación sindical y a la información relacionada con la salud y la vida sexual —artículo 2.5—. En dicho contexto, las historias clínicas y sus exámenes de laboratorio, califican como datos sensibles para un paciente.

Como se puede advertir, la normativa peruana asume una noción amplia del concepto de datos personales. Es decir, considera como "dato personal" cualquier tipo de información que permita relacionar o identificar a una persona. Ello incluye información que —individualmente— podría no considerarse personal, pero que enlazada o analizada con otra, sí permitiría la identificación de una persona, como lo hace el *Big Data* —más adelante desarrollaremos lo que es *Big Data*, sus funciones, y los retos que esta conlleva para la normativa de protección de datos personales—.

Asimismo, tenemos en la definición de dato personal aquella información que identifique a la persona, ello quiere decir que directamente se pueda saber de quién se está hablando, por ejemplo, sabiendo el Documento Nacional de Identidad de una persona podemos reconocerla. Sin perjuicio de ello, existe aquella información que puede hacer identificable a una persona, así por ejemplo tenemos el IP —*Internet Protocol*—, las *cookies*, entre otros elementos.

A modo de ejemplo tomaremos el caso del IP, el cual es un número único que usan los dispositivos digitales —computadoras, *laptops, tablets, smartphones*— para poder ser identificados, resultando casi como una dirección física. Así, pues, cuando utilizamos estos dispositivos conectados al Internet, se transmiten paquetes pequeños de información, cada uno de los cuales contiene una dirección IP del emisor y del destinatario, lo cual hace identificable la procedencia o el origen de la información. Por otro lado, los servidores de nombres de dominio DNS, traducen el nombre de dominio en una dirección IP. Ciertas herramientas existentes en la red permiten encontrar el vínculo entre el nombre de dominio y el usuario.

En este sentido, de un correo electrónico que recibamos, podemos extraer, entre otras cosas y a los efectos que aquí nos interesan, la dirección IP

7. DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES. Oficio N° 625-2015-JUS/DGPDP. Disponible en: <https://www.minjus.gob.pe/wpcontent/uploads/2016/01/OF_625_F.pdf>

del dispositivo desde el cual se remite. También aparecen otros datos identificativos —como el remitente y su correo— que, asociados a la IP, pueden convertir esta información —a través de relacionar información diversa— en un dato de carácter personal. Si bien la utilización de la IP como identificadora del origen del correo puede considerarse normal, los posteriores usos que se hagan de la misma una vez asociada a un dato personal pueden no serlo.

Bajo este escenario y como señala Chaveli:

> "*(…) lo habitual es que el registro de la dirección IP sirva para fines "normales" como son las estadísticas de acceso a determinados sitios y no para otros que plantean mayores problemas en materia de protección de datos, como pueda ser deducir "hábitos" de navegación. Pero no siempre es así. Ello nos obliga a abordar la posible conceptuación de la IP como dato de carácter personal*"[8].

Al respecto, Eduard Chaveli advierte que: "*la dirección IP en sí misma, sin que pueda asociarse a otra información, no constituye un dato de carácter personal*". Sin embargo, sí lo será desde el momento en que el usuario haya comunicado determinada información y sea posible, a partir de entonces, relacionar su dirección IP con el mismo. A mayor abundamiento, los administradores de redes, teniendo el IP, pueden utilizar medios razonables e identificar a los usuarios en internet a partir de la información y datos ahí vertidos.

Si revisamos la legislación española, podremos advertir que su Ley de Protección de Datos no contempla expresamente la dirección IP como dato personal. Sin embargo, la Agencia Española de Protección de Datos ha establecido mediante Informe 327/2003 que las direcciones IP, tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal, resultándole de aplicación las normas sobre protección de datos. Asimismo, el Grupo de Trabajo del Artículo 29, un órgano consultivo independiente integrado por un representante de la autoridad de protección de datos de cada estado miembro de la Unión Europea, el Supervisor Europeo de Protección de Datos y la Comisión Europea —si bien es un órgano consultivo y sus pronunciamientos no son vinculantes, es bastante citado por los tribunales— también lo ha señalado en varias ocasiones, como, por ejemplo, en el Dictamen 4/2007 que versa sobre el concepto de datos personales —puede consultarse en especial la página 18—.

En similar sentido se ha pronunciado recientemente la *Cour de Cassation* francesa en un caso bastante sonado. El caso versa sobre tres empresas que forman parte de un mismo Grupo —esto es, Grupo *Logisneuf*— que detectaron que —desde el interior de su red— había personas que se conectaban a la internet a través de computadores ajenos a los del Grupo *Logisneuf* sin siquiera usar los códigos de acceso reservados a los administradores del sitio web *logisneuf.com*. Frente a dicho panorama, estas empresas obtuvieron de un "juez de medidas de urgencia" —*juge de referés*— una orden a efecto de que las diversas empresas proveedoras de Internet comuniquen a *Logisneuf* la identidad de las personas titulares de las direcciones IP que se usaron para la conexión. Ante esta situación —y cabe mencionar que las IP's que se pedían analizar e identificar eran de la empresa de la competencia— el juez no vaciló en considerar que:

> "*(…) las IP —al permitir la identificación indirecta de una persona natural— son datos de carácter personal por lo que su recolección constituye un tratamiento de datos de carácter personal en el cual debe mediar una declaración previa de los mismos —a efectos de que se les pueda tutelar— ante*

8. CHAVELI DONET, Eduard Antoni. "*La protección de datos personales en Internet*". En Azpilcueta. Cuadernos de Derecho N° 20. Donostia: p. 85.

la Comisión Nacional de Informática y de Libertades —CNIL—"[9].

Es de esta forma como en Francia se puso fin al debate en torno a si las IP's constituían o no datos personales.

Al respecto, cabe precisar que nuestra legislación no lo establece de manera expresa, ni tampoco existen pronunciamientos de la Autoridad sobre ello. Por lo pronto en el Perú, se deberá analizar caso por caso las diferentes situaciones aplicando la definición de dato personal que como —hemos señalado líneas arriba— constituye una lista abierta, toda vez que en tanto el IP pueda ser enlazado a una persona en particular calificará como dato personal.

Por ejemplo, piénsese en el caso de un centro de labores en el cual a cada trabajador se le asigna una computadora que solamente este utiliza. En dicho caso, es fácilmente identificable el usuario que está detrás de este IP. Sin embargo, pensemos ahora en el caso de un *ciber café* o local público donde se ofrece a los clientes acceso a internet. Como todos sabemos, no se pide identificación a los clientes y no es que cada uno de estos se encuentre vinculado a una máquina en concreto por lo que el IP difícilmente podría relacionarse a un usuario en particular. Bajo dicho supuesto la IP no constituiría un dato personal.

Por último, es relevante señalar que los datos personales pueden estar o no organizados en un banco de datos personales y que esta organización sea automatizada o no. Por ejemplo, un archivo con distintos files físicos en el mismo establecimiento califica como un banco de datos personales. Del mismo modo, la planilla electrónica de trabajadores en una empresa también califica como base de datos personales.

Respecto a la información sistematizada en bases de datos, usualmente archivos de tipo texto mostrados en filas y columnas, son fácilmente ordenados y organizados a través de herramientas de procesamiento de la información.

De otro lado, existen otros tipos de datos como los no estructurados o semiestructurados, los cuales representan la mayor parte de la información generada y almacenada diariamente. Los datos semiestructurados son aquellos que no provienen de bases de datos relacionales pero tienen una organización interna que ayuda a su tratamiento. Ejemplo: hojas de cálculo, HTML —lenguaje de elaboración de las páginas web—, etc.

Los datos no estructurados carecen de estructura interna que sea identificable o de fácil organización. En otras palabras, es un conglomerado masivo y desorganizado de datos que no tienen mayor valor hasta que son procesados y correlacionados entre sí o con otras variables que faciliten su visualización y manejo. Por ejemplo: correos electrónicos, videos, documentos PDF o de texto, etc. La información no estructurada contenida dentro de un correo electrónico también puede calificar como dato personal o dato sensible, siempre y cuando las relaciones o correlaciones con otros datos y/o variables vulneren los procesos de anonimización y hagan identificable al individuo.

Por tanto, no debe dejar de remarcarse que, encontrándonos ante una definición abierta de datos personales, la lista de aquellos datos que califican como personales irá incrementándose a medida que la sociedad y la tecnología evolucionen.

V. ROL DEL CONSENTIMIENTO DENTRO DE AQUELLO QUE CALIFICA COMO DATOS PERSONALES

El consentimiento es un concepto clave de la protección de datos personales. Constituye un

9. COUR DE CASSATION. Chambre Commerciale, 15 octobre 2013. N° Pourvoi 12-21704. Disponible en: <https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028095230&fastReqId=48856858&fastPos=1>

mecanismo que le otorga al usuario autonomía a fin de decidir sobre la utilización o no de sus datos personales por terceros. Cabe precisar que el consentimiento es necesario cuando los datos personales no puedan anonimizarse o desasociarse.

Así, pues, si nos detenemos por un momento a pensar en cuánta información personal entregamos, por ejemplo, al momento de ingresar a una página web, al comprar *online*, al registrarnos en una nueva red social, al participar de un sorteo publicitado en redes sociales o —simplemente y llanamente— al navegar por internet, quizás nos sorprendamos de su magnitud y empecemos a reflexionar sobre el trato que recibe nuestra información, sobre quién se beneficia con ella y si se cumple lo establecido en la normativa de protección de datos personales.

En nuestra opinión, el usuario del servicio de internet queda expuesto a la recolección de sus datos en todo momento, sea mediante la información que el propio usuario entrega, como, por ejemplo, a través de formularios de compra o al crear un usuario, o a través de otros mecanismos u otras herramientas insertadas por los propietarios del sitio web que se visita o aquellas incluidas en dicho sitio por terceros, como son las denominadas *cookies*. No obstante, son los administradores de los sitios web quienes deberían resguardar los datos entregados por los usuarios y sólo se debería efectuar el traslado de dicha información a terceros si es que hubiere mediado un consentimiento previo por parte del usuario.

Sin embargo, en este punto surge la interrogante de si, en efecto, los administradores de las redes sociales guardan de manera segura la información personal de sus usuarios. No se olvide que los usuarios no pueden tener la certeza de que esto realmente se dé, toda vez que el manejo de dicha información la tiene quien administra la red.

Y lo que es más grave aún, es que los usuarios desconocen que —en muchas ocasiones— a través de ciertas herramientas se están recolectando sus datos personales. A nadie es ajeno que cuando uno se encuentra navegando en internet aparecen repentinamente ventanas solicitando consentimientos o que te re-direccionan a otras ventanas —las cuales la mayoría de las veces son desechadas o ignoradas por los usuarios—; empero que en muchos casos dada la premura o necesidad del usuario de acceder a una determinada información termina autorizando la recolección de su información personal sin saber el verdadero impacto de ello.

Con relación al uso de datos por plataformas o red sociales a las que usuarios —como nosotros— utilizamos a diario, llama la atención el caso *Cambridge Analytica,* una compañía privada que combinó la minería de datos y el análisis de datos con la comunicación estratégica para el proceso electoral de Donald Trump, actual presidente de los Estados Unidos de América; y los datos utilizados provinieron de nada menos que la red social *Facebook*.

En el año 2014, la empresa norteamericana *Cambridge Analytica*, una firma de analítica de datos políticos del Reino Unido, por medio de su aplicación "*thisisyourdigitallife*" habría obtenido el consentimiento de miles de usuarios de *Facebook* para el uso de sus datos con fines netamente académicos. Ello no conllevaría ningún acto ilícito sino fuera porque de manera posterior se descubrió que dicha firma de datos usó la información de aproximadamente 87 millones de usuarios de *Facebook* para fines distintos a los autorizados por el usuario. En concreto, *Cambridge Analytica* utilizó información proveniente de dichos usuarios para crear publicidad e influenciar a dichos usuarios para votar por un determinado candidato, en el marco de campañas electorales. La información entregada por los usuarios fue suficiente para que *Cambridge Analytica* creara avisos que puedan persuadir a una persona en su elección por un candidato.

Comercialmente, significa que el proveedor de servicios cuenta con herramientas importantes para agrupar, segmentar el mercado, dividiendo a las audiencias publicitarias en grupos, para que, posteriormente, se les dirijan anuncios a través de diversas plataformas.

Bajo este escenario, se pone de manifiesto una relación de desigualdad entre el usuario y quien administra determinada plataforma o red social encargada de la recolección de los datos. En efecto, este avance tecnológico pone al usuario en situación de asimetría frente a ciertos agentes que realizan la recolección de datos, en donde cierta información personal podría ser usada de manera ilegal, como en el ejemplo anteriormente dado, como también de manera legal, sin que las personas estén conscientes de ello. El objetivo debiera ser buscar un equilibrio entre la libre circulación de datos y la protección de la intimidad personal por parte de quienes realizan el tratamiento de los datos personales. Ello informando al usuario de manera clara, sencilla y concisa; optando por altos niveles de seguridad de los datos, e implementando los mecanismos de los que ya goza el usuario para tomar decisiones respecto de sus datos. Por ejemplo, la Autoridad ha reconocido en el Perú el famoso derecho al olvido, que faculta al usuario a pedir el borrado de sus datos bajo ciertos escenarios. En el Perú, los aspectos de este mediático caso pueden seguirse a través de la lectura de la Resolución Directoral N° 045-2015-JUS/DGPDP de la Dirección General de Protección de Datos Personales —que resolvió la reclamación— y de la Resolución Directoral N° 026-2016-JUS/DGPDP de la Dirección General de Protección de Datos Personales —que resolvió el recurso de reconsideración—.

Entonces, en el siguiente punto analizaremos cómo las redes sociales debieran cumplir con el requerimiento de obtener el consentimiento de manera previa, expresa, inequívoca e informada de los usuarios y, cuáles son las consecuencias de transferir datos personales sin el consentimiento de su titular.

VI. CARACTERÍSTICAS DEL CONSENTIMIENTO Y MODO DE OBTENCIÓN

En lo que se refiere a la protección de los datos de la persona, el artículo 7 del Reglamento ha establecido que:

> "(…) *el tratamiento de datos personales es lícito, cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de manera directa, como aquellas en las que se requiere presumir o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones deberá manifestarse en forma expresa y clara*".

Cuando navegamos en internet y es necesario obtener el consentimiento del titular de los datos, el artículo 12 del Reglamento señala que:

> "*(…) también se considera expresa la manifestación consistente en 'hacer click', 'cliquear' o 'pinchar', 'dar un toque', 'touch' o 'pad' u otros similares. En este contexto el consentimiento escrito puede otorgarse mediante firma electrónica, mediante escritura que quede grabada y pueda ser impresa, o por cualquier otro mecanismo que permita identificar al titular y recabar su consentimiento a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácil de leer y entender, para que el titular pueda hacer suyo, o no, el texto, mediante un 'click' o cualquiera de las otras formas establecidas en el párrafo anterior. El condicionamiento de la prestación de un servicio, o la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido, sí afecta la libertad de quien otorga consentimiento para el tratamiento de sus datos personales, si los datos solicitados no son indispensables para la prestación de los beneficios o servicios (…)*".

En razón a que la normativa de Protección de Datos Personales exige que el consentimiento del uso de los datos personales se otorgue de manera libre con la opción de poder no aceptar el tratamiento y continuar —sin ningún tipo de restricciones— con el servicio y, asimismo, teniendo presente que el consentimiento debe ser expreso es que se recomienda implementar dos "*click box*", uno para los términos de uso general de la aplicación y otro que demuestre la aceptación a las políticas de protección de datos personales.

No debe dejar de remarcarse que, en muchos servicios de redes sociales, se condiciona su uso a la aceptación de los términos o políticas de privacidad, las cuales añaden otros fines alternos como el uso de los datos para publicidad o transferencia de datos a terceras personas, las cuales no son necesarias ni indispensables para brindar el servicio. Estos proveedores no brindan alternativas u opciones para poder escoger los usos finales para los cuales una persona sí proporciona su consentimiento. Así, pues o se aceptan todas las condiciones o se rechazan en su conjunto. Para la mayoría de las empresas de *software* o aplicaciones, el rechazar su política de privacidad trae como consecuencia el no poder utilizar sus servicios.

Otra falta recurrente de las redes sociales consiste en la publicación de enunciados generales para cuando hay cambios en las políticas de protección de datos personales, señalando que a partir de que son colgadas en la web —luego de un determinado plazo— se entenderán como conocidas por los usuarios y, asimismo, que el simple hecho de seguir navegando implica que el usuario declara que las conoce y acepta. Sin lugar a dudas, dicho enunciado es contrario a la normativa, tanto en lo que refiere a la libertad del otorgamiento del consentimiento como al hecho que el mismo debe ser expreso e inequívoco.

Es menester tener presente que si bien se otorgó el consentimiento en un primer momento —esto es, al momento de iniciar contacto con la plataforma o la aplicación— ello no nos puede llevar a asumir que al volver a navegar en la aplicación o utilizar la plataforma, el usuario está brindando el consentimiento a los cambios efectuados de manera unilateral en dichas políticas, así tampoco el hecho que si el usuario no está de acuerdo, deberá optar por no seguir haciendo uso de la aplicación.

Por ejemplo, si uno de estos cambios consistiese en el uso para fines alternos de los datos personales recolectados, en dicho caso, la norma es clara en señalar que el consentimiento debe ser previo, así el numeral 2 del artículo 12 del Reglamento establece que: "*la recopilación debe ser con anterioridad a la recopilación de los datos o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron*".

El consentimiento debe ser expreso e inequívoco, es decir, sin posibilidad de duda o equivocación que el usuario manifestó su autorización. Es cuestionable que un comportamiento pasivo como el seguir utilizando el servicio, se interprete como consentimiento inequívoco. Es importante que la aplicación muestre las respectivas advertencias ante cambios unilaterales de las políticas de privacidad y protección de datos personales, mediante "*pop up*" o ventanas emergentes mostradas al usuario informando sobre los cambios, para que así se pueda obtener el consentimiento para el nuevo tratamiento. Asimismo, se deberá mencionar las repercusiones de no aceptar los cambios propuestos.

Es menester evocar el procedimiento administrativo sancionador seguido contra el Sistema de Administración Hospitalaria S.A.C. —en adelante, "SANNA"— en el cual se constató que dentro del enlace web "Términos y Condiciones" de este Centro de Salud, existían fórmulas que hacían presumir el otorgamiento del consentimiento. Este caso es paradigmático pues en él se ponen en evidencia las características del consentimiento:

> "*(…) el consentimiento requerido (…) no es libre, en la medida que no se daba al titular del dato personal la oportunidad de manifestar su consentimiento y menos denegarlo (…) que el consentimiento sea previo (…) significa que este debe ser otorgado con anterioridad a la recopilación de los datos personales o en su caso, con anterioridad al tratamiento distinto a aquel por el cual ya se recopilaron, lo que en el presente caso no ocurre pues la recopilación se daba con la sola navegación en la web (…). Una tercera característica del consentimiento es que éste debe ser expreso e inequívoco (…) no se verifica ninguna manifestación de voluntad del titular del dato personal*

toda vez que SANNA, presumía el consentimiento (…)"[10].

En el caso de información que esté en redes sociales, subida por el propio usuario, no basta con que la información sea pública para poder tratarla; se deben seguir los principios de consentimiento y finalidad. Así en el Oficio N° 569-2014-JUS/DGPDP de la Dirección General de Protección de Datos Personales se ha señalado que:

"*(…) los términos y condiciones de uso y políticas de privacidad y confidencialidad de la información de la red social Facebook indican que si un tercero recopila información de usuarios, deberá obtener un consentimiento previo, identificarse y publicar una política de privacidad que explique qué datos recopilará y cómo los usará. En ese sentido, la propia red social reconoce la aplicación de los principios de consentimiento y finalidad para el tratamiento de los datos personales.*

(…)

Asimismo, los términos y condiciones de uso y políticas de privacidad y confidencialidad de la información de la red social indican que si el usuario publica contenido o información con la configuración "público", que permite que todos, incluidas las personas que son ajenas a la red social, accedan y usen dicha información y la asocien a su persona —es decir, nombre y foto del perfil—. No obstante ello, debe recordarse que la información cuya configuración es pública en la red social, continúa perteneciendo a la esfera de la privacidad del usuario, conforme con lo señalado en los numerales 4 y 5 del artículo 2 de la LPDP y numerales 4 y 6 del artículo 2 del Reglamento, por lo que su tratamiento debe hacerse de acuerdo con la legislación de la materia, más allá de que el acceso esté autorizado"[11].

Finalmente, es posible obtener el consentimiento del usuario a través de correos electrónicos cuando este se requiera por primera vez, informando de manera explícita y clara los datos personales que se tienen almacenados, la finalidad de los mismos y el tratamiento que les dará la empresa. Así, por ejemplo, la Autoridad de protección de datos personales ha señalado en la absolución de una consulta que:

"*(…) la necesidad de consentimiento previo no significa la prohibición absoluta de contacto, puesto que de lo contrario no será posible obtener el consentimiento. La autoridad considera que puede hacerse contacto siempre y cuando el contenido de las comunicaciones constituya para el consumidor, receptor o usuario solamente el mecanismo de información y obtención de la autorización y sí y solo sí tales comunicaciones se hacen en formas y horarios razonables; lo cual quiere decir que: a) se comunican para obtener consentimiento informado, previo y libre, no para el asunto comercial o de interés del emisor, b) se usan horarios razonables y días útiles, y c) se evita la insistencia o la reiterancia de comunicaciones a quienes ya expresaron su negativa*"[12].

Por tanto, las empresas prestadoras de servicios a través de internet o administradoras de "*apps*" deben implementar todas las herramientas necesarias para obtener el consentimiento del usuario con todas las características aquí desarrolladas. Asimismo, no olvidar que para

10. DIRECCIÓN DE SANCIONES DE LA DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES. *Resolución N° 101-2015-JUS/DGPDP-DS*. Disponible en: <https://www.minjus.gob.pe/wpcontent/uploads/2016/02/RD-1ra.-Instancia-consentida-Sanna.pdf>.

11. DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES. *Oficio N° 569-2014-JUS/DGPDP*. Disponible en: <https://www.minjus.gob.pe/wpcontent/uploads/2015/06/Resoluciones_126.pdf>.

12. MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS. *Documento con Registro 53701*. Disponible en: <https://www.minjus.gob.pe/wp-content/uploads/2015/04/4.pdf>.

demostrar la obtención del consentimiento, la carga de la prueba recaerá siempre en el titular del banco de datos o quien resulte responsable del tratamiento; ello en virtud del artículo 15 del Reglamento.

VII. CONTENIDO DEL CONSENTIMIENTO Y SU RECOLECCIÓN

En el consentimiento se debe establecer de manera expresa cual es la empresa que recopila los datos, su denominación o razón social, Registro Único de Contribuyente —RUC—, dirección y a título de qué recolecta los datos, es decir, si es titular de la BDP o es un encargado del tratamiento de datos personales quién presta servicios para el titular de la BDP.

Cuando se solicite el consentimiento para una forma de tratamiento que incluya la transferencia nacional o internacional de los datos, el titular de los mismos deberá ser informado de forma expresa e inequívoca a quién o quiénes serán transferidos dichos datos y la finalidad para la cual recibirá los mismos. Cabe señalar que, la Autoridad ya ha sancionado a diversas empresas por no detallar de manera expresa la denominación o razón social completa de quien recibe los datos personales; es decir, no basta con señalar que los datos serán transferidos a terceras personas o prestadoras de servicios o empresas del grupo.

Por ejemplo, con relación al tópico de la transferencia de datos personales entre empresas de un mismo grupo se formuló una muy interesante consulta en sede nacional. Así, pues, la Autoridad debía resolver la pregunta de si era necesario o no el consentimiento del titular de los datos personales cuando se otorgaba el consentimiento a una empresa de un determinado grupo para una determinada relación contractual, empero, al interior de dicho grupo esta información circulaba entre empresas. Al respecto, la Autoridad señaló que:

> "*(…) resulta importante tener en cuenta que el tratamiento de datos personales al interior de un grupo empresarial no faculta ni legitima que las empresas del grupo compartan deliberadamente dicha información por el solo hecho de que formen parte del grupo, y sin que dicha transferencia de datos haya sido autorizada por el titular de los mismos, mediante su consentimiento en los términos exigidos por la LPDP y su Reglamento (…)*"[13].

De otro lado y en relación a la transferencia de los datos, tenemos el *cloud computing*, que de acuerdo a la definición suministrada por el *National Institute Of Standards and Technology* —NIST— constituye *"un modelo para permitir el conveniente acceso a la red bajo demanda y a un conjunto de recursos compartidos de computación configurable —por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios— que pueden ser rápidamente suministrados y liberados con un mínimo esfuerzo de gestión o interacción del proveedor de servicios"*, se puede tener acceso a la información mediante una conexión a Internet desde cualquier dispositivo móvil o fijo ubicado en cualquier lugar geográfico y que se accede a través de redes.

El artículo 33 del Reglamento regula el tratamiento de datos personales por medios tecnológicos tercerizados, el cual es aplicable cuando el tratamiento se terceriza de acuerdo con los servicios como *cloud computing*.

Así, pues la Dirección General de Protección de Datos Personales, según el Oficio N° 213-2015-JUS/DGPDP ha señalado que el *cloud computing* puede clasificarse en:

> "*(i) Pública, cuando quien requiere el servicio de computación en la nube o cloud computing tiene una relación contractual con el prestador del servicio, quien a su vez le proporcionará los recursos necesarios para gestionar y administrar su información en la nube.*

13. DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES. *Oficio N° 575-2015-JUS/DGPDP*. Disponible en: <https://www.minjus.gob.pe/wp-content/uploads/2015/12/575-II.pdf>

(ii) Privada, cuando la propia entidad controla, gestiona y administra sus servicios mediante computación en la nube o cloud computing para los conglomerados que la conforman, sin que en la misma participen entidades externas. En este caso, puedes contratarse un tercero que actuará bajo la supervisión de la entidad en función de sus necesidades"[14].

Empresas como *Microsoft, Google, Amazon* y otros brindan servicios de *cloud computing*. Ello implica que los datos se transfieren en un abrir y cerrar de ojos, y pasan a terceras manos sin siquiera saberlo, siendo ello poco transparente para los usuarios. Esto genera una pérdida del control para los usuarios de sus datos personales; más aún cuando no siempre se les informa quiénes realmente reciben dicha información y dónde están alojados físicamente.

De otro lado, tenemos el *Big Data*, pues su valor reside en la recolección de información de manera masiva y constante, la cual no necesariamente tiene que ser utilizada en el momento de la recolección, sino que puede ser utilizada en el futuro —a través de una distinta combinación de datos— puede dársele nuevos usos a dicha información. Así, tal y como ha señalado Gil:

"*(…) es precisamente en estos usos secundarios donde reside el potencial del Big Data. Esta forma de concebir el consentimiento obligaría a que cada vez que se descubra un nuevo uso para los datos, el responsable debería volver a pedir el consentimiento a cada uno de los individuos cuyos datos están siendo tratados por segunda vez. Esto, en muchas ocasiones, podrá ser técnicamente inviable, por no decir que las empresas no podrían asumir los costes*"[15].

Esto claramente atenta contra la obligación de informar las finalidades para las cuales se recolectan estos datos, pero también en caso estos datos lleguen a manos de terceros atentaría en contra de la obligación de informar al usuario a qué terceros se les transfiere su data. Es decir, no sólo se vulneraría la voluntad del titular de los datos personales respecto a los fines para los cuales ha brindado su consentimiento, sino que de existir flujo transfronterizo de sus datos, el titular no sabrá a quiénes son transferidos, quienes se benefician de los mismos, que usos le dan a los mismos, entre otros.

Finalmente, en el consentimiento se deberá señalar el medio por el cual el titular de los datos personales podrá hacer efectivo sus derechos de acceso, rectificación, cancelación y oposición. Se deberá consignar alguno de los siguientes datos: correo electrónico, dirección o teléfono, a través del cual se puedan encausar las solicitudes del titular de datos personales.

VIII. EL *BIG DATA*

El término *Big Data* fue utilizado por primera vez por los científicos de la NASA en 1997 para describir el problema de visualización de gráficos virtuales y otros sets de datos debido a su gran tamaño. La magnitud de tal información incluso requería de mayores recursos logísticos, como memorias locales y remotas o mejores procesadores[16].

Herramientas como el internet facilitan enormemente la obtención y transferencia de cantidades enormes de información, para ser analizada por computadores y programas automatizados y que, además, tiene un flujo constante y permanente, es decir se crean en todo momento y sobre todas las cosas.

14. DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES. *Oficio N° 213-2015-JUS/DGPDP.* Disponible en: <https://www.minjus.gob.pe/wp-content/uploads/2015/06/item1.pdf>

15. GIL, Elena. "*Big Data, Privacidad y Protección de Datos".* Madrid: Agencia Española de Protección de Datos, 2016, p. 67.

16. Cox Michael y Ellsworth David. *"Application-controlled demand paging for out-of-core visualization".* Disponible en: <https://www.nas.nasa.gov/assets/pdf/techreports/1997/nas-97-010.pdf>

El Grupo de Trabajo del Artículo 29 en la *Opinion 03/2013 on Purpose Limitation* cataloga al *Big Data* como: *"gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos"*[17].

Bill Schmarzo, nos da luces de los grandes aportes del *Big Data* para el mundo empresarial y económico, argumentado que:

> "*(…) la clave de los Big Data no está en igualarse a los demás, de implementar las mismas tecnologías para ser como el resto, sino en aprovechar los conocimientos únicos que se obtienen sobre los clientes, productos y operaciones y aplicarlos para reestructurar el proceso de creación de valor, optimizar las principales iniciativas empresariales y descubrir nuevas posibilidades de monetización*"[18].

Un ejemplo de cómo las empresas pueden utilizar el *Big Data* para generar valor y beneficios a los usuarios es, por ejemplo, *Waze Inc*. Como todos bien sabemos, "*Waze*" es una aplicación gratuita, social y colaborativa de navegación por GPS, que funciona en tiempo real a través de aparatos móviles como *tablets* y *smartphones*.

La información recogida por el *software* de *Waze* es amplia y en tiempo real, proporcionada por los usuarios de la aplicación al momento de usarla. Puede recabar información tan variada como: nombres de usuarios, todas las direcciones exactas de partida y llegada, así como datos de la ruta elegida por cada usuario en todos sus viajes utilizando el servicio o las direcciones guardadas como "casa" o "trabajo" en su plataforma. También recaba información sobre lugares, fechas y horas de accidentes en las rutas, desvíos por obras, policías en los caminos, velocidades de los vehículos, etc.

Este *Big Data* es utilizada por el *software* automatizado de la compañía para ofrecernos mejores alternativas de rutas con menor tráfico para llegar a donde queremos ir en el menor tiempo posible. Sin embargo, ello no significa que toda la información recogida sea destinada a ese motivo. *Waze* podría utilizar la información para muchos otros objetivos propios o ceder los datos a terceros —siempre y cuando cuente con los consentimientos adecuados—. Por ejemplo, la compañía puede "mapear" o visualizar con coordenadas GPS los lugares donde ocurren la mayor cantidad de accidentes vehiculares o determinar el promedio en horas al día que las personas manejan en cualquier ciudad o país. También puede ofrecer diversas herramientas de marketing a negocios locales determinando la cantidad de usuarios de la aplicación que transitan cerca a sus locales semanalmente y así tomar mejores decisiones en sus estrategias de venta.

Otro ejemplo es la Tarjeta *Bonus* del supermercado *Wong*, la cual es gratuita y en principio sirve para acumular puntos para que luego puedan ser canjeados por diversos productos; sin embargo, esa no es la única razón. Realmente es un programa de fidelización de clientes de la empresa Cencosud que recolecta enormes cantidades de información que son analizadas y utilizadas por la empresa a través de diversas herramientas para procesar *Big Data*.

Al pasar la tarjeta en cada compra, se recolecta diversa información, por ejemplo: ¿cuáles son sus gustos alimenticios?, ¿cuáles son los productos que más consume? ¿cuándo compra? ¿dónde compra? Esta información está vinculada a un cliente o usuario, pudiendo conocer sus hábitos y gustos, además de otros factores que determinan la elección de un producto —ubicación, precio, periodicidad, etc.—. Esto le permite a la empresa a diseñar estrategias de fidelización, de captación

17. GRUPO DE TRABAJO DEL ARTÍCULO 29. *Opinión 03/2013 on Purpose Limitation*. Disponible en: <http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2013/wp203_en.pdf>.

18. SCHMARZO, Bill. "*Big Data: Understanding How Data Powers Big Business*". Indianapolis: John Wiley & Sons Inc, 2013, p. 19.

de clientes, de generación de nuevos productos con marcas propias, entre otros.

Recientemente *Wong* ha lanzado una máquina dispensadora de cupones personalizados, mediante la cual cualquier cliente que cuente con tarjeta bonus, podrá ingresando su número de Documento Nacional de Identidad, recibir cupones de descuento. Lo curioso es que las ofertas no son iguales para todos, sino que están dirigidas según los intereses de consumo de cada cliente, compras históricas, hace cuanto tiempo que no compra un tipo de producto, etc.

Así podemos advertir que *Wong* utiliza algoritmos que buscan identificar patrones complejos en el *Big Data* de la empresa para efectuar segmentación avanzada de clientes, análisis de captación y retención, análisis de comportamiento de la cesta de la compra, sistemas de recomendación. Es decir, se pueden anticipar a las decisiones de compra del cliente —ventas, inventarios, nuevos productos—.

Asimismo, de la data recolectada y con las herramientas tecnológicas respectivas, pueden analizar la pérdida de clientes, abandono de compra de productos. La empresa puede saber a través de la data, a qué precio un cliente decide no comprar el producto, incluso a qué precio un producto líder deja de ser atractivo para el cliente y decide adquirir la competencia.

Como podemos apreciar, *Wong* ha entendido el valor que tiene la data y actualmente la utiliza para generar valor a su empresa. El equilibrio está en informar a los clientes sobre la data que se obtiene, su finalidad, así como recolectar de manera legal el consentimiento de los clientes para poder darle un uso adecuado a dicha data.

IX. PROBLEMAS DEL *BIG DATA* FRENTE A LA PROTECCIÓN DE DATOS PERSONALES

Nuestra legislación presenta serias limitaciones frente a los avances tecnológicos, como el procesamiento de *Big Data,* ya que se puede estar atentando contra la privacidad de las personas. El consentimiento con todas las características requeridas por ley es uno de esos límites. En efecto, el procesamiento de grandes cantidades de datos hace imposible prever todas las finalidades para las cuales se utilizarán dichos datos; o determinar quiénes se beneficiarán de los mismos, entre otros. Al respecto, nos recuerda Schmarzo que:

> "*Las empresas que están adoptando los Big Data como medio de transformación están pasando de una visión retrospectiva que utiliza fragmentos parciales de datos globales o muestreados para monitorizar los negocios a un enfoque operativo predictivo y previsor que saca partido de todos los datos disponibles —incluyendo los datos estructurados y sin estructurar que puede haber más allá de los muros de la empresa— (…)*"[19].

Un gran reto de nuestra sociedad es la de actualizar constante y oportunamente nuestra legislación para que acompañe a la innovación tecnológica y así mejorar las garantías que el Estado brinda sobre el derecho a la privacidad y a la protección de datos personales.

Nuevos reglamentos como el de la Unión Europea —Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y, por de abril de 2016, el que se deroga la Directiva 95/46/CE— dotan de mayor poder de control a los sujetos sobre sus datos personales, a través de medidas como: asegurar la transparencia en el manejo y el uso de la información, reforzando la importancia y la claridad del "consentimiento informado", estableciendo nuevos derechos individuales y cambiando las normas y las advertencias acerca de la creación de perfiles de personas o usuarios.

Dentro de dicho contexto, por ejemplo, no puede dejar de evocarse esfuerzos como el de la

19. *Íbid.*, p. 25.

Agencia Española de Protección de Datos —en adelante, "la AEPD"— la cual ha venido emitiendo interesante jurisprudencia con relación a la protección de los datos personales. Así, pues, en un emblemático caso, la AEPD sancionó a *Facebook* con una multa total de 1 200 000 euros por una serie de infracciones a la Ley Orgánica de Protección de Datos.

Y es que si echamos un vistazo a las infracciones cometidas por la red social en el presente caso, se puede advertir que las políticas de *Facebook* no —necesariamente— están en consonancia con la protección de los derechos de los internautas. Así, pues la infracción considerada como muy grave y que equivalió la mitad de la multa —esto es, 600 000 euros— consistió en que: "la red social trata datos especialmente protegidos con fines de publicidad, entre otros, sin obtener el consentimiento expreso de los usuarios como exige la normativa de protección de datos" —el resaltado es nuestro—. Ahora, ello no queda allí, pues se pudo evidenciar que: "*la política de privacidad de Facebook contiene expresiones genéricas y poco claras, y obliga a acceder a una multitud de enlaces distintos para poder conocerla*"[20].

Debe remarcarse que, con relación a lo antes señalado, muchas veces las proveedoras en internet presentan un lenguaje ambiguo dentro de sus políticas a efectos de poder tener un mejor y mayor manejo —*rectius*, control— de la información. Así, por ejemplo, se podría destinar la información recabada a otros fines —totalmente ajenos al para qué fueron entregados— o se podría, incluso, cederla a terceras personas.

En este punto es interesante traer a colación un muy interesante caso resuelto por la Dirección de Sanciones de la Autoridad en el procedimiento administrativo sancionador seguido contra el Banco Ripley, en el cual se le impuso una multa de 4,5 UIT, pues en el "Formato de Obtención de Consentimiento para el Tratamiento de Datos Personales y Reglamento de protección de Datos Personales" se evidenció que se empleaban fórmulas muy genéricas:

> "*(…) que en ningún caso hacen referencia específica a la información que mínimamente debe ser proporcionada al titular el dato personal, haciéndose referencia a que el consentimiento brindado se mantendrá vigente de manera indefinida 'para elaborar Bases de Datos, transferidas a terceras personas vinculadas o no al banco (…) con la finalidad de (i) otorgarme el producto o servicio solicitado, y/o (ii) ofrecerme otros productos, y/o servicios, y/u ofertas, y/o publicidad, entre otros, del Banco y/o cualquier otra empresa que pertenezca o pueda pertenecer en el futuro al Grupo Ripley domiciliada o no en el país (…)*"[21].

El Considerando 32 del Nuevo Reglamento Europeo de Protección de Datos —pues entrará en vigor el 25 de mayo de 2018— se entiende por consentimiento lo siguiente:

> "*(…) debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, especifica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las*

20. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *"La AEPD sanciona a Facebook por vulnerar la normativa de protección de datos"*. Disponible en: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-ides-idphp.php>.

21. DIRECCIÓN DE SANCIONES DE LA DIRECCIÓN GENERAL DE PROTECCIÓN DE DATOS PERSONALES. *Resolución N° 195-2016-JUS/DGPDP-DS*. Disponible en: <https://www.minjus.gob.pe/wpcontent/uploads/2017/02/RD_195.pdf>.

casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta"[22].

El principio de transparencia aplicado a los datos personales se basa en regular que la información sea recogida y procesada de manera legal, leal y transparente; recabada con fines determinados, explícitos y legítimos; limitada a lo que le atañe en relación con los fines expuestos —minimización de datos—; buscar data actualizada, exacta y segura contra procesos no autorizados o robos, etc.

Los datos de carácter personal no se limitan al nombre, dirección, teléfono, datos bancarios, sino que también lo son nuestros gestos, nuestros comportamientos, cuando ponemos "corazón" en *Instagram* y hasta las "reacciones" que mostramos en *Facebook*. Ello es relevante si lo vemos desde el punto de vista del *Big Data* y la gran cantidad de datos que esta tecnología utiliza para analizarlos y obtener un conocimiento. El concepto de *Big Data* desde su forma de activación ya atenta contra los principios de finalidad y proporcionalidad que recoge la LPDP.

La mencionada ley establece como principio fundamental, el principio de finalidad, referido a que los datos personales que son recopilados deben corresponder a una finalidad determinada, explícita y lícita. En otras palabras, el tratamiento de los datos personales no puede extenderse a otra finalidad para la cual el titular de los datos personales no ha dado su consentimiento. Salvo en los casos que dicha información sea utilizada para actividades de valor histórico, estadístico o científico mediando un proceso de anonimización o disociación. Asimismo, establece el principio de proporcionalidad, el cual señala que todo tratamiento debe ser adecuado, relevante y no excesivo para la finalidad para la cual se recolectaron los datos.

Claramente, con el *Big Data* estos principios no se respetan en la medida que sólo serán útiles los datos recolectados cuando son tratados de manera masiva y dependiendo de los resultados obtenidos serán utilizados de distintas maneras y para propósitos disímiles.

La automatización de los procesos de análisis de datos, en especial de personas, también debe ser vista desde el ámbito de los derechos humanos para no permitir escenarios de discriminación o ceder ante estereotipos. Por ejemplo, la inclusión de variables sensibles —religión, afiliaciones políticas o sindicales, orientación sexual, etc.— para la obtención o retención de puestos de trabajo basados en "perfiles" generados automáticamente. Los responsables del tratamiento de la información deben de estar obligados a presentar los motivos de la toma de la data y los efectos previstos de la creación de perfiles con datos personales.

X: NUEVOS RETOS IMPUESTOS POR EL *BIG DATA*

Nuevas soluciones son necesarias, debido a que el *Big Data* nos presenta desafíos interesantes en muchos de los puntos claves de la privacidad y la protección de datos personales. El valor de la información ya no reside solamente en su uso original o primario, sino que es compartida con los múltiples usos secundarios a la cual será sometida para encontrar correlaciones. La gran cantidad de data facilita la "re-identificación" de sujetos luego de la anonimización de la información. Los investigadores de seguridad ya han advertido que el uso de herramientas para anonimizar datos no es cien por ciento fiable; más aún en el caso de *Big Data* debido al

22. Considerando (32) del Nuevo Reglamento Europeo de Protección de Datos. 2016.

formato estructurado y la masiva cantidad de los datos, siendo posible re identificar al individuo. El Consejo de Asesores del Presidente de los Estados Unidos sobre Ciencia y Tecnología —"PCAST"— fue determinante al reconocer estos riesgos. A continuación, presentamos una traducción libre de parte de dicho documento:

> "*La anonimización de un registro de datos puede parecer fácil de implementar. Desafortunadamente cada vez es más fácil derrotar la anonimización por las mismas técnicas que se están desarrollando para muchas aplicaciones legítimas de Big Data. En general, como el tamaño y la diversidad de los datos disponibles crece, la probabilidad de poder volver a identificar a los individuos —es decir, volver a asociar sus registros con sus nombres— incrementa sustancialmente. (...)*
> *La anonimización sigue siendo útil como salvaguarda adicional, pero no es robusta contra los futuros métodos de re-identificación a corto plazo*"[23].

De otro lado, como se ha mencionado en párrafos precedentes, el consentimiento también pierde relevancia cuando no se sabe específicamente cuáles serán los fines de la información recogida. Frente al problema del consentimiento, han propuesto Cate y Mayer-Schönberger "*cambiar el foco de la responsabilidad y control, del individuo al 'usuario' de los datos*"[24], es decir a las organizaciones encargadas del procesamiento de los datos. También proponen la creación de sistemas de rendición de cuentas y un manejo responsable de la custodia de los datos. Esto significa enfocarse en las formas de utilización de los datos obtenidos más que en el momento en que se otorga el consentimiento para la recolección de información. Así, el consentimiento tendría relevancia cuando sea acotado a situaciones donde el individuo renuncie a derechos o tratamientos previamente reconocidos[25].

La custodia responsable de la información almacenada toma relevancia en un mundo digital, expuesto a ataques, robos, fuga de información o extravíos. Debido a que, el usuario de la data —organizaciones encargadas del procesamiento de los datos— es el responsable de dicha información. Se necesitan protocolos de seguridad adaptables y dinámicos que garanticen la protección de los datos.

Los retos que los avances tecnológicos suponen para la privacidad nos hacen pensar que no solo debemos centrarnos en la normativa y cómo ésta es aplicable a la nueva tecnología, sino que debemos pensar en la privacidad e intimidad personal desde que son diseñadas y desarrolladas dichas tecnologías. Por tanto, no solo pensar en los gastos que pudiera incurrir la empresa para implementar los mecanismos necesarios para cumplir con seguridad y protección de los datos, sino por el contrario, verlo como una ventaja competitiva si es que cuando se está pensando en el negocio y desarrollo de las herramientas, éstas ya contemplan las necesidades de los usuarios y las mayores medidas de seguridad.

Existen otras tendencias en el ámbito mundial para resolver los problemas de protección y privacidad de los datos. Una de ellas aborda el tema de la privacidad de los individuos desde la construcción y el diseño de los sistemas operativos para asegurar herramientas con mayor grado de protección. Así, la protección de datos se convierte en un parámetro más

23. PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY. "*Report to the President. Big Data and Privacy: a technological perspective*". Disponible en: <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf>

24. CATE, Fred y MAYER-SCHÖNBERGER, Viktor. "*Notice and consent in a world of Big Data. International Data Privacy Law*". Segunda edición. Vol. III. Oxford: 2013, pp. 67-73.

25. BAROCAS, Solon y NISSENBAUM, Helen. "*Big Data's End Run around Anonymity and Consent*". En: LANE, Julia; STODDEN, Victoria; BENDER, Stefan y NISSENBAUM, Helen. *Privacy, Big Data, and the Public Good*. Oxford: 2014, Cambridge University Press, pp. 44-75.

en el desarrollo de sistemas de recolección de datos[26].

Otra tendencia es la de implementar nuevos modelos de negocio entre todos los actores. Empresas de internet en la actualidad como *Instagram, Facebook, Google*, entre otras, han conseguido que los individuos compartan datos personales voluntaria y públicamente. Este nivel de confianza alcanzado por los usuarios de la información permite que se cree valor en el proceso y movimiento de la información, mientras más relacionada se encuentre la información, mayor valor es capaz de generar. Es así como los Derechos de Propiedad de los datos y sus responsabilidades se convierten en derechos comunes entre usuarios e individuos. El valor que estos generan surge de la interacción de varios actores.

Otro modelo incipiente se centra en el empoderamiento de los individuos. El diseño de permisos y consentimientos debe partir del diálogo entre todos los agentes involucrados, incluyendo a los entes reguladores y los desarrolladores de tecnología, generando diversos tipos de permisos en función a la información tomada y su uso. Lo relevante de este modelo, es que los individuos se convierten en un agente económico más, gestionan su propia información, para sus propios fines, y comparten una parte de esta información con las empresas para comunicar qué quieren, cómo y cuándo, y para obtener beneficios conjuntos[27]. Los posibles beneficios de este modelo incluyen un mejor manejo de la data personal de los individuos por estos mismos, una mayor calidad de los datos a procesar, menos costos de almacenamiento para los agentes procesadores de Big Data, entre otros.

XI. A MANERA DE CONCLUSIÓN

En la mayoría de los casos, las políticas de privacidad y protección de datos personales ofrecidas a los usuarios son unilaterales y de difícil comprensión, las cuales pocas veces son leídas; por lo que, los nuevos retos para la aplicación de la normativa a estas tecnologías serán: (i) desarrollar mecanismos idóneos y pertinentes para recabar el consentimiento; (ii) informar de manera clara, sencilla y previa al usuario del tratamiento de sus datos personales, de manera tal que ante cualquier cambio en las políticas se notifique adecuadamente; y (iii) poder identificar a los terceros con los cuales se va a compartir información.

Las nuevas herramientas que nos abordan día a día, como la geolocalización, el internet de las cosas, *cloud computing* y más, así como el acelerado avance en las técnicas de procesamiento de grandes cantidades de datos —*Big Data*—, son tan evidentes como los múltiples beneficios económicos y sociales que podríamos obtener de sus resultados. Es por eso que se tienen que encontrar soluciones aceptables a los problemas de privacidad que se generan con el desarrollo del *Big Data* en relación a la protección de datos personales, buscando mitigar los riesgos sin renunciar a los beneficios que esta proporcione.

Será un reto para la Autoridad adaptarse al dinamismo de este entorno tecnológico y determinar cuándo es aplicable la normativa a dichas herramientas. Asimismo, la otra cara de la moneda es que las empresas cumplan con la normativa adoptando las medidas necesarias a fin de fomentar una cultura de resguardo de los datos de carácter personal, sin dejar de ser competitivos y contribuyendo con el desarrollo económico.

Finalmente, en tanto nos encontramos en una época en que el comercio electrónico, *cloud computing* y el *Big Data* efectúan flujo transfronterizo de los datos sin precedentes, son necesarios mecanismos internacionales armonizados o garantías adicionales globales que brinden real protección al individuo a pesar de la extraterritorialidad que puede existir al ser transferidos y almacenados los datos personales fuera del territorio, es decir a un país distinto al país de origen.

26. CAVOUKIAN, Ann y JONAS, Jeff. *"Privacy by Design in the Age of Big Data"*. Disponible en: <https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf>

27. ROUBISTEIN, Ira. "*Big Data: The End Of Privacy Or A New Beginning?*" En: *International Privacy Law*. Segunda edición. Vol. III. 2013, pp. 74-87.