1340

PERÚ | Ministerio de Justicia y Derechos Humanos

Despacho Viceministerial de Justicia

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del diálogo y la reconciliación nacional"

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
MESA DE PARTES
06 MAR 2018
RECIBIDO
Firma Hora

Miraflores, 06 MAR. 2018

OFICIO N° 225 -2018-JUS/VMJ

47399

Señor
JAVIER VELÁSQUEZ QUESQUÉN
Congresista de la República
Presente.-

Asunto : *Remite información sobre acciones realizadas por el sector frente a la venta ilegal de bases de datos personales en el centro de la ciudad de Lima.*

Referencia : *Oficio 409-2017-2018-CDNOIDALCD/CR*
Oficio 430-2017-2018-CDNOIDALCD/CR

De mi mayor consideración:

Tengo el agrado de dirigirme a usted para saludarlo cordialmente y a la vez dar respuesta a los documentos de la referencia, mediante los cuales solicitó información a este Ministerio sobre el tema del asunto.

Al respecto, me permito remitir copia del Informe N° 06-2017-JUS/DGTAIPD, elaborado por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del sector, con el que se atiende dicho requerimiento.

Sin otro de momento, aprovecho la ocasión para expresarle los sentimientos de mi consideración y estima.

Atentamente,

JUAN TEODORO FALCONI GÁLVEZ
Viceministro de Justicia
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

CONGRESO DE LA REPÚBLICA
COMISIÓN DE DEFENSA NACIONAL, ORDEN INTERNO, DESARROLLO ALTERNATIVO Y LUCHA CONTRA LAS DROGAS
07 MAR 2018
RECIBIDO
Firma Hora

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
Despacho Viceministerial de Justicia
08 ENE 2018
RECIBIDO
Hora 5:15
Firma
N° REGISTRO

INFORME N° 06-2017-JUS/DGTAIPD

A	:	**Juan Teodoro Falconi Gálvez** Viceministro de Justicia
DE	:	**Miriam Isabel Peña Niño** Directora General (e) de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
ASUNTO	:	Acciones de la APDP frente a la venta ilegal de bases de datos personales en el Centro de Lima
REFERENCIA	:	Oficio N° 430-2017-2018-CDNOIDALCD/CR
FECHA	:	Miraflores, 29 de diciembre de 2017

Me dirijo a usted para informarle respecto a las acciones de la Autoridad Nacional de Protección de Datos Personales frente a la venta ilegal de bases de datos en el Centro de Lima.

I. La protección normativa del derecho de acceso a la información pública y de los datos personales

El reconocimiento y desarrollo de los derechos fundamentales a la protección de datos personales y de acceso a la información pública se ha realizado, en primer término, en la Constitución Política del Perú.

La Norma Fundamental reconoce en su artículo 2, numeral 5, el derecho de toda persona al acceso a la información pública de la siguiente manera:

> *5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. (...)*

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

Por su parte, el artículo 2, numeral 6, de la Constitución reconoce el derecho de toda persona a la protección de sus datos personales de la siguiente manera:

> *6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*

Luego de casi diez años después, en el año 2002, se aprobó la Ley No. 27806, Ley de Transparencia y Acceso a la Información Pública, y en el año 2003 se aprobó su Reglamento, mediante Decreto Supremo No. 072-2003-PCM y su

Texto Único Ordenado, mediante Decreto Supremo No. 043-2003-PCM. Estas normas tuvieron como finalidad la promoción de la transparencia de los actos del Estado y regular el derecho fundamental del acceso a la información pública, estableciendo las obligaciones de todas las entidades estatales respecto a la adecuada protección de dicho derecho fundamental, entre ellas la vigencia del principio de publicidad de todas las actividades y disposiciones emitidas por las entidades estatales, el establecimiento del Portal de Transparencia Estándar, las sanciones a los funcionarios en casos de incumplimiento, el procedimiento de atención de los pedidos de acceso a la información, los derechos de los administrados, entre otros aspectos.

Dichas normas son de obligatorio cumplimiento para todas las entidades a las que hace mención el artículo I del Título Preliminar del TUO de la Ley No 27444, Ley del Procedimiento Administrativo General:

- Poder Ejecutivo.
- Poder Legislativo.
- Poder Judicial.
- Gobiernos regionales y gobiernos locales
- Organismos constitucionales autónomos
- Entidades, organismos, proyectos y programas del Estado, cuyas actividades se realizan en virtud de potestades administrativas
- Personas jurídicas privadas (por concesión, delegación o autorización del Estado):
    - Prestan servicios públicos.
    - Ejercen funciones administrativas.

Además de las entidades antes mencionadas, de acuerdo con el desarrollo en estos años de la jurisprudencia del Tribunal Constitucional, se han establecido expresamente otras entidades que también están obligadas a dar cumplimiento a los pedidos de acceso a la información pública tales como:

- Administradoras privadas de fondos de pensiones.
- Asociaciones mutualistas.
- Caja de beneficios y seguridad social del pescador.
- Cajas municipales de ahorro y crédito.
- Colegios profesionales.
- Empresas de agua potable y alcantarillado.
- Empresas de comercialización y distribución de energía eléctrica.
- Empresas privadas de telefonía.
- Empresas privadas de transporte aéreo.
- Notarías.
- Universidades públicas y privadas.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA

En materia de protección de datos personales, en el año 2011 se promulgó la Ley No. 29733, Ley de Protección de Datos Personales -LPDP-, con el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen. La aplicación de dicha norma es para

los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada.

La Ley de Protección de Datos Personales encarga su tutela en sede administrativa al Ministerio de Justicia y Derechos Humanos estableciendo que este Sector ejerce la Autoridad Nacional de Protección de Datos Personales - APDP. Corresponde a dicha autoridad realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de LPDP y de su reglamento. Para dicho efecto, la Ley le ha otorgado potestad sancionadora, así como de potestad coactiva.

En el año 2017, se publicó el Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública y fortalece el régimen de la protección de datos personales, el cual entró en vigencia con la publicación de su Reglamento, aprobado mediante Decreto Supremo No. 019-2017-JUS. Con ello, se crea una nueva institucionalidad en materia de transparencia, acceso a la información pública y protección de datos personales, encargando ambas Autoridades al Ministerio de Justicia y Derechos Humanos, específicamente, se ha designado a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales el ejercicio de tales funciones.

Entre las novedades en materia de acceso a la información pública, la Autoridad tiene la función de *"supervisar el cumplimiento de las normas en materia de transparencia y acceso a la información pública"* y *"fomentar la cultura de transparencia y acceso a la información pública"*, así como de establecer lineamientos de clasificación/desclasificación de información conjuntamente con las entidades públicas involucradas. Se establece también un nuevo régimen de sanciones para los funcionarios y servidores públicos, ante el incumplimiento de sus obligaciones sobre la materia.

El Decreto Legislativo no solamente crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública -ANTAI-, sino también el Tribunal de Transparencia y Acceso a la Información Pública, que será la última instancia administrativa que resuelva las controversias que se presenten en materia de acceso a la información a nivel nacional, resolviendo las apelaciones contra las denegatorias de entrega de información pública, lo que incluye a los gobiernos regionales y locales.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

Una de las funciones más importantes del Tribunal es que se encarga de resolver también los conflictos que se presenten entre el derecho de acceso a la información pública y el derecho a la protección de datos personales.

En materia de protección de datos personales, el citado Decreto Legislativo ha precisado que la responsabilidad de los obligados en materia de protección de datos personales es objetiva; es decir, no será relevante para verificar una infracción (aun cuando sí para la graduación de la sanción) la conciencia y voluntad de incumplir esta regulación.

Ello obliga a las empresas a ser aún más cuidadosas en el cumplimiento de esta regulación, cuyas exigencias implican entre otros: i) contar con el consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, como regla general para su tratamiento, salvo las excepciones previstas por la Ley; y, ii) asegurar que los bancos de datos personales y su tratamiento cuenten con los estándares que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado, en especial cuando el tratamiento de datos sea encargado a terceros, quienes asumen las mismas obligaciones que el titular del banco de datos.

II. Nueva institucionalidad de la Autoridad Nacional de Protección de Datos Personales

Tal como se ha señalado, la Autoridad Nacional de Protección de Datos Personales ha tenido cambios en su estructura, dado que, hasta junio de 2017, las funciones de la APDP eran ejercidas por la Dirección General de Protección de Datos Personales, que pertenecía al Viceministerio de Derechos Humanos y Acceso a la Justicia.

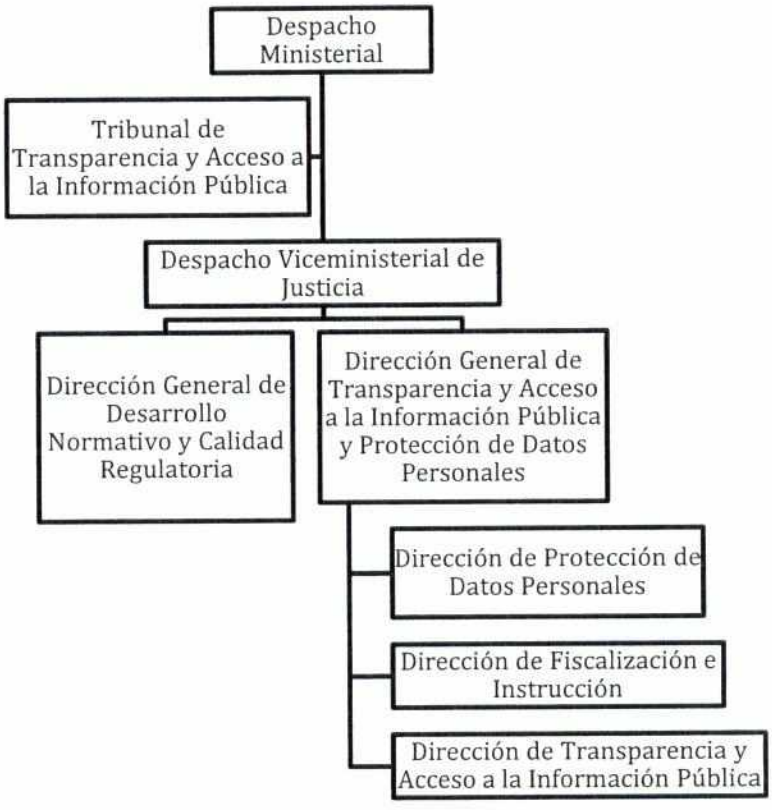
Con la vigencia del Decreto Legislativo No. 1353 y su reglamento, y el nuevo Reglamento de Organización y Funciones del MINJUS, aprobado en junio de 2017, mediante el Decreto Supremo N° 013-2017-JUS, se crea la Dirección General de Transparencia, Acceso a la Justicia y Protección de Datos Personales, que depende jerárquicamente del Viceministerio de Justicia.

Dicho órgano de línea ejerce tanto las funciones de la Autoridad Nacional de Protección de Datos Personales, como de la nueva Autoridad Nacional de Transparencia y Acceso a la Información Pública, creada mediante el Decreto Legislativo N° 1353, vigente desde el 15 de setiembre del presente.

Atendiendo a la nueva normativa vigente, la estructura orgánica de la Autoridad Nacional de Protección de Datos Personales y de la Autoridad Nacional de Transparencia y Acceso a la Información Pública ha quedado establecida de la siguiente manera:

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

Nueva estructura de la Autoridad Nacional de Protección de Datos Personales



III. Autoridad Nacional de Protección de Datos Personales

El numeral 6 del artículo 2 de la Constitución Política del Perú, señala que toda persona tiene derecho a que *"los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"*.

En ese marco, la Ley N° 29733, Ley de Protección de Datos Personales, modificada mediante el Decreto Legislativo N° 1353, y su reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS, desarrollan el derecho fundamental a la protección de datos personales.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

De acuerdo con el artículo 33 de la LPDP, la APDP ejerce las siguientes funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras:

- Representar al país ante las instancias internacionales en materia de protección de datos personales.
- Cooperar con las autoridades extranjeras de protección de datos personales para el cumplimiento de sus competencias y generar

mecanismos de cooperación bilateral y multilateral para asistirse entre sí y prestarse debido auxilio mutuo cuando se requiera.

- Administrar y mantener actualizado el Registro Nacional de Protección de Datos Personales.
- Publicitar, a través del portal institucional, la relación actualizada de bancos de datos personales de administración pública y privada.
- Promover campañas de difusión y promoción sobre la protección de datos personales.
- Promover y fortalecer una cultura de protección de los datos personales de los niños y de los adolescentes.
- Coordinar la inclusión de información sobre la importancia de la vida privada y de la protección de datos personales en los planes de estudios de todos los niveles educativos y fomentar, asimismo, la capacitación de los docentes en estos temas.
- Supervisar el cumplimiento de las exigencias previstas en la LPDP, para el flujo transfronterizo de datos personales.
- Emitir autorizaciones, cuando corresponda, conforme al reglamento de la LPDP.
- Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
- Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.
- Emitir las directivas que correspondan para la mejor aplicación de lo previsto en la LPDP y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.
- Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales.
- Celebrar convenios de cooperación interinstitucional o internacional con la finalidad de velar por los derechos de las personas en materia de protección de datos personales que son tratados dentro y fuera del territorio nacional.
- Atender solicitudes de interés particular del administrado o general de la colectividad, así como solicitudes de información.
- 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.
- Velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores.
- 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.
- Supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan conforme a ley.

- Iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la LPDP y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.
- Las demás funciones que le asignen la LPDP y su reglamento.

IV. Facultad fiscalizadora y sancionadora de la APDP

La APDP tiene facultad de fiscalizar de oficio o por denuncia actos contrarios a la LPDP[1].

Las actuaciones de fiscalización están a cargo de la Dirección de Fiscalización e Instrucción, unidad orgánica de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, y tienen una duración de 90 días hábiles, plazo que puede ser ampliado por única vez hasta un periodo de 45 días hábiles, dependiendo de la complejidad del caso[2].

La fiscalización puede comprender visitas de fiscalización como revisión de documentos[3]. Es preciso señalar que de acuerdo con el artículo 101 del Reglamento de la LPDP, el personal fiscalizador está dotado de fe pública en el ejercicio de sus funciones.

Asimismo, es preciso señalar que, de acuerdo con el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 007-2017-JUS, los fiscalizadores están facultados para:

---

[1] **Artículo 37. Procedimiento sancionador**
El procedimiento sancionador se inicia de oficio, por la Autoridad Nacional de Protección de Datos Personales o por denuncia de parte, ante la presunta comisión de actos contrarios a lo dispuesto en la presente Ley o en su reglamento, sin perjuicio del procedimiento seguido en el marco de lo dispuesto en el artículo 24.
Las resoluciones de la Autoridad Nacional de Protección de Datos Personales agotan la vía administrativa. Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.

[2] **Artículo 105.- Desarrollo de la fiscalización**
El procedimiento de fiscalización tendrá una duración máxima de noventa (90) días, este plazo corre desde la fecha en que la Dirección de Supervisión y Control recibe la denuncia o da inicio de oficio al procedimiento y concluirá con el informe que se pronunciará sobre la existencia de elementos que sostengan o no, la presunta comisión de infracciones previstas en la Ley.
El plazo establecido podrá ser ampliado por una vez y hasta por un periodo de cuarenta y cinco (45) días, por decisión motivada, atendiendo a la complejidad de la materia fiscalizada y con conocimiento del Director General de Protección de Datos Personales.

[3] **Artículo 106.- Programa de visitas.**
La fiscalización podrá incluir diversas visitas para obtener los elementos de convicción necesarios, las cuales se desarrollarán con un plazo máximo de diez (10) días entre cada una. Luego de la primera visita, se notificará un programa de visitas al titular del banco de datos personales o al encargado o al responsable del tratamiento y, en su caso, al denunciante.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

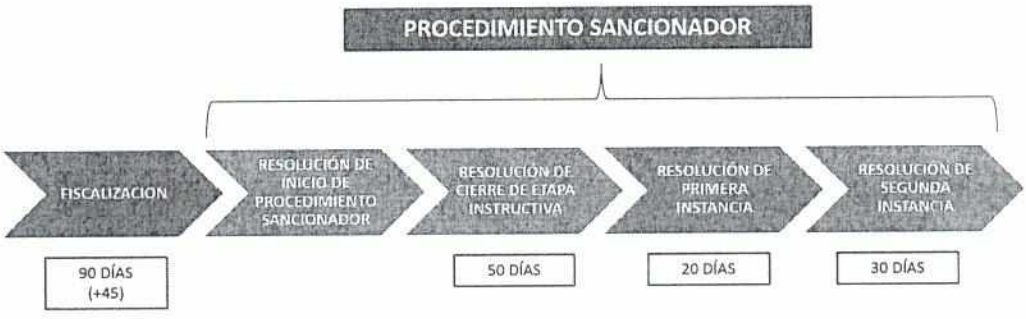
- Requerir al administrado objeto de la fiscalización, la exhibición o presentación de todo tipo de documentación, expedientes, archivos u otra información necesaria, respetando el principio de legalidad.
- Interrogar a las personas materia de fiscalización o a sus representantes, empleados, funcionarios, asesores y a terceros utilizando los medios técnicos que considere necesarios para generar un registro completo y fidedigno de sus declaraciones.
- Realizar inspecciones, con o sin previa notificación, en los locales y/o bienes de las personas naturales o jurídicas objeto de las acciones de fiscalización, respetando el derecho fundamental a la inviolabilidad de domicilio cuando corresponda.
- Tomar copia de los archivos físicos, ópticos, electrónicos y otros, así como tomar fotografías, realizar impresiones, grabaciones de audio o en video con conocimiento previo del administrado y, en general, utilizar los medios necesarios para generar un registro completo y fidedigno de su acción de fiscalización.
- Realizar exámenes periciales sobre la documentación y otros aspectos técnicos relacionados con la fiscalización.
- Utilizar en las acciones y diligencias de fiscalización equipos que consideren necesario.
- Ampliar o variar el objeto de la acción de fiscalización en caso de que, como resultado de las acciones y diligencias realizadas se detecten incumplimientos adicionales a los expresados en el referido objeto.

La fiscalización en materia de protección de datos personales culmina con un informe que indica si existen o no indicios de actos contrarios a la LPDP y su reglamento. De acuerdo con el artículo 113 del Reglamento de la LPDP, dicho informe determina con carácter preliminar las circunstancias que justifiquen la instauración del procedimiento sancionador o la ausencia de ellas. De ser el caso, se establecerán las medidas que deberá ordenarse al presunto responsable, en vía cautelar. La determinación de la presunta responsabilidad contenida será notificada al fiscalizado y al denunciante, de ser el caso, en un plazo que no excederá de cinco (5) días.

En atención a dicho informe se resolverá iniciar o no un procedimiento sancionador, cuya etapa de instrucción está a cargo de la Dirección de Fiscalización e Instrucción, y tiene una duración de cincuenta (50) días contados desde el inicio del procedimiento.

Finalmente, la Dirección de Protección de Datos Personales resolverá en primera instancia si se han cometido infracciones e impondrá las multas coercitivas correspondientes.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.



De acuerdo con el artículo 39 de la LPDP, la Autoridad Nacional de Protección de Datos Personales puede imponer a los infractores multas que van de 0,5 a 100 UIT, clasificando las infracciones en leves, graves y muy graves.

Resulta necesario resaltar que la LPDP y su Reglamento no otorgan a la APDP, en el marco de una fiscalización, otro tipo de facultades como:

- Clausurar locales.
- Decomisar soportes que contengan datos personales.
- Cancelar licencias de funcionamiento.
- Emitir y ejecutar órdenes de captura.
- Hacer uso de la fuerza.
- Cualquier otra medida que limite algún derecho fundamental.

V. Fiscalizaciones realizadas por la APDP

Con la finalidad de velar por el derecho a la protección de datos personales, la APDP realiza desde setiembre del año 2014 fiscalizaciones de oficio o por denuncia a entidades públicas y privadas de diversos rubros económicos.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

El asunto sobre el cual la Comisión de Defensa Nacional, Orden Interno, Desarrollo Alternativo y Lucha Contra las Drogas del Congreso de la República ha requerido información está relacionado con el uso de datos personales tales como los nombres, direcciones, teléfonos, e información financiera de los ciudadanos, obtenidos ilícitamente que son comercializados en mercados clandestinos, debido, presuntamente a faltas de medidas de seguridad de las empresas que son titulares de dichos bancos de datos.

Al respecto, la APDP incluye en las fiscalizaciones realizadas el cumplimiento de las medidas de seguridad establecidas en los artículos 39 al 46 del Reglamento, tanto respecto a tratamientos automatizados como no automatizados.

En ese marco, entre el año 2014 y el 29 de diciembre de 2017, la APDP ha realizado las siguientes fiscalizaciones para verificar el cumplimiento o incumplimiento de las disposiciones sobre protección de datos personales:

Fiscalizaciones realizadas					
Estado	**2014**	**2015**	**2016**	**2017**	**Total**
Iniciadas	85	74	90	112	**361**
Concluidas	10	137	65	86	**298**
Visitas	80	122	129	200	**531**

Las fiscalizaciones incluyen la solicitud y revisión de documentos como visitas de fiscalización a las diversas sedes de las entidades fiscalizadas, por lo que una fiscalización puede incluir más de una visita.

VI. Otras medidas adoptadas

Respecto a la erradicación de la venta ilegal de bases de datos, así como de cualquier otra acción en materia de tratamiento inadecuado de datos personales, la Autoridad Nacional ha realizado las siguientes acciones:

1. Firma de compromisos públicos para la protección de datos personales. Esta estrategia tiene como objetivo informar a los sujetos obligados sobre sus responsabilidades en materia de protección de datos personales y comprometerlos a tomar o fortalecer las medidas de protección.

   A la fecha se han firmado 4 compromisos públicos para la protección de datos personales:

   1. Empresas de taxi por aplicativo,
   2. Entidades que prestan servicios de salud,
   3. Entidades públicas y
   4. Centrales privadas de información.

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
M. PEÑA N.

2. Atención de consultas en materia de tratamiento de datos personales (e-mail, teléfono y presencial):

2014	2015	2016	2017
822	1920	1836	1172

VII. Visita de Fiscalización a mercado ilícito de datos en la avenida Wilson

Con fecha 29 de octubre del presente se emitió un reportaje periodístico en el que se informaba sobre la venta ilegal de bancos de datos personales en

establecimientos ubicados en la avenida Wilson, advirtiéndose entre ellos al establecimiento ubicado en Av. Garcilaso de la Vega N° 1268, Cercado de Lima.

Con fecha 07 de noviembre de 2017 se emitió la Orden de Visita de Fiscalización N° 056-2017-JUS/DGTAIPD-DFI, dirigida a fiscalizar el local ubicado en Av. Garcilaso de la Vega N° 1268, Cercado de Lima.

En la misma fecha el equipo fiscalizador (conformado por un abogado y un ingeniero de sistemas) se apersonó al local ubicado en Av. Garcilaso de la Vega N° 1268, Cercado de Lima a fin de levantar un Acta de Visita de fiscalización.

Es preciso señalar que, si bien la Dirección de Fiscalización e Instrucción tiene entre sus funciones fiscalizar, de oficio o de parte, los presuntos actos contrarios a lo establecido en la LPDP y su Reglamento, de iniciarse un procedimiento de fiscalización conforme a lo establecido en los artículos 99, 105, 106, 107, 108, 109, 110 del Reglamento de la LPDP, que concluya que existen indicios de infracción, la Autoridad tiene la potestad de imponer multas por infracción a las disposiciones sobre protección de datos personales, en el marco de un procedimiento administrativo sancionador, pero no tiene competencia para investigar ni sancionar la comisión de delitos.

El 09 de noviembre de 2017, se emitió el Informe N° 015-2017-JUS/DFI-KAT, informe sobre la visita de fiscalización al local ubicado en Av. Garcilaso de la Vega N° 1268, Cercado de Lima, en el cual se concluyó que existen indicios de la comisión del delito de tráfico ilegal de datos personales, por lo que es necesaria la intervención del Ministerio Público.

En ese marco, el 29 de diciembre de 2017, mediante el Oficio N° 290-2017-JUS/DGTAIPD-DFI, se remitió a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú el mencionado informe para que realice las actuaciones correspondientes.

VIII. Delito de Tráfico Ilícito de Datos Personales

PERÚ Ministerio de Justicia y Derechos Humanos
Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
PEÑA N.

El Código Penal tipifica el delito de tráfico ilícito de datos personales en el artículo 154-A, de la siguiente manera:

> ***Artículo 154-A. Tráfico ilegal de datos personales***
> *El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.*
> *Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior."*

Como se puede apreciar, la venta de bases de datos, que contienen datos personales, sin el consentimiento de sus titulares y de forma ilegítima, constituye un delito, que debe ser perseguido por el Ministerio Público como titular de la acción penal.

Por ello, una adecuada fiscalización de cara a la erradicación del mercado ilícito de banco de datos personales requiere el trabajo conjunto de otras instituciones como la Policía Nacional del Perú y el Ministerio Público.

IX. Temas en agenda

Con la finalidad de proteger los datos personales y de prevenir el delito de tráfico ilícito de bases de datos personales, la Autoridad Nacional de Protección de Datos Personales tiene planificado realizar las siguientes acciones en corto plazo:

- Continuar la fiscalización a entidades públicas y privadas respecto al cumplimiento de medidas de seguridad y principio de confidencialidad.
- Continuar con las charlas informativas a las instituciones públicas y privadas sobre las obligaciones en materia de protección de datos personales, enfatizando en la implementación de medidas de seguridad.

X. Conclusiones:

1. Con la vigencia del Decreto Legislativo No. 1353 y su reglamento, y el nuevo Reglamento de Organización y Funciones del MINJUS, aprobado en junio de 2017, mediante el Decreto Supremo N° 013-2017-JUS, se crea la Dirección General de Transparencia, Acceso a la Justicia y Protección de Datos Personales, que depende jerárquicamente del Viceministerio de Justicia. Hasta junio de 2017, las funciones de la APDP eran ejercidas por la Dirección General de Protección de Datos Personales, que pertenecía al Viceministerio de Derechos Humanos y Acceso a la Justicia.

2. La Dirección General de Transparencia, Acceso a la Justicia y Protección de Datos Personales es el órgano de línea que ejerce las funciones de la Autoridad Nacional de Protección de Datos Personales, como de la nueva Autoridad Nacional de Transparencia y Acceso a la Información Pública, creada mediante el Decreto Legislativo N° 1353, vigente desde el 15 de setiembre del presente.

3. De acuerdo con el artículo 33 de la LPDP, la APDP ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.

4. En ejercicio de su función sancionadora, la Autoridad Nacional de Protección de Datos Personales puede imponer a los infractores multas que van de 0,5 a 100 UIT, clasificando las infracciones en leves, graves y muy graves.

5. La LPDP y su Reglamento no permiten a la Autoridad Nacional de Protección de Datos Personales realizar de acciones como: clausurar locales, decomisar soportes que contengan datos personales; cancelar licencias de funcionamiento; emitir y ejecutar órdenes de captura; hacer uso de la fuerza o cualquier otra medida que limite algún derecho fundamental.

6. El asunto sobre el cual se ha requerido información está relacionado con el uso de datos personales relacionados con los nombres, direcciones, teléfonos, e información financiera de los ciudadanos, obtenidos ilícitamente que son comercializados en mercados clandestinos debido, presuntamente, a faltas de medidas de seguridad de las empresas que son titulares de dichos bancos de datos.

7. Debemos señalar que la Autoridad Nacional de Protección de Datos Personales, respecto a dicha materia, desde su creación, ha realizado 298 fiscalizaciones a entidades públicas y privadas, respecto a sus obligaciones en materia de protección de datos personales.

8. El 07 de noviembre de 2017 el equipo fiscalizador de la Dirección General se apersonó al local ubicado en Av. Garcilaso de la Vega N° 1268, Cercado de Lima para fiscalizar el tratamiento de datos personales. Sin embargo, al estar frente a la posible comisión de un delito, se remitió la información a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú.

9. Finalmente, cabe destacar, que la Autoridad Nacional de Protección de Datos Personales tiene planificado, en corto plazo, continuar la fiscalización a entidades públicas y privadas respecto al cumplimiento de medidas de seguridad y principio de confidencialidad; y continuar con las charlas informativas a las instituciones públicas y privadas sobre las obligaciones en materia de protección de datos personales, enfatizando en la implementación de medidas de seguridad.

Atentamente,

Miriam Isabel Peña Niño
Directora General (e) de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
Ministerio de Justicia y Derechos Humanos