El Derecho Fundamental a la Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales APDP

PERU

Ministerio de Justicia y Derechos Humanos

José Alvaro Quiroga León

Director General

ASPECTOS CONTROVERSIALES

Cuál es el límite de la privacidad en Facebook

MIGUEL ALONSO JUAPE PINTO
miguel.juape@diariogestion.com.pe

Un informe de la Autoridad Nacional de Datos Personales (APDP), despertó la relevancia del tema de la información contenida en redes sociales, ya que la Policía Nacional del Perú (PNP) preguntó si esta es pública o privada, con la finalidad de llevar a cabo investigaciones.

El informe detalló que "los datos personales (nombre, fotos, trabajo, ubicación y otros) de cualquier red social (sin importar el nivel de privacidad) no pueden ser empleados por terceros para ningún tipo de finalidad, ya que no son fuentes accesibles al público de acuerdo a ley".

Al respecto, Andrés Calderón, socio del estudio Muñiz, opinó que la APDP tiene un objetivo bueno (proteger la privacidad), pero parte de una premisa equivocada (asumen que todas las personas requieren que la APDP cuide su privacidad más allá de sus decisiones) y termina en un resultado irreal (busca proteger algo que en la práctica se entiende como información pública).

Por su parte, el jefe de la APDP, José Quiroga, explicó que las redes sociales no son una fuente acceso público según la ley, sirve para intercambio de información y puede incluir datos personales "puede ser privado si así se configura", por lo que su tratamiento comercial, periodístico u otro, requerirá del consentimiento del titular de datos personales, ya que de lo contrario se vulnera su derecho a la privacidad.

Red social. *Pública o privada.*

Pero también existe información que se comparte en la red social sin restricciones (Facebook de negocios y otros), en cuyo caso no se requeriría el permiso.

Sin embargo, es claro que existe una sensación generalizada de que la información de esta red social es pública, pero no siempre es así, concluyó.

ECONOMIST
GESTIÓN

A PARTIR DE MAYO

Se endurecerá fiscalización a empresas por datos personales

—La Autoridad Nacional de Datos Personales realizó 100 supervisiones y tiene registrados 1,378 bancos de datos personales, detalló José Quiroga.

MIGUEL ALONSO JUAPE PINTO
miguel.juape@diariogestion.com.pe

El consentimiento para el uso de un dato personal (nombre, dirección, imagen y otros) es una parte de los procesos que todas las empresas tendrán que adecuar para cumplir con la Ley de Protección de Datos Personales (LPDP), ya que ello será exigible desde mayo de este año, aseguró Daniel Flores abogado del estudio Pizarro, Botto & Escobar.

Sin embargo, el jefe de la Autoridad Nacional de Datos Personales (ANDP), José Quiroga, precisó a Gestión que lo que será suspendido hasta mayo del 2015, son las medidas de seguridad que las empresas deberán implementar sobre los bancos de datos personales. Es decir, asignar a un responsable del acceso o uso de la información del banco de datos y otros.

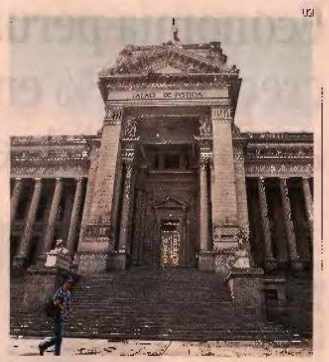
Pero la obligación de obtener el consentimiento del titular del dato personal, para un uso determinado de esta información, ya es exigida a las empresas, ya la fecha se han realizado 100 supervisiones, dijo.

OPINIÓN

José Álvaro Quiroga León
JEFE DE LA ANDP

LAS OBLIGACIONES SON PRECISAS

El centro de gravedad de la Ley de Protección de Datos Personales no es el "banco de datos" sino el "tratamiento de los datos personales". Entonces, las normas que regulan el plazo de adecuación indican que los bancos de datos tienen un plazo de adecuación que vence en mayo del 2015, con excepción a la obligación de inscribir. Es decir, las empresas ya están obligadas a registrar los bancos de datos personales que tengan (existen 1,378 registrados). Así, las normas sobre el tratamiento de datos personales regulan dos obligaciones, las medidas de seguridad y la inscripción. En consecuencia, la única obligación que está suspendida para las empresas que tengan banco de datos es que cuenten con medidas de seguridad.



Expreso. La ley regula el consentimiento expreso, verbal o escrito, pero no tácito, de los datos personales, afirma José Quiroga León.

Consentimiento tácito

De otro lado, Daniel Flores opinó que puede existir un consentimiento tácito del uso de los datos personales, aunque habrá un problema al momento de probar esta autorización en las fiscalizaciones.

Por ejemplo, dijo, es posible demostrar que existe un consentimiento tácito para ser filmado si la empresa coloca un aviso, ya que la filmación es una obligación impuesta por algunas municipalidades por temas de seguridad.

SEMANAeconómica

TECNOLOGÍA EN TU EMPRESA Por Guillermo Guzmán-Barrón

- ***Big data*: Hoja de ruta para implementarla**
- ***Los datos son la nueva moneda de las empresas***
- ***Computación en la nube*: realidad del futuro, éxito de hoy**
- ***Tendencias tecnológicas* mirando el 2015**

Computación en la Nube, Grandes Datos (Big Data), Social y Movilidad.

www.semanaeconomica.com Lima, 14 de diciembre del 2014 | Año XXX | Nº 1450 | PRECIO: S/.30

SEMANAeconómica

SECTOR PÚBLICO
¿Presidentes regionales *probusiness* y... corruptos? (P. 24)

MEDIO AMBIENTE
La COP 20 y un Perú sin petróleo en el 2015 (P. 26)

MARCO LEGAL

EL SOBRECOSTO DE LA PRIVACIDAD

Los inoportunos excesos de la ley de protección de datos personales (P. 4)

SEMANAeconómica

LAS 10 TECNOLOGIAS QUE CAMBIARAN LA FORMA DE HACER NEGOCIOS

- VEHICULOS NO TRIPULADOS
- CLOUD COMPUTING
- INTELIGENCIA ARTIFICIAL
- INTERNET MOVIL
- INTERNET DE LAS COSAS
- BIG DATA
- GENOMA HUMANO

Videovigilancia
Tracking
Geolocalizacion
Perfilamiento

JOSÉ ÁLVARO QUIROGA, director general de la Autoridad Nacional de Protección de Datos Personales

FOTO: SANDRA GUTIÉRREZ

"La ley no nos permite decidir sobre indemnizaciones"

El jefe de la Autoridad Nacional de Protección de Datos Personales responde a los temores sobre las nuevas obligaciones que exige la ley, calificadas como sobrecostos por el mercado

POR VIVIANA GÁLVEZ

Existe el temor de que la excesiva regulación de datos personales afecte la competitividad de las empresas por las obligaciones que genera.

La ley de protección de datos personales [LPD] no inventa nada: sólo desarrolla un derecho fundamental que está en la Constitución [el de la privacidad de los datos personales]. Tampoco impone obligaciones nuevas: sólo establece las conductas que deben seguir todos para respetar ese derecho fundamental.

Una de las críticas a esas obligaciones está en que es excesivo el detalle que se debe dar en el momento de pedir el consentimiento a las personas para usar sus datos personales [cláusula de consentimiento].

Ni la ley, ni el reglamento ni la Autoridad Nacional de Protección de Datos Personales [ANPDP] han dicho cómo tiene que ser la cláusula. He visto cláusulas de seis líneas que cumplen con la ley y cláusulas de cinco páginas que también lo hacen. Si quieres tener una autorización que te permita hacer todo, te extiendes en la cláusula y, si te la firman, te la firman. No es un problema de la autoridad. ¿Quieres hacer quinientas cosas con los datos personales de un ciudadano? Tendrás que decírselo. No es razonable que quieras hacer quinientas cosas y sólo le informes que harás dos. La extensión de la cláusula depende de lo que quieras hacer con los datos. No de la ley, no del ciudadano, no de la autoridad.

¿Pero los grupos económicos deberán especificar qué empresas del grupo podrán usar los datos o podrán usar un enunciado general?

En tu pregunta hay una lógica de que los grupos empresariales hacían las cosas bien y ahora se les complica la vida.

No digo que las hicieran bien, sino que las hacían de una manera...

Lo hacían de una manera que perjudicaba la privacidad de los ciudadanos. Pueden seguir obteniendo el resultado, pero tendrán que pasar por obtener el consentimiento del ciudadano.

Pero, entonces, ¿tendrán que enumerar todas las empresas o podrán usar un enunciado general?

Todos los que tratan datos, en la medida en que obtendrán tu consentimiento, tienen que transmitirte la información necesaria sobre qué cosas harán. Si tú quieres hacer una cosa, informarás de una cosa. Pero si la complejidad, la diversificación, la potencia a nivel nacional o internacional de tu negocio —no del ciudadano, no de la autoridad— hacen que necesites o quieras o tengas interés o propongas hacer un tratamiento diversificado, múltiple en muchísimas empresas, lo que corresponde es que informes al ciudadano de la dimensión y la magnitud de tu negocio. El problema no está en el ciudadano ni en la autoridad —y digo 'problema' en sentido figurado—: la realidad es que si tienes un negocio simple, el consentimiento será simple. Si tienes un negocio complejo, todas tus actividades son complejas. La complejidad no viene de la ley, sino de la magnitud de tu negocio.

¿No hay maneras menos costosas de proteger este derecho?

En tu pregunta hay una afirmación implícita: cumplir con la ley es costoso. ¿Por qué?

Genera un costo...

Para tu línea de negocio que quiere tomar información que no es tuya.

También a una persona natural le resulta costoso cumplir con las leyes en general...

Pero es un costo legítimo.

Claro, pero se tiene que llegar a un consenso...

Exactamente. El consenso no consiste en eliminar la privacidad. El consenso consiste en encontrar las formas como el ciudadano sea protegido recibiendo el mínimo de la información suficiente para que tome una decisión acertada. Y explicando la realidad de la ley de acuerdo a lo que la ley dice, no a lo que la ley no dice.

Hay una gran diferencia: yo quiero hacer negocios usando la información privada de la gente distintos de los de mi relación contractual establecida. ¿Tengo que obtener un consentimiento con ciertas características? Sí. ¿Eso me genera un costo? Sí. ¿Es un sobrecosto? No. Porque tú haces ese negocio porque quieres ganar dinero; te resulta económicamente rentable abrir esa otra línea de negocio. Eso tiene costos legítimos.

Hay costos desproporcionales.

¿Cuáles?

Si yo no quiero que me ofrezcan servicios no solicitados por correo electrónico, está la regulación de la ley de *antispam*, que permite optar por no recibir más este tipo de correos. Esta opción es menos onerosa para la empresa y respeta también la privacidad de la persona. En cambio la ley de protección de datos personales indica que para ofrecerle eso, primero se debe obtener el consentimiento, lo cual es más costoso.

El sistema de las comunicaciones comerciales —la ley *antispam* y el [registro] "Gracias, no insista"— está vigente. No ha sido derogado. Si cumples con la ley y verificas que la persona no está en el registro, le envías la comunicación. Si no quieres adecuarte a ello, tienes que obtener el consentimiento previo. Eso es más costoso para el comerciante que quiere hacer negocio.

Hay sistemas más costosos para el comerciante y otros más costosos para el ciudadano: el sistema *opt out* —que permite al ciudadano salir; es el caso de la ley *antispam* y el registro "Gracias, no insista"— es más costoso para el ciudadano; y el *opt in* —por el cual para poder enviar comunicaciones se debe esperar a que la gente se inscriba— es más costoso para el comerciante. Lo que tratamos de hacer es una cosa que no sea desequilibrada. Yo no veo que nuestro sistema sea desequilibrado.

¿Una empresa sí podría enviarle publicidad vía correo electrónico?

Y no será infracción siempre que cumpla con los requisitos de la ley *antispam* y el registro "Gracias, no insista" [SE 1456]. Las otras comunicaciones también puede hacerlas, pero previamente tendrá que obtener consentimiento.

¿Por qué no es posible hacerlo vía telefónica, luego de verificar que los números no han sido inscritos en ese registro?

Porque no existe un régimen que así lo autorice, como sí ocurre con los correos electrónicos [ley *antispam*].

Una diferencia entre la regulación peruana y la española, por ejemplo, está en que en la primera existe la posibilidad de que las empresas tengan que pagar una indemnización.

Una autoridad administrativa, como es el caso de la ANPDP, es incompetente para dilucidar un tema de indemnización de responsabilidad extracontractual, porque, además, en ninguna parte de la LPD o del reglamento se establecen fórmulas o procedimientos que incluyan el establecimiento de una indemnización. [Lo señalado en la LPD sobre indemnización] es una norma reiterativa de un mandato general: aquel que hace daño debe repararlo. Si lo que les preocupa es que la ANPDP intervenga en un tema de indemnizaciones, yo considero que la ley no nos permite hacerlo.

Otra exigencia alta es que las empresas tienen que cumplir con estándares ISO en cuanto a las medidas de seguridad.

Eso es falso. Las únicas entidades obligadas a alcanzar estos estándares de normas técnicas son las entidades públicas. Nosotros decimos que la ley establece determinadas condiciones de seguridad. Nosotros no decimos cómo cumplirlas [ver nota *No pero sí* en la pág. 17].

La manera como se ha desarrollado esta protección de la privacidad va contra tendencias del mercado en general, como *data analytics* e inteligencia comercial.

Esas afirmaciones también tienen una carga ideológica. La información está en la red, pero no significa que sea libre. Por ejemplo, tu información privada está en Facebook, pero no por eso deja de ser privada [SE 1456].

¿Qué medidas se han adoptado para acompañar al sector empresarial en la comprensión de la regulación de datos personales?

Hemos absuelto consultas. He recibido a representantes de empresas en mi oficina para reuniones informativas, hemos realizado charlas, hemos tenido capacitaciones en provincias. A todos les he entregado material de difusión, y, si nos piden charlas, se las damos.

¿Las consultas tienen efectos vinculantes?

No.

¿Cómo generar certeza respecto a esta regulación que es nueva para el Perú?

Es complicado de un año para el otro. Nosotros abrimos nuestras puertas para explicar la posición de la ANPDP, que refleja la del resto de autoridades en el mundo, y explicar qué es lo que dice la ley. Tratamos de construir una cultura de protección de datos personales y explicar lo más razonablemente posible los criterios que la conforman. No hemos encontrado nunca ningún tratamiento legítimo y razonable ni en el sector público ni en el privado que tenga que dejar de hacerse porque la LPD lo impide.

¿Qué medidas se han adoptado o adoptarán para atacar el tráfico de datos personales en el mercado negro, por ejemplo, en las galerías de la avenida Wilson [en el centro de Lima]?

Estábamos trabajando un operativo para intervenir ahí. Y mientras lo hacíamos, se modificó el Código Penal [2013] y se criminalizó esa actividad [se volvió un delito]. Hasta antes de esa modificación, el tráfico de banco de datos era una infracción administrativa de nuestra competencia. Pero al criminalizarlo, pasó a ser competencia de la policía y del Ministerio Público.

Nuestra responsabilidad está en advertir que esa información que circula en el mercado negro ha salido de alguna parte. Entonces tenemos que enfocarnos en cerrar el caño en el origen de la salida de esa información, a través de la generación de conciencia de la necesidad de medidas de seguridad. ■

CIFRAS DE LA ANPDP

Presupuesto 2015	S/. 2.9 millones
N° de trabajadores	19
Rango del monto de multas	1 UIT - 100 UIT [S/.3,850 - S/.385,000]

Fuente: Fuente: ANPDP

PARA SABER MÁS:
SE 1450 (14/12/2014): *Sobrecostos inadvertidos*. La regulación de datos personales que se viene resulta muy costosa y el MEF no atinó a neutralizarla en sus paquetes reactivadores.

La protección de datos personales

A propósito del caso "datosperu.org".

José Álvaro Quiroga León
Director general de Protección de Datos Personales - MINJUS

La Autoridad Nacional de Protección de Datos Personales –APDP– del Ministerio de Justicia y Derechos Humanos atendió dos reclamaciones contra la web "datosperu.org", que difundía datos personales e impuso las primeras multas.

Los infractores usaron Twitter para exponer su ignorancia sobre las leyes que regulan su negocio, agraviar y afirmar hechos falsos. Sin argumentos ni respeto por la verdad y la legalidad, al ser tocados en sus ingresos, atacaron. Asumiendo que los *tuits* sean realmente suyos, porque no se identifican, es curioso que hablen de transparencia y se nieguen a identificarse.

Algunos autodenominados "expertos" rápidamente apoyaron al infractor, sin importarles sus calidades ni las de sus argumentos. Han llegado a ofrecerle defensa gratuita y le dieron "tips" para eludir las sanciones, exhibiendo una llamativa valoración positiva sobre un infractor, que es consciente de que debe esconderse. Sus defensores, en cambio, han dejado firmados sus "argumentos".

¿La APDP impide difundir información pública?

No, se trata de información privada de personas naturales. La condición de "información pública" se refiere a la "naturaleza" de la información y no depende de opiniones subjetivas, sino de: a) La Constitución que establece el derecho de acceso a la información pública y excluye de tal acceso a la información personal,
b) La Ley de Transparencia que establece que la información en poder del estado es pública y excluye a la información personal por ser "confidencial". Entonces, NO TODA LA INFORMACIÓN EN PODER DEL ESTADO ES PÚBLICA. Existen excepciones y la información personal es una de ellas. No hace falta mencionar la Ley de Protección de Datos Personales, bastan la Constitución y la propia Ley de Transparencia.

¿Que la información esté "publicada" cambia las cosas?

No, a) porque publicar es un "tratamiento" que no modifica la naturaleza de la información privada. No se debe identificar "lo publicado" con "información pública", existe "información privada" "publicada" que no deja de ser privada, de la misma forma que la información "pública" (la que está en poder del Estado y no está exceptuada) no deja de serlo porque se mantenga en secreto. Una cosa es el "tratamiento" "publicar" o "esconder" y otra la naturaleza de la información y b) porque lo contrario significaría que la persona cuyo nombre es "publicado" perdería su privacidad insostenible, ¿verdad?

El diario oficial *El Peruano* sí puede publicar nombres en las resoluciones –y ello no permite que cualquier otro pueda replicarla– porque tal "tratamiento" está autorizado para las entidades administrativas que expiden actos administrativos y para el diario que cumple con publicarlas. Esos "tratamientos" no requieren consentimiento del ciudadano porque la ley los autoriza. Ahora bien, un diario es fuente de información accesible al público y no se requiere consentimiento de los titulares de la información para acceder a ella, pero no se debe confundir "fuente accesible al público" con "fuente de información pública". No son lo mismo. Para entenderlo basta leer la Ley de Protección de Datos Personales. Entonces, la información personal publicada sigue estando protegida y quien quiera hacer algo más que acceder a ella, debe respetar la ley.

El Comercio

MIERCOLES 13 DE MAYO DEL 2015 |

06:00Editorial

Lo que la ley esconde

- La Ley de Protección de Datos Personales tiene un objetivo positivo, pero su implementación presenta serios problemas.

- El viernes pasado entró en vigencia la llamada Ley de Protección de Datos Personales,
- A primera vista, la ley resulta pertinente. Después de todo, sin el cuidado adecuado los datos personales pueden ser utilizados para fines bastante menos inocuos que una que otra campaña comercial molesta.
- Sin embargo, la ley, tal y como está planteada, despierta cuestionamientos tanto desde el punto de vista económico como desde las libertades para acceder a información pública.

- La ley impone restricciones a la posibilidad de contactar a una persona para ofrecer un servicio, ni siquiera se puede ofrecer un puesto de trabajo.
- Para obtener consentimiento debe tener una cantidad de información que hace de esta una tarea extremadamente complicada.
- La más simple base de datos tiene que contar con complejos mecanismos de seguridad que la mayoría de empresas e instituciones públicas no cumple y tal vez no tenga los recursos para hacerlo.
- La restricción de acceso a información pública, la interpretación de la ley por parte de la APDP es preocupante. En el caso DatosPeru.org, dictaminó que la republicación de información aparecida en el diario oficial "El Peruano" de forma que sea más amigable para los usuarios iba en contra de la norma.
- La norma impediría iniciativas vinculadas al periodismo de datos
- Los programas para buscar los antecedentes de los candidatos a cargos políticos estarían vetados: primero habría que pedirle permiso a los más de 11.000 candidatos que participan en las elecciones regionales y municipales, y a los más de 1.500 que aspiran al Congreso.
- La publicación del listado de personas espiadas por la DINI tampoco hubiese sido posible bajo esta norma.
- La protección de datos personales es una tarea valiosa y cada vez más urgente en. La manera no debe ser imponiendo costos desproporcionados a las empresas ni impidiendo el manejo de información pública.

El Comercio

La protección de datos

por José Álvaro Quiroga León

La protección de datos personales (PDP) es un derecho constitucional, no una parte prescindible de la cadena de producción, un sobrecosto o un problema de competitividad.
Veámoslo al revés: ¿Puede considerarse legal un negocio basado en violar la privacidad? No, y solo ese tipo de negocios resulta inviable como efecto de la LPDP.

Los demás pueden incorporar la PDP en el modelo de negocio como un valor que genera confianza.

¿Una llamada ofreciendo trabajo es perjudicial? No, entonces, ¿por qué la LPDP lo impediría?

- La LPDP no regula –y no puede restringir– el acceso a información pública. La Constitución y la Ley de Transparencia dicen que la "información pública" es accesible y que la información personal no está en esa categoría. La LPDP no dice nada nuevo.

- Las empresas no necesitan el consentimiento de sus clientes para tratar su información, en la ejecución de la relación contractual que los vincula.
- Para otros casos, la LPDP requiere consentimiento y quien usa nuestros datos se debe informar: responsable, para qué y dónde. Es información básica para controlar lo que otro hace con algo nuestro.
- Si trabajas con datos de otros, lo mínimo es que te hagas cargo de las responsabilidades y sin esa información sería imposible

- Datosperu.org no fue sancionada por difundir información pública o normas legales, sino por negociar información personal. Que dicha información haya sido previamente publicada por un diario no cambia su naturaleza privada (de la misma manera que ocultar información pública no la convierte en privada).
- Dicen que salieron de la red porque Google les cortó la plataforma para publicidad. ¿Google está en contra de difundir información pública?

- La LPDP no dicta mecanismos de seguridad. Establece deberes para evitar accesos no autorizados, pérdidas o alteraciones y cada quien puede implementar los mecanismos que decida.
- La Directiva de Seguridad es una guía que se toma el trabajo de diferenciar cinco niveles (de básico a crítico), para sugerir mecanismos "a la medida".
- En cuanto a libertad de información, la LPDP no puede restringirla, porque también es un derecho fundamental y si el interés público sostiene el trabajo de la prensa, la protección de datos no impide su desarrollo.

- Más bien recordemos que la PDP ayuda a proteger muchos otros derechos: al honor a la imagen, a la no discriminación, a la salud, a la libertad religiosa y de contratación y un largo etcétera.

Ley de Protección de Datos Personales: ¿cuán protegidos estamos?

22 OCTUBRE 2015

A cinco meses de entrar en plena vigencia, los defectos de la ley empiezan a notarse, aunque disminuye la reticencia de los empresarios para adecuarse.

Cuales son esos defectos ?
Los que se levantaron en la entrevista que no publicaron

- A la PDP Se echan sombras, atribuyéndole contenidos que no tiene.

Que hacer?

Sigamos hablando y debatiendo de este derecho fundamental y permitamos así que la luz disipe el desconocimiento.

MUCHAS GRACIAS

José Alvaro Quiroga León

apdp@minjus.gob.pe