Análisis teórico de cumplimiento del estándar peruano de protección de datos personales: El caso Facebook | Claudia Legua

Por **Hernández & Cía** - 3 marzo, 2021

Escrito por Claudia Legua Zúñiga

1. Introducción:

En el 2011, se promulgó la Ley de Protección de Datos Personales[1], la cual ha establecido y fomentado un estándar de protección de datos. Al ser un tema nuevo, existen creencias comunes que restan relevancia pública a este tema. No obstante, últimamente ha cobrado más relevancia con el incremento de poder de las redes sociales, entre ellas Facebook, que es la más popular.

En el presente artículo, describiremos cómo es el panorama realmente: cuánta información se recopila, qué clase de información se recopila y por qué es importante o qué pueden hacer con ella. En ese contexto, evaluaremos si Facebook podría cometer infracciones bajo nuestra normativa.

2. ¿Facebook se rige bajo la LPDP?:

Es común que se piense que la normativa peruana no aplica para el funcionamiento y resolución de controversias de Facebook al ser una red social internacional, cuya central se encuentra en Estados Unidos. Sin embargo, ello no es así por dos motivos: (i) las disposiciones de la LPDP y (ii) los Términos y Condiciones de Facebook.

De acuerdo con el artículo 3 de la LPDP[2], la Ley se aplica para los datos personales cuyo tratamiento se realiza en territorio peruano. Considerando el concepto de tratamiento de datos personales[3] de la misma ley, es posible afirmar que se aplica la LPDP a las interacciones de los Usuarios con Facebook, en caso la recopilación de información se haya realizado dentro del país (p.e. creación de perfiles, subida de fotos, etc.). Los artículos 32[4] y 33[5] de la LPDP determinan que la Autoridad Nacional de Protección de Datos Personales[6] es la encargada de procurar el cumplimiento de la LPDP y su Reglamento, para lo cual puede resolver procedimientos de oficio, denuncias de partes o reclamaciones de titulares de datos personales; además de poseer facultades sancionadoras.

Por otro lado, los Términos y Condiciones de Facebook[7] establecen que, para el caso de los consumidores (entendiendo estos como los usuarios que son personas naturales), aplican las leyes de su país de residencia en caso de cualquier reclamación, causa o disputa; además de que la causa podrá resolverse en cualquier tribunal competente del país que tenga jurisdicción[8].

Teniendo en consideración ambos instrumentos normativos, podemos concluir que, tanto por ley como por la naturaleza contractual de los T&C (que vinculan a Facebook y los Usuarios), la ley aplicable es la peruana y la Autoridad tiene jurisdicción para conocer reclamaciones o denuncias de los usuarios.

3. La Importancia de la Protección de Datos Personales en Facebook:

Últimamente, ha quedado más claro el valor de los datos personales como activos empresariales. Sin embargo, muchos no ven la importancia de estos como parte de su privacidad o asumen que, al no ser personas de interés, estos no son relevantes y no serán recopilados indebidamente o, incluso, monitoreados.

La realidad es totalmente contraria a esto. Como comenta Marta Peirano para TEDxMadrid[9], la premisa de este razonamiento es que se subestima la cantidad de información que se produce. La periodista relata el caso de Malte Spitz, quien requirió a su compañía de telefonía móvil la información que tenían almacenada respecto de sus actividades. Deutsche Telekom (la compañía) le dio su registro de llamadas correspondientes a seis (06) meses. Al cruzar esta información con otros datos que fueron recopilados de fuentes públicas, **como sus redes sociales**, se pudo generar un mapa donde se ve el día a día de Malte, incluyendo la localización en tiempo real.

Una situación similar se ha visto en Perú, pero a nivel masivo. Un reportaje hecho por Ernesto Cabral para Ojo Público[10] reveló que Telefónica vendió bases de datos con la ubicación de Usuarios de Lima, Callao y otras regiones por S/ 3.9 millones. Si bien estos datos estaban presuntamente "anonimizados"[11], se

encontraron maneras para re-identificar a los usuarios a partir de la ubicación del teléfono. Por ejemplo, cruzando ello con la información de **redes sociales**, RENIEC y OSIPTEL, se logró individualizar a un usuario (con fines investigativos) al cual llamaron J.C.L.

Además, Telefónica ha vendido esta información a Clear Channel (empresa de publicidad) para que puedan realizar un análisis de frecuencia y cantidad de personas que transitan por sus avisos; así como su edad, género y nivel socioeconómico.

A partir de los ejemplos, hemos visto que diferentes empresas (e, incluso, el estado) no hace distinción al momento de recopilar información; por lo que independientemente de si un sujeto es "conocido" o no, se ve afectado por estas amenazas a la privacidad. También vemos ello no afecta el valor de los datos pues las empresas están dispuestas a pagar millones por nuestros datos personales.

Entonces, activamente se recopila información personal de todos nosotros; pero ¿qué pueden hacer con estos datos? ¿es peligroso que los recopilen?

En el 2018, ocurrió el escándalo de Facebook y *Cambridge Analytica*. La historia se centra en cómo *Cambridge Analytica* pudo obtener la información de casi 87 millones de personas[12], haciendo uso de términos y condiciones de Facebook (del 2013), los cuales permitían el acceso a los datos personales de los contactos (conocidos como "amigos") de los titulares de perfiles en Facebook sin su consentimiento[13].

A través del uso de los datos personales de los usuarios de Facebook, se armaron perfiles psicológicos (sin autorización alguna), de manera que, en base a ellos, se pudo canalizar y realizar publicidad de ciertos partidos o representantes políticos de manera que ganen ventaja respecto de sus contrincantes. Esta empresa ha sido contratada por políticos como Ted Cruz[14] y se le atribuye un papel fundamental en la elección de Donald Trump, así como en la elección del Brexit.

Este evento refleja la relevancia de la cantidad y calidad de información que **realmente** es transmitida por Facebook[15]; y su poder, al ser posible utilizarlos de manera que se pueda localizar permanentemente a los usuarios o moldear sus inclinaciones personales. De esta manera, queda evidenciada la importancia de la protección de los datos personales de todos nosotros (independientemente de quién se trate).

4. ¿Facebook Cumple con el Estándar de Protección de Datos Peruano?

Habiéndose establecido la importancia de la protección de datos personales de las personas en general (o un usuario cualquiera), debemos analizar si las actividades de Facebook podrían constituir infracciones a la LPDP, según el criterio de la Autoridad.

A primera vista, pareciera que existiría una infracción al deber de consentimiento, reconocido en el artículo 5 de la LPDP[16] y 7 de su Reglamento[17]; el cual establece que, para realizar cualquier tipo de tratamiento de datos personales, se requiere el consentimiento libre, previo, expreso, informado e inequívoco de su titular. Es decir, Facebook no puede utilizar nuestros datos (de cualquier manera) si no lo autorizamos.

No obstante, se acuerdo con el artículo 14 de la LPDP, hay situaciones excepcionales donde no será necesario requerir el consentimiento del titular. En el presente artículo, nos concentraremos en dos: cuando los datos están destinados a o están contenidos en fuentes de acceso público y cuando se tratan como parte de la ejecución de un contrato.

La información que ponemos en Facebook a disposición de nuestros amigos (fotos, videos, estados, etc.) se considera como fuente de acceso público (en los casos de los perfiles públicos), de acuerdo con el criterio de la Autoridad seguido en la Resolución Directoral No. 1623-2019-JUS/DGTAIPD-DPDP[18]. Así, el tratamiento de la información que ponemos en nuestro "muro" o disponible para cualquier usuario no requeriría consentimiento.

No obstante, como lo menciona la misma Resolución, ello no significa que puede haber un tratamiento irrestricto de datos personales. La recolección y cualquier tratamiento posterior a esta necesita consentimiento[19]. Además, esta excepción únicamente abarca ciertos datos que recolecta Facebook (que se hallan en los perfiles), necesitándose aún consentimiento para utilizar datos que no son públicos como las preferencias de los usuarios o los datos que seleccionan para que permanezcan privados. Así, vemos que la excepción no cubre todas las funcionalidades de Facebook.

Respecto a la parte no cubierta, entra a colación la segunda excepción: ejecución de relación contractual. Los usuarios se encuentran dentro de una relación de consumo (o prestación de servicios) con Facebook; pero ¿qué servicio nos presta Facebook? De acuerdo con sus términos y condiciones[20], proporcionan:

- Una experiencia personalizada.
- Conexión con personas y organizaciones de interés del usuario.
- Herramientas para que el usuario se exprese y hable de temas que le sean importantes.
- Descubrir contenido, productos y servicios que podrían interesarle al usuario.
- Combaten las conductas perjudiciales y protegen a la comunidad de usuarios.
- Usan y desarrollan tecnologías para brindar servicios seguros y funcionales.
- Investigan formas para mejorar sus servicios.
- Ofrecen experiencias uniformes y sin interrupciones de los productos de las empresas de Facebook.
- Permiten el acceso a sus servicios desde cualquier lugar.

Ello va de acuerdo con lo señalado por Richter y Koch[21]: las redes sociales ofrecen al usuario un reflejo de las interacciones a nivel real pero dentro del mundo digital. De esta manera, uno puede expandir su círculo social e interactuar en Facebook sin las barreras del espacio-tiempo.

Es en virtud de la provisión de este servicio que se aplica la excepción del numeral 5 del artículo 14 de la LPDP, ya que los datos se comparten y difunden para dar una mejor experiencia social al usuario: comprar en Marketplace, realizar video llamadas, etc. En suma, al formar parte del servicio brindado por Facebook[22], los datos que no se encuentran en nuestro perfil también pueden ser usados sin nuestro consentimiento.

Sin perjuicio de las excepciones al deber de consentimiento, es necesario que se cumpla con los otros principios de la LPDP y su Reglamento. Entre ellos, se encuentra el deber de información, establecido en el artículo 18 de la LPDP[23], que establece que se debe comunicar al titular de datos personales (o a los usuarios) acerca de tratamiento que se dará a sus datos.

Este deber está estrechamente relacionado con el deber de consentimiento pues este debe ser informado. No obstante, de acuerdo con el reciente criterio de la Autoridad (cambiado hace 4 años), podría constituirse una infracción por no informar a los titulares por el tratamiento, independientemente de si es aplicable una excepción al consentimiento[24].

Así, el artículo 18 determina 8 puntos que deben ser informados, entre los cuales hemos identificado que no se estaría cumpliendo con los siguientes:

- Informar la identidad y domicilio (país) de los destinatarios, y la finalidad de transferencia à Facebook señala en su política de privacidad[25] que los "Socios" reciben datos de los usuarios cuando visitan o utilizan sus servicios en Facebook. No obstante, no se precisa a quiénes exactamente es que se transfiere la información, ya que se "informa" acerca de la transferencia utilizando un término general para referirse a los destinatarios (Socios), lo cual incumple con la LPDP pues la información debe ser detallada.
- Flujo Transfronterizo à este concepto se refiere a la transferencia internacional de datos, la cual debe ser comunicada a los usuarios, así como el país al cual se transfieren los datos. Sin considerar a los Socios que se encuentren fuera del país, el propio almacenamiento de datos por parte de Facebook implica un flujo transfronterizo ya que sus servidores están en Estados Unidos. Ninguna de las dos situaciones es comunicada, por lo que habría una infracción.
- Finalmente, Facebook no detalla exactamente cuáles son las finalidades del tratamiento que da a los datos de los Usuarios. Por ejemplo, no enlista por qué o para qué transfiere o recopila qué datos.

5. Conclusiones:

A partir de lo expuesto, vemos que Facebook sí debe cumplir con el estándar peruano de protección de datos personales (para el caso de personas naturales). Además, es importante que cuidemos de esta información pues es valiosa, no solo para las empresas, sino para nuestra privacidad. Finalmente, se concluye que Facebook, está eximido de cumplir con el deber de consentimiento, pero, bajo el criterio actual de la Autoridad, podría estar cometiendo una infracción al deber de información.

Imagen obtenida de https://cutt.ly/al0q53B

* Asociada Contratada del Área de Competencia; Telecomunicaciones, Medios y Tecnología; y Propiedad Intelectual del Estudio Hernández & Cía Abogados y Miembro extraordinario de la Asociación Ius Et Veritas.

[1] En adelante, la "LPDP".

[2] ***Artículo 3. Ámbito de aplicación.*** *La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles.*

[3] ***Artículo 2. Definiciones.*** *Para todos los efectos de la presente Ley, se entiende por: (…) 19. Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.*

[4] ***Artículo 32. Órgano competente y régimen jurídico.*** *El Ministerio de Justicia, a través de la Dirección Nacional de Justicia, es la Autoridad Nacional de Protección de Datos Personales. (…) Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces. (…).*

[5] ***Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales.*** *La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes: (…)8. Supervisar el cumplimiento de las exigencias previstas en esta Ley, para el flujo transfronterizo de datos personales. (…) 15. Atender solicitudes de interés particular del administrado o general de la colectividad, así como solicitudes de información. 16. Conocer, instruir y resolver las reclamaciones formuladas por los titulares de datos personales por la vulneración de los derechos que les conciernen y dictar las medidas cautelares o correctivas que establezca el reglamento. 17. Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores. 18. En el marco de un procedimiento administrativo en curso, solicitado por la parte afectada, obtener de los titulares de los bancos de datos personales la información que estime necesaria para el cumplimiento de las normas sobre protección de datos personales y el desempeño de sus funciones. 19. Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley. 20. Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento. (…).*

[6] En adelante, la "Autoridad".

[7] https://www.facebook.com/legal/terms

[8] *4. Disputas: Intentamos imponer reglas claras para poder limitar o, mejor aún, evitar disputas contigo. No obstante, si surge alguna disputa, es útil saber con anticipación dónde se puede resolver y qué leyes se aplican. Si eres consumidor,* ***las leyes del país donde resides se aplicarán a cualquier reclamación, causa o disputa que presentes contra nosotros*** *y que surja como consecuencia de estas Condiciones o los Productos de Facebook, o en relación con ellos. Asimismo,* ***puedes resolver la reclamación en cualquier tribunal competente del país que tenga jurisdicción.*** *En todos los demás casos, aceptas que la reclamación debe resolverse de forma exclusiva en el Tribunal Federal del Distrito Norte de California de los Estados Unidos o en un tribunal estatal ubicado en el condado de San Mateo. Asimismo, aceptas someterte a la jurisdicción personal de cualquiera de estos tribunales con el propósito de litigar cualquier reclamación y que las leyes del estado de California regirán estas Condiciones, así como cualquier reclamación, independientemente de las disposiciones sobre conflictos de leyes.*

[9] PEIRANO, Marta. "¿Por qué me vigilan, si no soy nadie?" Madrid: TEDxMadrid. 2015. <https://www.youtube.com/watch?v=NPE7i8wuupk>

[10] CABRAL, Ernesto. "Telefónica del Perú vende ubicación de clientes y pone en riesgo su privacidad". Lima: Ojo Público. 2019 < https://ojo-publico.com/1393/telefonica-vende-ubicacion-de-clientes-y-amenaza-seguridad>

[11] [LPDP] ***Artículo 2. Definiciones****. Para todos los efectos de la presente Ley, se entiende por: (…) 14. Procedimiento de anonimización. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.*

[12] KANG, Cecilia. "Facebook admite que Cambridge Analytica accedió a los datos de 87 millones de usuarios" *New York Times*. Nueva York, 04 de abril de 2018. Consulta: 10 de mayo 2019. <https://www.nytimes.com/es/2018/04/04/facebook-cambridge-analytica-87-millones/>

[13] MEREDITH, Sam. "Facebook-Cambridge Analytica: A timeline of the data hijacking scandal". *Consumer News and Business Channel.* Estados Unidos, 10 de abril de 2018. Consulta: 09 de mayo de 2019. <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

[14] TIMMONS, Heather. "If Cambridge Analytica is so smart, why isn't Ted Cruz president?". *Quartz.* 21 de marzo de 2018. Consulta: 11 de mayo de 2019. <https://qz.com/1234364/cambridge-analytica-worked-for-mercer-backed-ted-cruz-before-trump/

[15] En adelante, "Facebook" hará referencia a las plataformas por analizar en el presente trabajo; es decir, Facebook, Instagram y WhatsApp.

[16] Artículo 5. Principio de consentimiento. *Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.*

[17] ***Artículo 7.- Principio de consentimiento.*** *En atención al principio de consentimiento, el tratamiento de los 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 forma 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.*

[18] *40. (…) [E]s necesario tener presente el hecho de que el perfil de Facebook de la denunciante se encontraba en modo "público", vale decir, eran libremente accesibles para cualquier otro usuario de dicha red social, sin necesidad de estar dentro de sus contactos; (…). Dicha carencia de restricciones de acceso a las cuentas personales de Facebook deriva en que estas constituyan fuentes de datos personales accesibles al público, de acuerdo con la definición establecida en el numeral 9 del artículo 2 de la LPDP (…).*

[19] *Sin embargo, aún cuando en este caso se halle una fuente accesible al público, ello no significa un tratamiento irrestricto de los datos personales que contengan dichas fuentes (…). 43. De lo expuesto, se tiene que si bien la cuenta Facebook de la denunciante constituye una fuente de acceso pública, la extracción y las posteriores actividades de tratamiento que se efectúe con las imágenes que contiene, debe acatar los principios de la LPDP y su reglamento.*

[20] https://www.facebook.com/legal/terms

[21] RICHTER, Alexander y Michael KOCH. "Functions of Social Networking Services" en *8th International Conference on the Design of Cooperative Systems.* Francia: Institut d'Etudes Politiques d'Aix-en-Provence. 2008, , pp. 87-98.

[22] Independientemente de si sea correcto o preciso.

[23] ***Artículo 18. Derecho de información del titular de datos personales.*** *El titular de datos personales tiene derecho a ser informado en forma detallada, actualizadas sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.*

[24] Ver Resolución Directoral Nº 807-2017-JUS/DGTAIPD-DPDP.

[25] https://www.facebook.com/about/privacy/update

Hernández & Cía