FACULTAD DE DERECHO

La obtención del consentimiento y el cumplimiento del Deber de Información en el tratamiento de los Datos Personales en el Perú

Trabajo de Suficiencia Profesional para optar el Título de Abogado

Macarena Sara María del Busto Calosi

Revisor(es):
Dr. Carlos Guillermo Hakansson Nieto

Lima, noviembre de 2022

NOMBRE DEL TRABAJO

La obtención del consentimiento y el cumplimiento

AUTOR

Macarena Del Busto

RECUENTO DE PALABRAS

20462 Words

RECUENTO DE CARACTERES

114357 Characters

RECUENTO DE PÁGINAS

76 Pages

TAMAÑO DEL ARCHIVO

715.2KB

FECHA DE ENTREGA

Oct 25, 2022 9:38 AM GMT-5

FECHA DEL INFORME

Oct 25, 2022 9:53 AM GMT-5

4% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

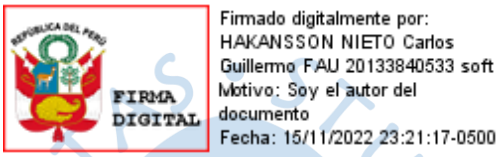
- 4% Base de datos de Internet
- Base de datos de Crossref
- 1% Base de datos de trabajos entregados
- 0% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Bloques de texto excluidos manualmente
- Material citado
- Coincidencia baja (menos de 10 palabras)

Aprobación

El trabajo de suficiencia profesional titulado "*La obtención del consentimiento y el cumplimiento del Deber de Información en el tratamiento de los Datos Personales en el Perú"*; presentada por Macarena Sara María del Busto Calosi, en cumplimiento con los requisitos para optar el título de Abogado, fue aprobada por el Director, Dr. Carlos Guillermo Hakansson Nieto.



Director de Trabajo de Suficiencia Profesional

UNIVERSITAS STUDIORUM PIURENSIS

Dedicatoria

Para mi angelito en el cielo, espero te sientas orgullosa de mí; y para mi gran amiga Fiorella, quien me alentó desde el inicio para culminar esta importante etapa académica.

UNIVERSITAS STUDIORUM PIURENSIS

Agradecimientos

Quiero darle un especial agradecimiento al Dr. Carlos Guillermo Hakansson Nieto, por el apoyo y la buena disposición en dedicarme su tiempo para conversar y orientarme en el desarrollo de este documento.

Me siento afortunada de haberlo podido tener como asesor, no solo por ser un impecable profesional; sino también por la calidad de persona que es. Su disciplina, cariño y empuje fueron determinantes para concluir el presente trabajo de suficiencia profesional.

UNIVERSITAS STUDIORUM PIURENSIS

Resumen

En el presente trabajo de suficiencia profesional se expone sobre los retos que tuvo que enfrentar estando a cargo del área de Protección de Datos Personales del Estudio Lazo & de Romaña Abogados, debiendo implementar las exigencias contempladas en la normativa en distintas empresas respecto de las cuales brindaba asesoría jurídica. Ello, tomando en consideración que la presente regulación es transversal a todas las industrias, en la medida que efectúen tratamiento de datos personales.

La metodología del trabajo se ha basado en un método descriptivo y analítico. Mientras que, en el desarrollo se detallan: (i) los principales cuestionamientos que se generaron sobre el deber de solicitar el consentimiento y el cumplimiento del deber de información, (ii) el análisis realizado para resolver dichos cuestionamientos y, (iii) algunas dificultades que aún persisten en el contexto de la revolución tecnológica que como sociedad estamos viviendo.

Como resultado, la autora, como líder del área de Protección de Datos Personales del Estudio Lazo & De Romaña Abogados, efectuó la adecuación de diversas empresas -atendiendo a los rubros a los que se dedicaban y el tratamiento de información personal que realizaban-, a las exigencias establecidas en la normativa en materia de protección de datos personales; interpretando adecuadamente la misma y ejecutando acciones para superar la problemática en relación a la aplicación y cumplimiento del deber de consentimiento y de información evitando, de este modo, que las empresas bajo su asesoría incurran en infracciones y sean sancionadas por la Autoridad de Protección de Datos Personales.

UNIVERSITAS STUDIORUM PIURENSIS

Tabla de contenido

Lista de figuras

UNIVERSITAS STUDIORUM PIURENSIS

Introducción

El presente trabajo de suficiencia profesional tiene como objetivo reflejar el conocimiento adquirido por la informante sobre la regulación de protección de datos personales, el cual le ha permitido poder absolver los principales cuestionamientos por parte de diversas instituciones del sector privado sobre la interpretación o sentido de la normativa, así como su aplicación práctica. Ello, tomando en consideración que la totalidad de disposiciones de la normativa de protección de datos personales entraron en plena vigencia en el año 2015 siendo precisamente, desde dicho año hasta la fecha, donde la informante se ha desempeñado como asesora legal especializada en protección de datos personales de diversas empresas del sector privado dedicadas a distintos rubros tales como alimentos y bebidas, construcción, educación, salud y bienestar, servicios financieros, hotelería y turismo, etc. Asimismo, tomando en consideración la experiencia en esta materia, la informante realiza algunas reflexiones sobre posibles limitaciones que aún presentaría la normativa sobre la utilización de la información personal en el contexto de la revolución tecnológica que estamos viviendo.

Tomando en consideración lo expuesto, el presente trabajo se estructura en cuatro (4) capítulos. El primer capítulo contempla la experiencia profesional de la informante desde su egreso de la Universidad de Piura.

El segundo capítulo aproxima al lector a la normativa en materia de protección de datos personales; en ese sentido se describe el marco normativo legal peruano en la protección de los datos personales y su evolución en estos últimos 11 años. Asimismo, se presentan los conceptos básicos contemplados en la normativa aplicable.

En el tercer capítulo se indican las principales interrogantes planteadas a la informante respecto a la obtención del consentimiento y el cumplimiento del deber de información; consideradas las piedras angulares de la protección de datos en el Perú; ello tomando en cuenta que la entrada en vigor de la normativa exigió a las empresas -entre otros- que trataban datos personales, adecuarse a las obligaciones previstas en la misma. Por lo demás, en este capítulo se brindan las respuestas a las interrogantes planteadas en base al análisis normativo efectuado por la informante, despejándose la incertidumbre existente con relación al cumplimiento de la normativa en los aspectos descritos. Cabe señalar que el análisis realizado tuvo como consecuencia que las empresas que estuvieron bajo la asesoría de la informante no incurrieran en infracciones a lo previsto en la normativa y, por lo tanto, no sean sancionadas por la Autoridad de Protección de Datos Personales.

Finalmente, el capítulo cuatro contiene algunas reflexiones de la informante sobre ciertas dificultades que a su criterio aún persistirían en el contexto de la nueva era digital en la que nos encontramos y la aplicación del test de incompatibilidad que podría -en determinados casos- ayudar a superar algunas dificultades vinculadas al tratamiento de información en proyectos de *Big Data*.

Capítulo 1

Información académica y profesional de la informante

1.1 Formación académica

La informante inició sus estudios en el año 2008, ingresando a la Facultad de Derecho campus Piura. En el año 2011 hizo su traslado a campus Lima, egresando de la universidad en el primer semestre del año 2015. Obtuvo el grado de bachiller en el año 2017.

En la etapa profesional, en el año 2018, la informante llevó un curso internacional de especialización sobre la protección de datos personales en la Universidad del Pacífico Business School, obteniendo la certificación como "Experto Certificado en Protección de Datos Personales", el cual es expedido por el Institute of Audit & IT - Governance (IAITG); lo cual, le permitió afianzar sus conocimientos en la presente materia.

1.2 Experiencia preprofesional

La informante inició sus primeras prácticas en diciembre del año 2011 hasta diciembre del año 2012 en el Estudio Miranda & Amado Abogados, en el área de Litigios. Durante ese lapso, el área se encontraba liderada por el Dr. Juan Luis Avendaño Valdéz y el Dr. Mauricio Raffo La Rosa.

Dicha experiencia le permitió a la informante involucrarse en procesos en todas las instancias del Poder Judicial, desde los juzgados hasta la Corte Suprema; así como el Tribunal Constitucional en todos los procesos constitucionales, especialmente en procesos de amparo. La informante también participó en la elaboración de estrategias procesales, así como en el acompañamiento durante la tramitación de procesos judiciales en materia contencioso administrativa, civil, entre otras.

En julio del año 2014, la informante inició su segundo periodo de prácticas en el Estudio Lazo, De Romaña & Gagliuffi Abogados (denominado así en ese entonces) en el área de Competencia y Protección al Consumidor. Durante ese periodo, el área se encontraba liderada por el Dr. Ivo Gagliuffi Piercecchi y el Dr. Luis Miguel León Luna.

En dicho periodo, la informante adquirió experiencia en aspectos analíticos como regulatorios referidos a la protección al consumidor y derecho de la competencia, aprendiendo sobre una amplia gama de actividades económicas tales como servicios financieros, farmaceúticos, *retail*, educación, construcción, entre otros.

1.3 Experiencia profesional

En julio de 2015, la informante egresó de la universidad, siendo contratada por el estudio de abogados donde laboraba como Asociada Junior en el área de Competencia y Protección al Consumidor, la cual estaba compuesta por las siguientes especialidades: libre competencia, competencia desleal, protección al consumidor, publicidad y barreras burocráticas.

Las principales funciones que desempeñó la informante fueron las siguientes:

- Defensa a importantes compañías del sector privado en procedimientos por infracciones a las normas de competencia desleal, libre competencia, publicidad y protección al consumidor.
- Asesoría en denuncias contra entidades públicas por imposición de barreras burocráticas.
- Implementación de programas de cumplimiento en materia de protección al consumidor y competencia desleal y libre competencia.
- Revisión de material publicitario con la finalidad de prevenir cualquier posible incumplimiento a las normas de publicidad comercial y competencia desleal.
- Revisión de contratos de consumo con la finalidad de verificar el cumplimiento de las normas de protección al consumidor.
- Asistencia a audiencias de conciliación ante el Indecopi en el marco de procedimientos administrativos de protección al consumidor y a nivel de reclamos.
- Capacitación de directivos y colaboradores de distintas empresas sobre el cumplimiento de la legislación y evitar contingencias legales.

A continuación, se detallan los principales clientes atendidos por la informante:

- Pacífico Compañía de Seguros y Reaseguros S.A.
- La Positiva Seguros y Reaseguros S.A.
- Seguros Sura S.A.
- BNP Paribas Cardif S.A.
- Protecta S.A. Compañía de Seguros
- Empresa Editora el Comercio S.A.
- Inchcape Motors Perú S.A e Inchcape Latam Perú S.A.
- Supermercados Peruanos S.A.
- BBVA Banco Continental
- Banco Internacional del Perú S.A.A (Interbank)

- Banco Azteca del Perú S.A.
- Constructora Galilea S.A.C.
- Grupo Inmobiliario Imagina
- Librerías Crisol S.A.C
- Corporación Lindley S.A.
- Promotora Miraflores S.A.C ("Le Cordon Bleu")
- Bayer S.A.
- Pagosonline Perú SAC (PAYU)
- Inversiones Centenario S.A.
- Procter & Gamble Perú S.R.L
- Toyota del Perú

En el año 2016, la informante -adicionalmente a sus labores como parte del área de Competencia y Protección al Consumidor-, ingresó al área de Protección de Datos Personales; siendo promovida en el año 2019 como Asociada Senior y jefa del área de Protección de Datos Personales.

Las principales funciones que desempeñó la informante fueron las siguientes:

- Asesoría integral en temas de privacidad y cumplimiento de las normas de protección de datos personales.
- Revisión de contratos vinculados a transferencias internacionales de datos personales.
- Auditorias de cumplimiento para revisar la correcta implementación de políticas de privacidad y medidas de seguridad.
- Patrocinio en procedimientos administrativos sancionadores iniciados por la Autoridad de Protección de Datos Personales.
- Capacitación de directivos y colaboradores de distintas empresas para asegurar el correcto cumplimiento de la normativa.

A continuación, se detallan los principales clientes atendidos por la informante:

- GSP Servicios Generales S.A.C - Auna
- Especialidades Médicas S.A.
- Great Retail S.A.C. (Tiendas Tambo y Tiendas Aruma)
- Grupo Patio S.A.C
- Mediterranean Shipping Company
- Inchcape Motors Perú S.A e Inchcape Latam Perú S.A.

- Derco Perú S.A
- Fresenius Kabi Perú S.A.
- T Gestiona S.A.C.
- Banco Santander Perú S.A.
- Grupo Inmobiliario Imagina
- Grupo Inmobiliario Markagroup S.A.C.
- Cemex Perú S.A.
- Nessus Hoteles Perú S.A (Casa Andina)

La informante laboró hasta diciembre del año 2021 en el Estudio Lazo & De Romaña Abogados. A partir de enero de 2022, ha prestado asesorías jurídicas de forma independiente.

Capítulo 2

El derecho constitucional a la autodeterminación informativa y su regulación en el Perú

2.1 Marco normativo de la protección de datos personales en el Perú

En el ordenamiento jurídico peruano, el derecho a la protección de los datos personales encuentra su fundamento en la Constitución Política del Perú del año 1993. Es así como, el numeral 6 del artículo 2° consagra el derecho fundamental a la autodeterminación informativa; señalando expresamente que toda persona tiene derecho "a que los servicios informáticos, computarizados o no, públicos y privados, no suministren informaciones que afecten la intimidad personal y familiar".

Cabe señalar que si bien la disposición constitucional no menciona expresamente que toda persona tiene el derecho fundamental a la "autodeterminación informativa", el Nuevo Código Procesal Constitucional, aprobado por la Ley N° 31307, vigente desde el 24 de julio de 2021, complementa lo previsto en el referido texto constitucional, indicando su artículo 59° que el hábeas data procede en defensa del derecho de la autodeterminación informativa, enunciando las modalidades bajo las cuales puede ser invocado[1]. Así, se puede advertir que

[1] "Artículo 59 del Nuevo Código Procesal Constitucional: el habeas data procede en defensa del derecho de acceso a la información pública reconocido en el inciso 5 del artículo 2 de la Constitución. También procede en defensa del derecho a la autodeterminación informativa, enunciativamente, bajo las siguientes modalidades:

1) Reparar agresiones contra la manipulación de datos personalísimos almacenados en bancos de información computarizados o no.
2) A conocer y supervisar la forma en que la información personal viene siendo utilizada.
3) A conocer el contenido de la información personal que se almacena en el banco de datos.
4) A conocer el nombre de la persona que proporcionó el dato.
5) A esclarecer los motivos que han llevado a la creación de la base de datos.
6) A conocer el lugar donde se almacena el dato, con la finalidad de que la persona pueda ejercer su derecho.
7) A modificar la información contenida en el banco de datos, si se trata de información falsa, desactualizada o imprecisa.
8) A incorporar en el banco de datos información que tengan como finalidad adicionar una información cierta pero que por el transcurso del tiempo ha sufrido modificaciones.
9) A incorporar información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado.
10) A incorporar al banco de datos una información omitida que perjudica a la persona.
11) A eliminar de los bancos de datos información sensible que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona.
12) A impedir que las personas no autorizadas accedan a una información que ha sido calificada como reservada.
13) A que el dato se guarde bajo un código que solo pueda ser descifrado por quien está autorizado para hacerlo.
14) A impedir la manipulación o publicación del dato en el marco de un proceso, con la finalidad de asegurar la eficacia del derecho a protegerse.

dicho código concreta el contenido del derecho a la autodeterminación informativa, especificando las facultades o tributos que forman parte del mismo.

Asimismo, el Tribunal Constitucional reconoce el derecho a la autodeterminación informativa; indicando que "El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos".[2]

En este contexto y luego de dieciocho (18) años de consagrado este derecho de autodeterminación informativa en la Constitución, su desarrollo y regulación sería alcanzado con la aprobación de la Ley Nº29733, Ley de Protección de Datos Personales[3] (en adelante, "LPDP"), la cual, según lo mencionado en su artículo 1°, tiene como objeto garantizar el derecho fundamental a la protección de los datos personales, respetando los demás derechos fundamentales reconocidos en la Constitución[4]; ello en la medida que toda persona natural tiene derecho a mantener el control de su información personal y definir el acceso que le puede brindar a terceros respecto de esta.

Ahora bien, casi dos (2) años después de publicada la LPDP, se publicó su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, el cual según lo expresado en su artículo 1° tiene como objeto "garantizar el derecho fundamental a la protección de los datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado".

Cabe señalar que el citado reglamento dispuso en su primera disposición complementaria transitoria que aquellos que realizaban tratamiento de datos personales tenían el plazo de dos (2) años desde su entrada en vigor, para adecuarse a sus obligaciones y a las establecidas en la LPDP. Es así como, desde el 08 de mayo de 2015, la Autoridad Nacional de Protección de Datos Personales (ANPDP) fiscaliza su cumplimiento a efectos de garantizar el respeto de las normas en materia de protección de datos personales.

---

15) A solicitar el control técnico con la finalidad de determinar si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.
16) A impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada".

[2] EXP. N° 4739-PHD/TC, fundamento 2.

[3] Publicada en el Diario Oficial El Peruano el 03 de julio de 2011, cuya vigencia inició el 04 de julio de 2011.

[4] Artículo 1º de la LPDP: "La presente Ley tiene 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".

Ahora bien, en el año 2017 se vio la necesidad de aprobar el Decreto Legislativo Nº 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública; fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses (en adelante, DL 1353), realizándose algunas modificaciones a la LPDP.

Sobre el particular, de acuerdo con lo expresado en la exposición de motivos del DL 1353[5], el objetivo de esta norma es reforzar el ejercicio de los dos derechos fundamentales reconocidos en nuestra Constitución: el derecho al acceso a la información pública y el derecho a la protección de datos personales.

Cabe indicar que de la lectura de la citada exposición de motivos se aprecia que el desarrollo de la misma se centra en explicar el motivo por el cual resulta importante contar con una Autoridad que supervise las normas en materia de transparencia y acceso a la información pública; buscando "solucionar el problema de la falta de unidad en los lineamientos institucionales en materia de acceso y transparencia de la información pública"[6]; sin embargo no se hace mayor mención a los cambios en la LPDP y la justificación de los mismos[7], lo cual puede generar cierta incertidumbre y/o especulación sobre los motivos en virtud de los cuales se realizaron algunas modificaciones a la normativa.

Ahora bien, desde el año 2017 hasta aproximadamente mediados del año 2021, la normativa de protección de datos personales no ha sido objeto de cambios regulatorios. No obstante, el año pasado -específicamente el 10 de junio de 2021-, se aprobó en Comisión de Justicia y Derechos Humanos el Proyecto de Ley N°7870/2020[8] que crea la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos

---

[5] Exposición de Motivos del Decreto Legislativo N°1353. Recuperado de https://www.congreso.gob.pe/Docs/comisiones2016/ConstitucionReglamento/files/dl_1353_(1).pdf

[6] Ídem, p. 14.

[7] Al respecto, el DL 1353 propuso diversos cambios tales como: (i) establecer nuevas definiciones: encargado de tratamiento de datos personales y encargo de tratamiento. Cabe señalar que antes la LPDP solo contemplaba la definición de encargado del banco de datos; (ii) establecer la obligación de informar a los titulares de los datos personales en caso haya un nuevo encargado del tratamiento con posterioridad a la obtención del consentimiento; (iii) incorporar algunos supuestos en los cuales no se requerirá el consentimiento del titular de los datos personales para tratar sus datos personales; tales como finalidades vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo; para la preparación o celebración de una relación contractual (antes de la modificación solo se contemplaba la ejecución de la relación contractual); cuando el tratamiento se realiza en ejercicio del derecho fundamental a la libertad de expresión; (iv) atribuir las obligaciones que le correspondían al "encargado del banco de datos" al ahora "encargado del tratamiento de los datos personales", entre otras.

[8] Proyecto de Ley N° 7870/ 2020-PE; Proyecto de ley que crea la Autoridad Nacional Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/1939689/OFICIO%20N°%20337-2021-PR.pdf.pdf

Personales. Así, respecto a la LPDP, el mencionado proyecto buscaría fortalecer el derecho a la protección de datos personales[9]; realizándose modificaciones e incorporaciones a la ley.

Asimismo, el referido proyecto de ley propone la creación de la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (ANTAIPDP); siendo que su creación respondería a la necesidad de contar con una entidad rectora que se constituya como una autoridad técnico-normativa a nivel nacional, con capacidad de afrontar con mayor eficacia las funciones estatales en materia de transparencia, acceso a la información pública y protección de datos personales; generando de este modo una institución que promueva una unidad en la interpretación de normas; predictibilidad de las decisiones de la administración pública y seguridad jurídica.

Sobre este punto, debemos precisar que actualmente contamos con: (a) la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, la cual depende jerárquicamente del despacho viceministerial del Ministerio de Justicia y Derechos Humanos, y es la encargada de ejercer: (i) la ANPDP (que incluye a su vez a: la Dirección de Protección de Datos Personales y a la Dirección de Fiscalización e Instrucción) y (ii) la Autoridad Nacional de Transparencia y Acceso a la Información Pública "ANTAIP" (conformada por la Dirección de Transparencia y Acceso a la Información); y, (b) el Tribunal de Transparencia y Acceso a la Información Pública "TTAIP".

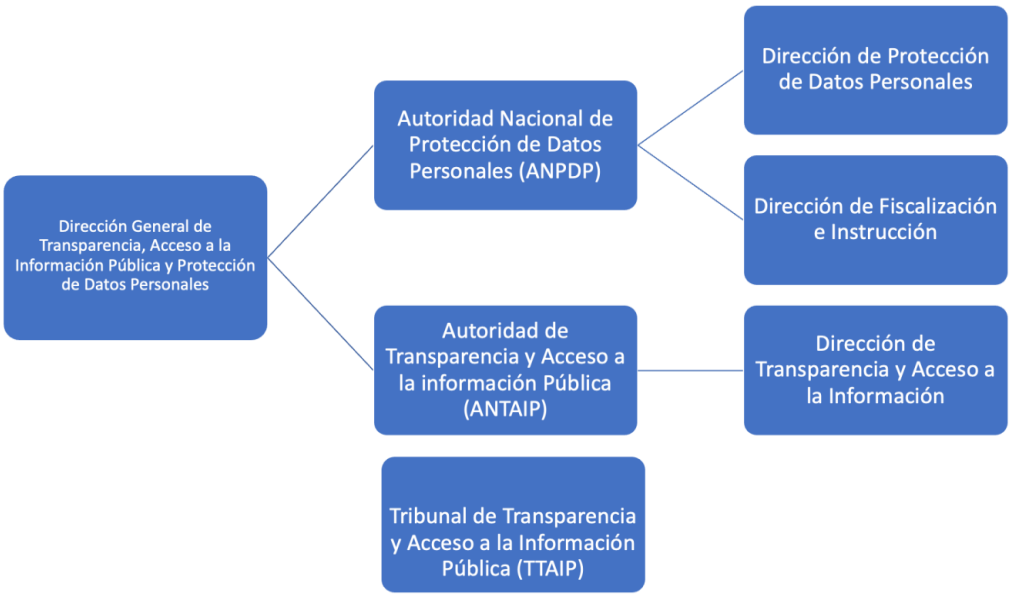
Sin embargo, como se puede evidenciar la existencia de tres actores: la ANPDP, la ANTAIP y el TTAIP, que conocen estas materias y se pronuncian de forma independiente, ha generado ciertas discrepancias sobre criterios que finalmente se encuentran vinculados, por lo que se propone la creación de la mencionada ANTAIPDP, con el objetivo de superar esta situación.

Para mayor compresión, a continuación, se presenta el organigrama de la conformación actual de la Autoridad de Datos Personales y de Transparencia:

[9] Al respecto, el Proyecto de Ley N°7870/2020 propone entre otros: (i) agregar definiciones tales como Oficial de Datos Personales; Incidente de seguridad de datos personales; Nivel suficiente de protección para los datos personales; (ii) reportar a la Autoridad los incidentes de seguridad que afecten los datos personales; (iii) obligación de designar a un Oficial de Datos Personales; (iv) regulación del derecho a la portabilidad de los datos personales; entre otras.

Figura 1.

Organigrama de la Autoridad de Datos Personales y de Transparencia



Nota. Adaptado de *Organización. Autoridad Nacional de Protección de Datos Personales*, de Perú. Ministerio de Justicia y Derechos Humanos, 2022, https://www.gob.pe/institucion/anpd/organizacion

Si bien el citado proyecto de ley aún se encuentra en evaluación; el mismo refleja la constante preocupación por fortalecer la normativa en materia de protección de datos personales y así proteger de forma más efectiva a las personas frente al uso indebido de su información personal. Ello, en el contexto que vivimos de la denominada "sociedad de la información", donde el uso de las tecnologías de la información y comunicación (TICs) se han implementado y adaptado a nuestro estilo de vida, entregándose millones de datos de forma diaria a una gran velocidad y facilidad para promover la adquisición de productos y/o servicios.

En ese sentido, se puede decir que hoy "cualquier ser humano puede acumular, sin mayor esfuerzo, un conocimiento detallado sobre miles de otros seres humanos en sus horas libres. Con cuánta mayor razón no acumulará sobre ellos alguien que se especialice en la tarea que, inclusive, la vea como un negocio potencial: acumula información y luego la vende como servicio".[10]

[10] RUBIO, Marcial y otros. *Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional: análisis de los artículos 1,2 y 3 de la Constitución.* Fondo Editorial de la Pontificia Universidad Católica del Perú, Lima, 2003; pp. 312-313.

Como se puede advertir, si bien el uso de las TICs supone una evolución y desarrollo, también conlleva desventajas y/o nuevos problemas que surgen con su uso; vinculado al flujo masivo de información personal que implican.

Ante dichas potenciales amenazas vinculadas a la obtención, procesamiento y transmisión de ilimitadas cantidades de datos personales; la LPDP y su Reglamento procuran proteger el derecho fundamental a la autodeterminación informativa mediante un adecuado tratamiento de los datos personales, haciendo frente a cualquier agresión que pueda producirse contra la persona humana por su uso extralimitado e indebido.

En este contexto y tomando en consideración que en el presente punto se ha descrito el marco normativo en nuestro país sobre la protección de los datos personales, a continuación, se procederá a presentar los conceptos básicos contemplados en la normativa aplicable.

2.2 ¿Qué son los datos personales?

Sobre el particular, de acuerdo a lo mencionado en el numeral 4 del artículo 2° de la LPDP, los datos personales son "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados". En este sentido, el Reglamento de la LPDP, complementa la referida definición estableciendo en su numeral 4 del artículo 2° que es "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados".

A continuación, daremos algunos ejemplos de datos personales que identifican o hacen identificable a una persona:

- Datos de carácter identificativo: nombres y apellidos, número de DNI, número de pasaporte, dirección de domicilio, número de teléfono, dirección de correo electrónico, imagen, voz, firma; entre otros.
- Datos de características personales: estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos académicos; entre otros.
- Datos económicos-financieros y de seguros: historial de créditos, información tributaria, seguros, datos bancarios, préstamos bancarios, bienes patrimoniales, deudas, hipotecas; entre otros.

Asimismo, la LPDP reconoce una categoría especial de datos personales denominada datos sensibles; ello en la medida que demandan una mayor protección ya que su afectación podría ocasionar perjuicios de superior gravedad. Esta categoría se encuentra definida en el

numeral 5 del artículo 2° de la LPDP como "datos personales constituidos por los datos biométricos[11] que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud[12] o a la vida sexual".

Por su parte, el Reglamento de la LPDP, en el numeral 6 del artículo 2° menciona que los datos sensibles son "aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad". De este modo se advierte que el reglamento asocia esta categoría especial de datos personales al derecho a la intimidad, lo cual, conllevará a un tratamiento singular.

En ese sentido, esta especial protección atiende a que estos datos por su naturaleza son particularmente sensibles en la medida que su tratamiento podría implicar importantes riesgos de otros derechos fundamentales[13].

2.2.1 *Ámbito de aplicación*

En relación con este punto, el artículo 3° de la LPDP indica que la misma se aplica "a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales

---

[11] La Opinión Consultiva N°032-2021-JUS/DGTAIPD con fecha 17 de agosto de 2021, define a los datos biométricos como: "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Un ejemplo de técnica de identificación biométrica física o fisiológica es el reconocimiento de iris; y, un ejemplo de técnica de identificación biométrica conductual es el análisis de pulsaciones de teclas o de firmas manuscritas.

[12] El artículo 2, numeral 5 del Reglamento de la LPDP define a los datos personales relacionados con la salud como: "aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética".. Asimismo, la Directiva Administrativa N°294-MINSA/2020/OGTI, "Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud" en el artículo 5.4, numeral 4 indica que los datos personales relacionados con la salud incluyen la información relacionada al acto médico o información en materia de salud que pueda afectar la intimidad personal y familiar o la imagen propia.

[13] El reglamento (UE) 2016/670 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, considerando N° 51 menciona específicamente lo siguiente respecto a la categoría especial de datos sensibles: "Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales".

de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles".[14]

Por su parte, el Reglamento de la LPDP señala en su artículo 3° que el mismo "se aplicará a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren".

De lo mencionado, se puede interpretar que la normativa de protección de datos personales resulta aplicable al tratamiento de datos personales de personas naturales. Al respecto, el numeral 16 del artículo 2° de la LPDP precisa que el titular de los datos personales en la persona natural a quien corresponde los datos personales; lo cual significa que el ámbito de aplicación no incluye a las personas jurídicas.

Lo indicado no significa que las personas jurídicas no sean titulares de datos personales o no tengan protección; sino que la LPDP no les resulta aplicable. Ahora bien, distinto es el caso de una persona natural con negocio, que cuenta con un Registro Único de Contribuyentes (RUC); ya que "incorpora sus datos personales a los datos personales de su negocio y en esa medida la protección de esos datos se encuentra dentro del ámbito de aplicación de la LPDP y su Reglamento, porque en este caso no son datos de una persona jurídica"[15]. En este sentido, se puede concluir que la delimitación del ámbito de aplicación de la LPDP no se establece en función al rol de empresario que pueda tener una persona, sino en virtud de si el titular de los datos personales en una persona natural o una persona jurídica.

Asimismo, es importante entender qué implica realizar tratamiento de datos personales; ello, en la medida que la LPDP y su Reglamento se aplican a toda modalidad o variedad de tratamiento de datos personales. Sobre este punto, el numeral 19 del artículo 2° de la LPDP define el tratamiento de datos personales como: "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".

---

[14] El mismo artículo 3° referido al ámbito de aplicación señala que la LPDP no será aplicable a los datos personales: "1. Contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar. 2. 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 a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito".

[15] Oficio N°137-2015-JUS/DGPDP con fecha 04 de marzo de 2015.

Cabe señalar que esta lista es enunciativa y no se limita a las acciones descritas; siendo que muchas acciones podrían ser consideradas tratamiento tales como: resumir, actualizar, comprimir, disgregar datos personales; entre otros.

2.2.2 *Sujetos*

En relación con este punto, "el universo del tratamiento de los datos de carácter personal gira en torno a cuatro sujetos, a saber, el titular del dato personal; el titular del banco de datos personales o responsable de tratamiento; el encargado del tratamiento o encargado del banco de datos; y, el tercero o subcontratante"[16].

En primer lugar, el titular del dato personal es "la persona natural a quien lo corresponde los datos personales".[17]. Así, la LPDP como su reglamento al desarrollar el contenido de la protección de los datos personales, se refieren a las personas naturales; no incluyendo a las personas jurídicas. Lo mencionado ha sido indicado en más de una oportunidad en las opiniones consultivas desarrolladas por la autoridad.[18]

Así, en los casos en que se requiera tratar los datos de una persona natural porque está representando a una persona jurídica y dichos datos son necesarios para ejercer la representación -tales como nombre, apellidos, N° de DNI-, dicho tratamiento no se encontrará bajo el ámbito de aplicación de la LPDP ni su Reglamento; pues forman parte de la persona jurídica.[19]

En segundo lugar, el titular del banco de datos personales o responsable de su tratamiento "persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad".[20] Por lo tanto, el titular de banco de datos es quien decide sobre tres aspectos importantes del banco de datos personales: las finalidades para las cuales serán tratados los datos personales, el tratamiento que se les dará y las medidas de seguridad aplicables.

Al respecto, un banco de datos personales es el "conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico

---

[16] LINARES, Sebastián. "En contenido constitucional del derecho fundamental a la autodeterminación informativa en el Derecho Constitucional Peruano". Recuperado de: https://pirhua.udep.edu.pe/handle/11042/4163

[17] Artículo 2, numeral 6, de la LPDP.

[18] Oficio N°873-2013-JUS/DGPDP con fecha 18 de noviembre de 2013 y el Oficio N°140-2014-JUS/DGPDP con fecha 21 de marzo de 2014.

[19] Oficio N°35-2020-JUS/DGPDP con fecha 22 de julio del 2020.

[20] Artículo 2, numeral 17 de la LPDP.

u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso".[21]

En tercer lugar, el encargado de tratamiento es "Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales".[22]

En este contexto, el encargado del tratamiento de los datos personales solo podrá realizar los tratamientos que le indique el titular del banco de datos personales para las finales que le determine. Ahora bien, en caso el encargado realizara un tratamiento distinto, se convertiría en titular del banco de datos creado para la realización de nuevos tratamientos.[23]

En cuarto y último lugar, el tercero o subcontratista, es la persona natural, jurídica de derecho privado o pública, diferente al encargado que realiza tratamiento de datos personales; siempre que haya sido autorizado por parte del titular del banco de datos personales o responsable del tratamiento. Este tercero realizará el tratamiento en el contexto de la celebración de un contrato o convenio celebrado con el encargado donde se indique que el tratamiento que lleve a cabo será en nombre y por cuenta del encargado del tratamiento.

Ahora bien, habiendo quedado claro los principales conceptos vinculados al marco normativo de la protección de datos en el Perú, qué se entiende por datos personales, qué implica realizar tratamiento de datos personales, el ámbito de aplicación de la norma y los sujetos en virtud de los cuales gira en torno al universo de la protección de los datos personales; a continuación se procederá a explicar las cuestiones fundamentales que dieron origen a una serie de cuestionamientos sobre cómo cumplir con la regulación de protección de datos personales.

[21] Artículo 2, numeral 1 de la LPDP.
[22] Artículo 2, numeral 7 de la LPDP.
[23] Oficio N°167-2017-JUS/DGPDP con fecha 03 de abril de 2017.

Capítulo 3

La obtención del consentimiento y el cumplimiento del deber de información. Cuestionamientos y su solución

3.1 El principio del consentimiento y el deber de información. Piedras angulares de la protección de datos personales

Como se ha mencionado al inicio del presente trabajo, las disposiciones de la normativa de protección de datos personales entraron en plena vigencia en el año 2015 siendo, precisamente dicho año, donde la informante se desempeñó como asesora legal especializada en protección de datos personales de diversas empresas del sector privado dedicadas a distintos rubros. De este modo, el presente capítulo reflejará el conocimiento adquirido por la informante, el cual, le permitió poder absolver los principales cuestionamientos por parte de las citadas empresas del sector privado sobre la interpretación o sentido de la normativa, así como su aplicación práctica.

Ahora bien, la informante ha identificado que las primeras y principales interrogantes que le plantearon las empresas a las cuales les brindaba asesoría se referían respecto a la obtención del consentimiento y el cumplimiento del deber de información. En atención a ello, resulta pertinente primero explicar ambos conceptos para luego poder desarrollar las referidas interrogantes.

3.1.1 *El consentimiento*

El consentimiento es una de las piedras angulares de la protección de datos personales; ello en la medida que le otorga al titular de los datos personales la posibilidad de controlar la información personal que le concierne. En esa línea se menciona que "la efectividad de esta garantía jurídica exige un sólido y necesario punto de partida (…) que el sujeto haya consentido que sus datos personales formen parte de algún fichero o bando de datos informatizado".[24]

En esta misma línea, el Tribunal Constitucional define el derecho a la autodeterminación informativa como:

> la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos (...). En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos,

[24] CASTILLO, Luis. *Comentarios al Código Procesal Constitucional*, 2da edición. Palestra Editores, Lima, 2006, pp. 1061 -1062.

> brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera 'sensibles' y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos.[25]

De este modo, se entiende que no puede ejercerse un control efectivo de la información personal sin que pueda conocerse cómo se utilizarán los datos, qué tratamiento se efectuará; a quiénes se les compartirá la información y sin que se solicite la autorización de la información personal cuando corresponda. En ese sentido, la LPDP establece los principios que rigen el tratamiento de los datos personales; de los cuales se desprenden los derechos de los titulares de los datos personales y las obligaciones a cargo de los responsables que efectúan dicho tratamiento.

Dentro de los principios, se encuentra el principio del consentimiento, regulado en el artículo 5° de la LPDP, el cual indica lo siguiente: "para el tratamiento de los datos personales debe mediar el consentimiento de su titular".

Por su parte, el artículo 7° del Reglamento de la LPDP también regula el referido principio del consentimiento, señalando expresamente que en atención a dicho principio: "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".

Ahora bien, de acuerdo con el mencionado principio, la LPDP en el numeral 5 del artículo 13° señala expresamente que: "los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco".

A su vez, el numeral 1 del artículo 28° de la LPDP establece como obligación para los responsables del tratamiento y encargados de este, realizar el tratamiento de los datos personales solo con previo consentimiento del titular de los datos personales, salvo con ley autoritativa. Asimismo, en el artículo 14° de la LPDP establece los supuestos de excepción a la solicitud del consentimiento.

Del análisis efectuado a las referidas normas, se observa que la única fuente de legitimación para el tratamiento de datos personales por parte de terceros proviene

---

[25] EXP. N°4739-2007-PHD/TC, fundamento 4.

exclusivamente del consentimiento otorgado por el titular de dichos datos personales. El referido consentimiento se constituye como una manifestación de voluntad que debe cumplir con ciertos requisitos de validez. Ahora bien, existen ciertos supuestos -los cuales serán desarrollados más adelante-, donde el referido consentimiento puede ser limitado; sin embargo, ello no implicará que los responsables del tratamiento se encuentren exentos de cumplir con las demás obligaciones establecidas en la normativa de protección de datos personales.

3.1.2 *El deber de información*

Ahora bien, respecto al deber de información, debemos partir de la premisa que toda persona natural tiene el derecho a ser informado sobre el tratamiento de la información que lo identifica o lo hace identificable. En este sentido, dicho derecho se condice con la obligación por parte de quien realiza el tratamiento de cumplir con el deber de información.

Al respecto, el artículo 18° de la LPDP regula el derecho a la información del titular de los datos personales; señalando expresamente lo siguiente:

> El titular de datos personales tiene derecho a ser informado en forma detallada, 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.

De la lectura del mencionado artículo 18° se advierte que los titulares de los datos personales tienen derecho a recibir información sobre el tratamiento que se realizará respecto de sus datos personales. Ello implicará precisar y/o pormenorizar diversos aspectos referidos a la finalidad del tratamiento, los destinatarios que accederán a los datos personales, la existencia del banco de datos que contiene los datos personales objeto de tratamiento, la identidad y domicilio del titular del banco de datos y/o de los encargados del tratamiento, el carácter obligatorio y/o facultativo de proporcionar los datos personales; a quiénes serán trasferidos los datos personales (de ser el caso), las consecuencias de entregar o no los datos personales solicitados, el tiempo que serán conservados y, finalmente, la posibilidad de ejercer los derechos reconocidos en la LPDP.

Ahora bien, como se ha mencionado previamente, la obligación de cumplir con el deber de información permanecerá aun cuando no sea obligatorio contar con el consentimiento del titular de los datos personales para tratar su información personal. Asimismo, el cumplimiento de este derecho exige que el titular del banco de datos o el encargado del tratamiento facilite la información de forma previa al titular de los datos personales, no siendo admisible que se recién se brinde la información cuando la misma sea solicitada por su titular.

Lo mencionado no significa que el titular no se encuentre facultado a solicitar información posteriormente a su recopilación siendo que, mediante el ejercicio del derecho de acceso, el titular puede requerir la información que desee por ser un derecho que le corresponde.

Por lo tanto, el hecho de recopilar datos personales sin cumplir con el deber de información conforme se encuentra regulado en el artículo 18°, implica una vulneración y/o afectación al bien jurídico protegido, entendido como el control que debe tener toda persona respecto de su información personal, ya que se le estaría imposibilitando conocer cómo será utilizada su información.

3.2 Interrogantes sobre la obtención del consentimiento y el cumplimiento del deber de información

Sobre este punto, como se ha mencionado anteriormente, la informante en adición a las labores que desempeñaba en el Estudio Lazo, De Romaña & Gagliuffi Abogados como Asociada Junior del área de Competencia y Protección al Consumidor, en el año 2016, ingresó al área de Protección de Datos Personales siendo recién, en el mes de mayo de 2015, cuando la ANPDP inició labores de fiscalización a las distintas entidades públicas y privadas respecto al cumplimiento de las obligaciones establecidas en la normativa en materia de protección de datos personales.

En atención a ello, la informante tuvo la oportunidad de atender los primeros cuestionamientos que surgieron respecto a la interpretación e implementación de las exigencias contempladas en la normativa; ello tomando en consideración que la presente regulación es transversal a todas las industrias, en la medida que efectúen tratamiento de datos personales.

A continuación, se detallarán los principales cuestionamientos planteados a la informante -en su calidad de asesora legal- sobre el deber de solicitar el consentimiento y el cumplimiento del deber de información, y, las soluciones brindadas en base al análisis

jurídico de la normativa aplicable; lo cual permitió que las personas jurídicas de derecho privado que solicitaron la asesoría de la informante comprendieran las exigencias contempladas en la normativa y así no incurrieran en incumplimientos que pudiesen generar el inicio de procedimientos administrativos sancionadores y eventuales imposiciones de sanciones.

3.2.1 *El cumplimiento del deber de información respecto de los titulares de los datos personales*

En relación con este punto, las primeras preguntas que surgieron por parte de las personas jurídicas de derecho privado -clientes del estudio de abogados donde laboró la informante- aludían a: (i) los alcances del deber de información previsto en la LPDP; y (ii) cómo materializar el cumplimiento del deber de información respecto de los clientes con los que pudiesen contratar o ya han contratado, los cuales, en calidad de titulares de sus datos personales tenían el derecho a ser informados sobre el tratamiento de su información personal.

Dichas dudas surgieron ya que las empresas de derecho privado se encontraban obligadas a cumplir con este deber de información por ser titulares del banco de datos de sus clientes o responsables del tratamiento de la información personal de los mismos.

A continuación, se desarrollarán las cuestiones mencionadas:

3.2.1.1 Primer cuestionamiento: ¿cuáles son los alcances del deber de información? Al respecto, para poder absolver esta primera duda surgida por parte de los clientes de la informante, correspondía analizar el artículo 18° de la LPDP, el cual es fundamental pues detalla dos aspectos de suma importancia: (1) la forma en la que debe ser trasladada la información a los titulares de los datos personales; y, (2) el contenido de la información proporcionada a los titulares de los datos personales. Posteriormente, se explicará cada aspecto.

3.2.1.1.1 ***Formalidad para el traslado de la información a los titulares de los datos personales*****.** Sobre este primer aspecto, el artículo 18° de la LPDP en el inicio indica que “el titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación” cómo será tratada su información. En ese sentido, se puede apreciar que la parte inicial de dicho artículo 18° describe las características sobre la forma en que debe trasladarse la información a los titulares de los datos personales.

Así, si bien la LPDP no define las referidas características, recurriendo a un método interpretativo literal, la Real Academia de la Lengua Española nos orienta sobre el significado de cada característica conforme se puede apreciar a continuación:

- Detallada: la información se debe trasladar de forma minuciosa meticulosa y precisa sin obviar ningún dato importante. [26]
- Sencilla: la información brindada relativa al tratamiento debe ser fácil de entender; utilizándose un lenguaje simple y claro.[27]
- Expresa: la información debe ser proporcionada de forma explícita y clara; sin asumir que la misma puede haber sido conocida previamente por el titular del dato personal.[28]Ahora bien, la presente característica no debe ser confundida con el atributo recogido en el numeral 3 del artículo 12° del Reglamento de la LPDP respecto a que el consentimiento debe ser expreso; ya que en dicho supuesto la citada cualidad hace referencia a que debe existir una exteriorización o manifestación de voluntad por parte del titular del dato personal.
- Inequívoca: la información se debe dar en un único sentido; sin que existan dudas sobre la misma.[29]
- Previa: la información se debe poner a disposición de los titulares de los datos personales antes de su tratamiento.[30]

Un punto importante es el relacionado al lenguaje; si bien la LPDP no indica en el artículo 18° en qué lenguaje debe brindarse la información, el artículo 62° del Reglamento de la LPDP regula los medios para cumplir con el derecho de acceso, precisando que la lengua utilizada debe ser asequible al conocimiento promedio de la población. En ese sentido, la información deberá ser facilitada en idioma castellano o aquel que predomine en la localidad donde habitan los titulares de los datos personales cuyos datos son objeto de tratamiento.

De este modo, del análisis realizado por la informante respecto al texto de la normativa, se puede concluir que para comprender los alcances del deber de información, como primer punto es fundamental atender a las características que se deben cumplir para comunicar la información al titular de los datos personales; debiendo satisfacerse los siguientes requerimientos sobre la información: (i) debe ser trasladada de forma minuciosa; (ii) el lenguaje debe ser simple y claro (en idioma castellano); (iii) deber de proporcionarse de forma explícita; (iv) tiene que utilizarse un único sentido, es decir, ser inequívoca; y, (iv)

[26] La Real Academia de la Lengua Española (RAE) define el término ‘detallar’ de la siguiente forma: “tratar o referir algo por partes, minuciosa y circunstancialmente”.
[27] La RAE define el término ‘sencillo’ como: “que no ofrece dificultad”.
[28] La RAE define el término ‘expreso’ como: “claro, patente, especificado”.
[29] La RAE define el término ‘inequívoco’ como: “que no admite duda o equivocación”.
[30] La RAE define el término ‘previo’ como: “anticipado, que va delante o sucede primero”.

ponerse a disposición de los titulares de los datos personales de forma previa a su recopilación y/o tratamiento.

3.2.1.1.2 ***Contenido de la información que debe ser trasladada a los titulares de los datos personales*****.** Con relación a este segundo aspecto, el artículo 18° de la LPDP indica qué información debe brindarse a los titulares de los datos personales. Por consiguiente, se procederá a analizar cada uno de los factores vinculados al contenido de la información que debe entregarse a los referidos a los titulares de los datos personales ello a efectos de poder absolver la interrogante planteada respecto a cuáles son los alcances del deber de información:

En ese orden de ideas, el deber de información implicará brindar la siguiente información:

- Identidad y domicilio del titular del banco de datos y del encargado(s) del tratamiento: se debe proveer la identificación del titular del banco de datos y de los encargados del tratamiento, de ser el caso. Los datos variarán si es que se trata de una persona natural (nombre completo y N° de DNI) o de una persona jurídica (razón social y N° de registro único de contribuyente).

  Sobre la indicación del domicilio, tomando en consideración lo indicado en el artículo 5° del Reglamento de la LPDP[31]; referido al ámbito de aplicación de la LPDP, se entiende que si el tratamiento es realizado por personas naturales, el domicilio que se deberá de indicar es la dirección del local donde se encuentre el principal asiento de sus negocios, el que se utilice para desempeñar sus actividades o su domicilio. Cabe señalar que, si el tratamiento es realizado por personas jurídicas, el domicilio que se deberá informar será donde se ubique la administración principal del negocio.
- Finalidad o finalidades del tratamiento de los datos personales: se debe describir los usos específicos que se les darán a los datos personales; es decir; el propósito del tratamiento. Al respecto, el Principio de Finalidad previsto en el artículo 6° de la LPDP señala que "Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe

[31] Artículo 5° del Reglamento: "(…) En el caso de personas naturales, el establecimiento se entenderá como el local en donde se encuentre el principal asiento de sus negocios, o el que utilicen para el desempeño de sus actividades o su domicilio.
Tratándose de personas jurídicas, se entenderá como el establecimiento el local en el que se encuentre la administración principal del negocio. Si se trata de personas jurídicas residentes en el extranjero, se entenderá que es el local en el que se encuentre la administración principal del negocio en territorio peruano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad".

extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación (…)".

De este modo, las finalidades deber ser expresadas claramente; mencionándose el (los) objetivo(s) en virtud de los cuales será tratada la información personal; solo así se puede considerar que las finalidades están determinadas.

- La identidad de los destinatarios de los datos personales: el presente punto hace referencia al supuesto que se efectúe una transferencia de datos personales. Para ello, resulta importante entender qué se entiende por transferencia de datos personales. Al respecto, el numeral 18 del artículo 2° de la LPDP, la transferencia de datos personales como: "toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional a una persona jurídica de derecho privado, a una entidad pública o una persona distinta del titular de los datos personales".

  De lo mencionado, se puede advertir que los destinatarios pueden encontrarse dentro o fuera del Perú y, pueden ser personas naturales o jurídicas de derecho público o privado. Asimismo, dicha definición no efectúa ninguna distinción en cuanto a el título o finalidad bajo la cual se efectúa la transmisión. En este sentido, ya sea que los datos se entreguen a un encargado o a un tercero; se debe indicar la identidad del destinatario.
- La existencia del banco de datos: sobre este punto, el artículo 34° de la LPDP dispone la creación del Registro Nacional de Protección de Datos Personales; disponiendo que en el mismo se inscribirán los bancos de datos personales ya sea de administración pública o privada. Al respecto, cuando se realiza una inscripción de un nuevo banco de datos ante el Registro Nacional de Protección de Datos Personales, se otorga un número de inscripción. En este sentido, la forma idónea de cumplir con el presente factor implicará brindar información sobre la identificación del banco de datos; esto es; la denominación del mismo y su número de inscripción.
- Tiempo de conservación de los datos personales: en relación al presente factor, resulta importante atender a lo dispuesto por el principio de calidad, regulado en el artículo 8° de la LPDP; el cual señala que los datos personales deben ser conservados por el tiempo necesario para cumplir con la finalidad del tratamiento.[32] En este sentido, se

[32] Artículo 8° de la LPDP:
"Principio de calidad: Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la

deberá precisar el plazo durante el cual se conservarán los datos personales de los titulares para cumplir con las finalidades en virtud de las cuales se realiza el tratamiento.

- Los datos personales de obligatoria entrega: sobre esta indicación, dependiendo de la finalidad o finalidades en virtud de la cual(es) se requerirá realizar el tratamiento de los datos personales, existirán determinados datos personales que será obligatorio entregar al responsable; por ellos es indispensable que se informe qué datos personales son obligatorios entregar por parte del titular de los datos personales para que, por ejemplo, se perfeccione una relación laboral o comercial, para el cumplimiento de una obligación legal; entre otras.
- Consecuencias de proporcionar los datos o su negativa a hacerlo: el presente punto se encuentra vinculado al anterior punto respecto a qué datos personales deben de ser entregados obligatoriamente, ya que existirán supuestos donde la recopilación es necesaria para cumplir con una determinada finalidad, debiendo informarse al titular de los datos personales sobre la obligatoriedad o no de prestar el consentimiento y las consecuencias que se derivarán de no hacerlo.
- Ejercicio de los derechos ARCO y los medios para ejercer dichos derechos: respecto a este factor, es obligatorio que se le informe al titular de los datos personales que goza de determinados derechos, los cuales, como se ha mencionado anteriormente, son reconocidos por la LPDP. Ello, a efectos de otorgarle un control sobre su información personal. Cabe señalar que el artículo 53° del Reglamento de la LPDP señala que los responsables del tratamiento de los datos personales deben establecer procedimientos sencillos para atender el ejercicio de estos derechos por parte de sus titulares. En este sentido, se debe informar a los titulares de los datos personales los canales de atención que tendrán a su disposición para ejercer los derechos ARCO. Sobre este punto, es importante precisar que no existe algún impedimento en la norma para que una solicitud de ejercicio de derechos sea atendida de forma virtual; ello en atención a lo indicado en el citado artículo 53° respecto a la sencillez del procedimiento para atender los referidos derechos.

Por lo tanto, se puede advertir que la informante realizó una interpretación del propio texto de la LPDP y su reglamento, atendiendo a los principios reconocidos en el texto

---

que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento".

normativo, así como a lo descrito en diversos artículos que conforman el cuerpo normativo- para comprender cada uno de los elementos que componen la información que debe trasladarse a los titulares de los datos personales.

De este modo, el análisis efectuado le permitió a la informante absolver la primera interrogante planteada por los clientes (personas jurídicas de derecho privado) que asesoró respecto a los alcances del deber de información previsto en la normativa de protección de datos personales.

3.2.1.2 Segundo cuestionamiento: ¿cómo materializar el cumplimiento del deber de información? Respecto a esta segunda duda, si bien ha quedado esclarecida la primera interrogante sobre el alcance del deber de información, los clientes de la informante mostraron incertidumbre respecto a cómo podría materializarse el cumplimiento dicho deber de información.

A efectos de ilustrar con mayor precisión este asunto, se debe precisar que: (i) los nuevos titulares de los datos personales son los nuevos clientes con los cuales podrían contratar las empresas de derecho privado; y; (ii) los antiguos titulares de los datos personales; son clientes que mantienen una relación comercial con las personas jurídicas de derecho privado.

Cabe señalar que las modalidades de cumplimiento no variarán dependiendo de si nos encontramos frente a antiguos o nuevos clientes.

Al respecto, tomando en consideración los medios a través de los cuales se puede captar la información personal de los nuevos clientes; dichos medios pueden asimismo constituir las modalidades para materializar el cumplimiento del Deber de Información. Así, la informante señala las siguientes modalidades:

3.2.1.2.1 ***Modalidad impresa*****.** Este tipo de modalidad se puede utilizar cuando los datos personales de los clientes son recogidos mediante documentación física; ya sea a través de contratos, formularios, cuestionarios, solicitudes, etc. La presente modalidad implicaría la redacción de una cláusula informativa que brinde la información señalada en el artículo 18° de la LPDP; la cual se ha detallado en el presente documento. Asimismo, dicha cláusula podría incorporarse en los contratos que se celebren con los clientes o, si la información es recogida a través de formularios, solicitudes o cuestionarios físicos, se podría anexar un documento denominado ‘clausula informativa’ que contenga la información mencionada. Asimismo, la presente cláusula informativa podría ser publicada en lugar visible en las

instalaciones abiertas al público de la empresa, ello, a efectos de que los clientes tomen conocimiento de la misma.

3.2.1.2.2 ***Política de privacidad en webs y aplicativos***. De acuerdo a lo señalado en el artículo 18° de la LPDP: "si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables". En ese sentido, se puede redactar una política de privacidad donde se cumpla con informar las características sobre el tratamiento de los datos personales de los clientes. Esta política debe estar publicada en una sección donde se pueda acceder fácilmente a su lectura.

3.2.1.2.3 ***Locuciones telefónicas***. En la medida que se obtenga información personal mediante una conversación telefónica, se puede cumplir con el Deber de Información a través de la misma locución; trasladando la información señalada en el artículo 18° al cliente.

Ahora bien, para el caso de antiguos clientes, las modalidades señaladas les serían igualmente aplicables. En estos supuestos, bastaría con enviar una comunicación por cualquier medio informando sobre la existencia de una cláusula informativa o política de privacidad, y, adjuntar la misma para que tomen conocimiento de su contenido.

De conformidad con lo mencionado, se puede concluir que para materializar el cumplimiento del deber de información se deberá atender a los medios a través de los cuales se puede captar la información personal de los clientes, los mismos, se resumen en el empleo de formatos físicos, elaboración de políticas de privacidad digitales y locuciones telefónicas.

Es importante señalar que la informante, con el análisis efectuado, despejó la interrogante referida a los alcances del deber de información y cómo materializar su cumplimiento, lo cual permitió que las diversas empresas -personas jurídicas de derecho privado- a las que asesoró no incurran en una infracción grave ni sean sancionadas con multas elevadas.

Al respecto, el artículo 132° del Reglamento de la LPDP señala en el numeral 2 inciso a que constituye una infracción grave: "No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley N° 29733 y su Reglamento". Así, como se ha indicado, uno de los derechos reconocidos en la normativa de protección de datos personales es el derecho de información, el cual se constituye como un derecho-deber de informar pues representa un derecho atribuible al titular

de los datos personales y, asimismo, una obligación para el titular del banco de datos o responsable del tratamiento.

En ese sentido, informar de manera incompleta o no cumplir con el deber de información son conductas sancionables bajo el citado artículo, cuya multa base es de más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias; de acuerdo a lo indicado en el artículo 39° de la LPDP.

3.2.2 *El consentimiento. ¿En qué casos es necesario obtener el consentimiento de los titulares de los datos personales*

En relación con este punto, un cuestionamiento que fue recurrente por parte de las personas jurídicas de derecho privado -como se ha mencionado previamente, nos referimos a los clientes del estudio de abogados donde laboró la informante- estuvo vinculado a si era necesario obtener el consentimiento de sus clientes para tratar sus datos personales en el marco de las relaciones comerciales de venta de productos o prestación de servicios.

Sobre el particular, como se ha indicado al inicio del presente capítulo, el consentimiento constituye una de las piedras angulares de la protección de los datos personales; ello toda vez la normativa establece para el tratamiento de los datos personales debe mediar el consentimiento del titular, de conformidad con lo establecido por el principio de consentimiento.

A su vez, el numeral 1 del artículo 28° de la LPDP establece como obligación de los responsables y encargados del tratamiento de los datos personales realizar el tratamiento solo con previo consentimiento del titular de los datos personales; salvo ley autoritativa, con excepción de los supuestos consignados en el artículo 14° de la LPDP.

Asimismo, es importante mencionar que la referida obligación de obtener el consentimiento por parte de los titulares de los datos personales tiene excepciones; las cuales se encuentran reguladas el artículo 14°[33] de la LPDP.

---

[33] "Artículo14°. Limitaciones al consentimiento para el tratamiento de datos personales:
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

1) Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2) Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3) Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4) Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que

En ese sentido, a efectos de poder absolver la interrogante planteada, en primer lugar, se debe determinar si la relación comercial entre una persona jurídica de derecho privado dedicada a la venta de productos y/o servicios y un cliente se encuentra contemplada dentro de alguna de las excepciones al consentimiento detalladas en el citado artículo 14° de la LPDP.

Pues bien, de la revisión de las referidas excepciones, se advierte que el numeral 5 establece que no se requiere el consentimiento del titular de los datos personales para su tratamiento cuando los datos personales sean "necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular sea parte".

De este modo, y aplicándolo al caso en concreto, se entiende que no se necesitará el consentimiento de los clientes cuando los datos personales que les sean requeridos por la persona jurídica sean fundamentales e indispensables para la preparación y/o desarrollo de la relación comercial respecto de la cual forman parte.

---

haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5) Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6) Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7) Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8) Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9) Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10) Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11) En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12) Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13) Otros que deriven del ejercicio de competencias expresamente establecidas por Ley".

Así, aquellos datos personales que sean necesarios o imprescindibles para que se pueda entablar y desarrollar la relación comercial entre las partes contratantes están amparados en el marco de dicha excepción. En atención a ello, se deberá analizar cada una de las prestaciones a las que se comprometerán las partes a fin de determinar si nos encontramos ante el supuesto de hecho previsto en la excepción contemplada en el numeral 5 del artículo 14° de la LPDP.

Ahora bien, el principio del consentimiento y las excepciones al mismo, no se pueden interpretar de forma aislada, sino de manera conjunta con los demás principios y disposiciones previstas en la LPDP y su Reglamento, debiendo tomarse en cuenta lo señalado por el principio de finalidad y de proporcionalidad.[34]

En ese sentido, haciendo un análisis integral de los referidos principios y vinculándolos al deber de solicitar el consentimiento, se puede concluir lo siguiente: (i) el tratamiento de los datos personales estará sujeto a aquello que haya autorizado su titular; no pudiendo extenderse el tratamiento a otras finalidades que no hayan sido señaladas -y autorizadas- de manera inequívoca; y, (ii) el tratamiento de los datos personales debe efectuarse respecto de información que es imprescindible para cumplir con la(s) finalidad(es) autorizada(s); limitándose a los datos que sean relevantes para cumplir con la(s) misma(s).

Bajo estas consideraciones, en segundo lugar, se debe tomar en consideración que si en una relación comercial existen prestaciones adicionales que no forman parte del objeto principal de dicha relación, su tratamiento no se encontraría exceptuado del consentimiento; debiendo solicitarse el mismo al titular de los datos personales.

Por ejemplo, para la contratación de un determinado servicio o venta de un producto, la empresa proveedora puede tener acceso a determinados datos de contacto del consumidor como el teléfono o correo electrónico. Así, en caso el proveedor busque satisfacer intereses comerciales y, en ese sentido, quisiera enviarle a su cliente promociones exclusivas, alguna encuesta u otra oferta al correo electrónico o número de teléfono que tiene en su poder, ello constituiría una prestación o finalidad adicional -finalidad publicitaria- a la que motivó la preparación, celebración y ejecución de la relación comercial, que fue la compra de un producto o prestación de un servicio. Bajo estos supuestos lo que correspondería sería solicitar el consentimiento para dicha finalidad publicitaria adicional.

[34] Artículo 7° de la LPDP. Principio de proporcionalidad: “Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados”.

Es por ello que resulta sumamente importante determinar con precisión: (i) la información personal del titular de los datos personales (cliente) que será objeto de tratamiento y su posición en la relación contractual, las razones que justifican su tratamiento y las prestaciones a las que cada una de las partes se han comprometido al momento de celebrar el contrato con la finalidad de establecer si el tratamiento se encuentra amparado o no en la excepción señalada previamente y, (ii) si existen finalidades adicionales, ello a efectos de obtener el consentimiento libre, previo, expreso, informado e inequívoco.

Es importante mencionar que si bien una relación comercial entre una empresa proveedora dedicada a la venta de productos y/o prestación de servicios y su cliente se puede encontrar exceptuada de obtener el consentimiento; ello no implica que dicha empresa se vea exenta de cumplir con las demás obligaciones señaladas en la LPDP y su Reglamento; entre ellas, cumplir con el deber de información, garantizar la confidencialidad de la información; cumplir con determinadas medidas de seguridad, etc.

Finalmente, es preciso indicar que ni la LPDP ni su Reglamento establecen mediante qué documentos se debe cumplir con la obligación de solicitar el consentimiento (en caso sea aplicable); sin embargo, atendiendo a lo desarrollado en el punto anterior vinculado a la materialización del deber de información, el consentimiento podría obtenerse a través de la firma en formatos impresos; la aceptación de cláusulas de tratamiento de datos personales vía online (a través de la marcación de *check boxes*), y mediante la aceptación verbal en locuciones telefónicas.

En conclusión, del análisis integral de la normativa en materia de protección de datos personales respecto a la obtención del consentimiento, se concluye que: (i) las empresas de derecho privado en calidad de proveedoras de productos o prestadoras de servicios, no requerirán el consentimiento de sus clientes para realizar el tratamiento de sus datos personales para la venta de sus productos o prestación de sus servicios; en la medida que los datos personales objeto de tratamiento sean necesarios o imprescindibles para que se pueda entablar y desarrollar la relación comercial entre las partes; (ii) en caso los datos personales quieran ser utilizados para finalidades adicionales que no se encuentran dentro de las prestaciones a las que cada una de las partes se han comprometido; se requerirá obligatoriamente obtener el consentimiento libre, previo, expreso, informado e inequívoco por parte del titular de los datos personales; y, (iii) la aplicación de la excepción al consentimiento no implica que las empresas se vean exentos que cumplir con las demás obligaciones establecidas en la normativa de protección de datos personales.

Es importante señalar que la informante con el análisis efectuado despejó la interrogante vinculada a la obligación de las empresas -personas jurídicas de derecho privado- de obtener o no el consentimiento de sus clientes para tratar sus datos personales en el marco de las relaciones comerciales de venta de productos o prestación de servicios; precisando en qué casos no sería necesario obtenerlo y, en qué casos es mandatorio contar con el mismo.

Al aclararse dicha interrogante la informante evitó que las empresas a las que les brindó asesoría incurran en una infracción grave y sean sancionadas con multas elevadas.

Al respecto, el artículo 132° del Reglamento de la LPDP señala en el numeral 2 inciso b que constituye una infracción grave: "Dar tratamiento a los datos personales sin el consentimiento libre, expreso, inequívoco, previo e informado del titular, cuando el mismo sea necesario conforme a lo dispuesto en la Ley Nº 29733 y su Reglamento".

En ese sentido, no pedir el consentimiento (cuando resulte necesario hacerlo) o solicitarlo no cumpliendo con sus características son conductas sancionables bajo el citado artículo; cuya multa base es de más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias; de acuerdo a lo indicado en el artículo 39° de la LPDP.

3.2.3 *La Ley Antispam y la obtención del consentimiento para el envío de publicidad comercial*

Sobre el particular, en repetidas oportunidades las empresas de derecho privado asesoradas por la informante le consultaron sobre la compatibilidad de las disposiciones contenidas en la LPDP y su Reglamento sobre la obtención del consentimiento -vinculado al envío de publicidad comercial- y la Ley N° 28493, ley que regula el uso del correo electrónico comercial no solicitado "SPAM" (en adelante, Ley Antispam) y su Reglamento aprobado por el Decreto Supremo N° 031-2005-MTC. Ello, en la medida que no resultaba claro si cumpliendo con las disposiciones de la Ley Antispam; ya no requerían solicitar el consentimiento libre, previo, expreso, informado e inequívoco o, si era exigible obtenerlo.

Al respecto, la informante realizó un análisis de ambas normas; evaluando su contenido, así como las fechas de promulgación, vigencia, entre otros aspectos para poder absolver la citada interrogante; conforme se apreciará a continuación:

El artículo 3° del Reglamento de la LPDP señala expresamente que: "La existencia de normas o regímenes particulares o especiales, aun cuando incluyan regulaciones sobre datos personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la ley y del presente reglamento. Lo

dispuesto en el párrafo precedente no implica la derogatoria o inaplicación de las normas particulares, en tanto su aplicación no genere la afectación del derecho a la protección de datos personales".

En ese sentido, en la medida que exista normativa particular o especial que regule el tratamiento de datos personales, y la misma no genere afectación a la protección de los datos personales de acuerdo a lo establecido en la LPDP y su Reglamento, podrá mantenerse vigente y ser aplicable a los casos que corresponda; ello atendiendo al rango de derecho fundamental que posee el derecho a la protección de los datos personales reconocido en la Constitución.

Aterrizando a la consulta formulada, como se ha mencionado, diversos clientes (empresas del sector privado) de la informante le consultaron si era posible que puedan enviar a sus clientes (personas naturales) comunicaciones publicitarias no solicitadas de conformidad con lo establecido con la Ley Antispam o ello contravenía las disposiciones de la LPDP y su Reglamento ya que las mismas indican que debe existir un consentimiento previo por parte de los titulares de los datos personales para el tratamiento de sus datos personales.

Sobre este punto, resulta importante realizar una diferenciación entre dos periodos, ya que con el transcurso de los años se han generado cambios normativos, los cuales han implicado un cambio de criterio respecto a la interpretación de las normas. En ese sentido, se procederá a establecer un primer periodo entre julio del 2005 y setiembre 2018 y un segundo periodo desde setiembre del 2018 hasta la fecha.

3.2.3.1 Primer periodo (julio de 2005 - setiembre de 2018). Respecto a este primer periodo, resulta pertinente indicar que la Ley Antispam entró en vigencia el 11 de julio del 2005 y tuvo como objeto regular el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas realizadas por correo electrónico; siguiendo determinadas características, según lo establecido en el artículo 5°[35] de la referida ley.

Así, de acuerdo a los señalado en el artículo 7° del Reglamento de la Ley Antispam: "un mensaje de correo electrónico comercial será considerado como "No solicitado" cuando

[35] Artículo 5. Correo electrónico comercial no solicitado.
Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:
a) La palabra "PUBLICIDAD", en el campo del "asunto" (o *subject*) del mensaje.
b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en Internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

haya sido enviado por el remitente sin que medie el pedido o consentimiento expreso del receptor"; es decir; no existe una relación contractual previa con el receptor o usuario.

Adicionalmente, el artículo 8° del Reglamento de la Ley Antispam desarrollaba la correcta aplicación de las condiciones para el envío del correo electrónico no solicitado precisadas en el artículo 5° de la Ley Antispam; tales como: incluir la palabra "publicidad" en el campo de "asunto" del correo electrónico; los datos del remitente del mensaje debían consignarse en la parte final del mensaje, añadiéndose el nombre de una persona de contacto; la dirección de correo electrónico que debía incluirse como mecanismo de contacto entre el receptor y el remitente debía tener coincidencia con dicho remitente; los mecanismos para atender solicitudes vinculadas a no recibir más correos comerciales no solicitados debían encontrarse operativos.

Cabe señalar que si un proveedor no cumplía con los requisitos establecidos en el referido artículo 5° de la Ley Antispam sería considerado ilegal, lo cual implicaba una infracción cuya fiscalización y sanción correspondía al Indecopi. Ello, según lo señalado en el artículo 9°[36] de la citada Ley Antispam. Por el contrario, si los proveedores cumplían con los parámetros indicados, se encontraban plenamente habilitados para el envío de correos electrónicos a sus consumidores sin tener que recabar su consentimiento de forma previa.

Complementariamente, la Directiva N° 005-2009/COD-Indecopi, Directiva de Operación y Funcionamiento del Registro de Números Telefónicos y direcciones de correo electrónico excluidos de ser destinatarios de publicidad masiva registro "Gracias…No insista"; la cual entró en vigencia el 16 de setiembre de 2009, reguló la implementación de un registro conformado por la lista de números telefónicos y direcciones electrónicas de los consumidores que no querían recibir publicidad masiva ya sea por vía electrónica o telefónica, pudiendo señalar el rubro de productos o servicios respecto de los cuales no quería recibir ninguna publicidad. Asimismo, les proporcionó a los proveedores -los cuales debían inscribirse en el citado registro- que emplearan *call centers*, sistemas de llamado telefónico, envío de mensajes de texto a celular, envío de correos electrónicos para el envío de publicidad masiva para promover sus productos o servicios, la información sobre los consumidores a los que no debían contactar por estar inscritos en el mencionado registro.

---

[36] "Artículo 9°. Autoridad competente. El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Indecopi, a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, será la autoridad competente para conocer las infracciones contempladas en el artículo 6° de la presente ley; cuyas multas se fijarán de acuerdo a lo establecido en el Decreto Legislativo N° 716, Ley de Protección al Consumidor, o en el Decreto Legislativo N° 691, normas de la publicidad en defensa del consumidor, según corresponda".

Posteriormente, el 02 de octubre de 2010 entró en vigencia la Ley N° 29571, Código de Protección y Defensa de Consumidor (en adelante, Código de Consumo), la cual, dispuso en su literal e del numeral 1 del artículo 58° que los proveedores estaban prohibidos de emplear estas prácticas comerciales respecto de números telefónicos y direcciones electrónicas que hayan sido incorporadas en el registro implementado por el Indecopi para registrar a los consumidores que no desearan ser sujetos de las referidas modalidades de promoción o publicidad.[37]

En consecuencia, si una empresa proveedora de productos o prestadora de servicios deseaba realizar tratamiento de los datos personales de sus clientes para el envío de comunicaciones promocionales o publicitarias; debía de cumplir con: (i) los requisitos señalados en el artículo 5° de la Ley Antispam; (ii) observar las consideraciones desarrolladas en el artículo 8° del Reglamento de la Ley Antispam; y, (iii) verificar que el consumidor no esté registrado en el registro "Gracias…No Insista" con la finalidad de excluir a aquellos que manifestaron su negativa a la realización del tratamiento de sus datos para dichos fines.

Así, en caso no se cumpliera con los puntos desarrollados previamente, obligatoriamente el proveedor requeriría obtener el consentimiento de los clientes; ello de conformidad con lo establecido por el principio del consentimiento, el cual ha sido ampliamente desarrollado en el presente documento.

En conclusión, durante el periodo comprendido entre julio del 2005 y setiembre del 2018 no se advierte alguna incompatibilidad entre la normativa antispam y la LPDP; en la medida que la Ley Antispam preveía mecanismos que protegían a los titulares de los datos personales del uso de su información para el envío de comunicaciones publicitarias o promocionales. En ese sentido, las personas jurídicas de derecho privado, en su calidad de proveedores de productos o servicios podían optar por: (a) cumplir con los requisitos establecidos en la Ley Antispam y su Reglamento respecto al envío de comunicaciones no solicitadas; verificando adicionalmente el registro "Gracias…No Insista"; lo cual les permitiría el envío de comunicaciones promocionales o publicitarias a los consumidores; o, (b) cumplir con solicitar el consentimiento de acuerdo con lo establecido en la LPDP y su

[37] El inciso e) numeral 1) del artículo 58° señala que: "Están prohibidas todas aquellas prácticas que importen: inciso e) "Emplear centros de llamada (*call centers*), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemercadeo, **a todos aquellos números telefónicos y direcciones electrónicas que hayan sido incorporados en el registro implementado por el Indecopi para registrar a los consumidores que no deseen ser sujetos de las modalidades de promoción antes indicadas**". (énfasis agregado).

Reglamento para el tratamiento de sus datos personales y encontrarse habilitados de enviar las promociones o publicidades que estimen pertinentes.

3.2.3.2 Segundo periodo (setiembre del 2018 a la fecha). El inicio de este segundo periodo se debe a la modificación del referido literal e del numeral 1 del artículo 58° mediante el Decreto Legislativo N° 1390 que modifica el Código de Protección y Defensa del Consumidor, el cual entró en vigencia el día 02 de setiembre de 2018, señalando expresamente que se requería el consentimiento para el envío de correos electrónicos con la finalidad de promover productos o servicios, conforme se puede apreciar a continuación:

> 58.1 El derecho de todo consumidor a la protección contra los métodos comerciales agresivos o engañosos implica que los proveedores no pueden llevar a cabo prácticas que mermen de forma significativa la libertad de elección del consumidor a través de figuras como el acoso, la coacción, la influencia indebida o el dolo.
> En tal sentido, están prohibidas todas aquellas prácticas comerciales que importen:
> (…)
> e. Emplear centros de llamada (*call centers*), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemercadeo, a todos aquellos números telefónicos y direcciones electrónicas de consumidores que no hayan brindado a los proveedores de dichos bienes y servicios su consentimiento previo, informado, expreso e inequívoco, para la utilización de esta práctica comercial. Este consentimiento puede ser revocado, en cualquier momento y conforme a la normativa que rige la protección de datos personales. (subrayado agregado).

De este modo, del análisis del citado artículo se aprecia que la modificación legislativa del Código de Consumo; implicó que ya no sea posible que las empresas proveedoras de bienes y servicios remitieran comunicaciones con contenido comercial a los consumidores (como sí lo permitía la Ley Antispam); salvo que hubiesen obtenido por parte de dichos consumidores el consentimiento expreso de forma previa.

Como se podrá evidenciar, la nueva disposición es manifiestamente incompatible e incoherente con lo establecido en la Ley Antispam, colisionando con su contenido pues con la modificación se requiere previamente solicitarle el consentimiento al consumidor para comunicarse con él, a efecto de ofrecerle productos o servicios.

Así, en la medida que dos disposiciones normativas no pueden ser contradictorias y que la entrada en vigencia de la modificación del Código de Consumo (06 de setiembre del 2018) fue posterior a la entrada en vigencia de la Ley Antispam (11 de julio de 2005); se puede determinar que se efectuó una derogación tácita de la Ley Antispam; ello de

conformidad con lo establecido en el artículo I del Título Preliminar del Código Civil[38], el cual, señala que la derogación de una norma puede darse por incompatibilidad entre la nueva y anterior ley.

De este modo, para poder remitir correos electrónicos para la prospección y venta de productos o servicios; se requiere contar con el consentimiento previo, expreso, libre, informado e inequívoco del titular del dato personal; siendo que este primer contacto con el consumidor o titular de los datos personales tiene como objetivo obtener su consentimiento, satisfaciéndose la característica de ser previo y, posteriormente, el proveedor podrá enviar las comunicaciones para publicitar o promocionar productos o servicios que estime convenientes.

Cabe señalar que la referida modificación del Código de Consumo implicó también la derogación del Registro "Gracias…No Insista" para evitar recibir comunicaciones sin haber dado el consentimiento o autorización; siendo que la propia exposición de motivos del Decreto Legislativo N° 1390 indicó que la problemática encontrada "luego de más de ocho años de vigencia del registro "Gracias...no insista" es, por un lado, que estaría cumpliendo limitadamente su objetivo de que las empresas no puedan ofrecer propuestas comerciales a las personas que no deseen ser contactadas y, por otro lado, el Código no se encuentra adecuado a lo señalado por la Ley de Protección de Datos Personales publicada en julio de 2011"[39]. Ello, toda vez que la LPDP señala como uno de sus principios rectores el de contar con el consentimiento, conforme se ha explicado a lo largo del presente documento.

Así, el análisis jurídico de las normas le han permitido a la informante determinar que, durante un primer periodo comprendido entre julio de 2005 y setiembre de 2018, una empresa proveedora de productos o servicios podía enviarle a sus clientes (personas naturales) comunicaciones comerciales no solicitadas cumpliendo con los requisitos señalados en la Ley Antispam; lo cual no implicaba contravenir las disposiciones de la LPDP y su Reglamento respecto a la obtención del consentimiento de forma previa; existiendo una armonía entre ambas normas. En ese sentido, las empresas que realizaran la citada práctica de remisión de correos no serían sancionadas por la ANPDP.

Sin embargo, desde la entrada en vigencia de la modificación del Código de Consumo sobre la remisión de comunicaciones promocionales o publicitarias a los consumidores en

[38] Título I. La ley se deroga sólo por otra ley. La derogación se produce por declaración expresa, por incompatibilidad entre la nueva ley y la anterior o cuando la materia de ésta es íntegramente regulada por aquélla. Por la derogación de una ley no recobran vigencia las que ella hubiere derogado.

[39] Disponible en: https://www.leyes.congreso.gob.pe/Documentos/2016_2021/Decretos/Legislativos/2018/DL13902018 0910.PDF

setiembre de 2018, el criterio esbozado previamente varió, siendo en la actualidad las empresas proveedoras de productos y servicios las que deben obtener previamente el consentimiento de sus clientes para poder enviarles comunicaciones con fines promocionales, de lo contrario, podrían incurrir en una infracción grave de acuerdo a lo previsto en el citado numeral 2, inciso b del artículo 132° del Reglamento de la LPDP.

De este modo, se puede concluir que el mencionado análisis normativo realizado por la informante implicó evitar que las empresas a las que les prestaba asesoría legal incurran en una práctica sancionable por desconocimiento y/o confusión respecto a la normativa que les resultaba aplicable en virtud a los cambios normativos que se han dado y por la coexistencia de normas que regulaban aspectos similares vinculados al tratamiento de la información personal.

3.2.4 *La omisión de solicitar el consentimiento en materia de protección al consumidor y protección de datos personales. ¿Non Bis In Ídem?*

Sobre este punto, las personas jurídicas de derecho privado -clientes de la informante-, le efectuaron reiteradas consultas vinculadas a si el envío de comunicaciones promocionales sin contar con el consentimiento de sus clientes, prohibidas por el Código de Consumo -lo cual ha sido ampliamente desarrollado en el punto anterior- y, el tratamiento de datos personales sin contar con el consentimiento de sus clientes, prohibido por la LPDP y su Reglamento, podría generar el inicio de dos procedimientos sancionadores contra la misma persona jurídica de derecho privado por los mismos hechos y en base al mismo fundamento jurídico. Ello, a efectos que determinar la contingencia a la que podrían enfrentarse por incumplir las referidas normativas o si, por el contrario, no se podrían iniciar dos procedimientos sancionadores con respecto al mismo hecho.

Sobre el particular, como se indicó al inicio del presente documento, la experiencia profesional de la informante en el Estudio de Abogados Lazo & De Romaña también abarcó brindar asesoría respecto a cuestiones vinculadas a la normativa de protección al consumidor. En ese sentido, dicho conocimiento le permitió estar en la capacidad de analizar ambas normativas y despejar la presente interrogante concluyéndose que la ausencia de consentimiento en ambos supuestos si podría implicar el inicio de dos procedimientos sancionadores, conforme se desarrolla a continuación:

- Ante el Indecopi por infracción del numeral 1, inciso e del artículo 58° del Código de Consumo por: “emplear centros de llamada (*call centers*), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos

para promover productos y servicios, así como prestar el servicio de telemercadeo, a todos aquellos números telefónicos y direcciones electrónicas de consumidores que no hayan brindado a los proveedores de dichos bienes y servicios su consentimiento previo, informado, expreso e inequívoco, para la utilización de esta práctica comercial".

- Ante la Autoridad de Datos Personales por infracción del numeral 2, inciso b del artículo 132° del Reglamento de la LPDP por: "realizar tratamiento de datos personales sin contar con el consentimiento libre, expreso, inequívoco, previo e informado del titular; cuando el mismo es necesario".

Cabe señalar que el inicio de ambos procedimientos administrativos sancionadores no responde a una identidad de sujetos, hechos y fundamentos; ya que ello implicaría atentar contra el principio del *non bis in ídem.*

En tanto, el citado principio del *non bis in ídem* se encuentra recogido en el numeral 11 del artículo 248° del Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, el cual, señala expresamente lo siguiente: "*Non bis in ídem*. No se podrán imponer sucesiva o simultáneamente una pena y una sanción administrativa por el mismo hecho en los casos en que se aprecie la identidad del sujeto, hecho y fundamento".

Al respecto, el Tribunal Constitucional ha mencionado que el referido principio tiene una doble dimensión[40]:

- Procesal: "Nadie puede ser juzgado por los mismos hechos". Lo cual aplica para procedimientos administrativos y procesos judiciales.
- Material: "Nadie puede ser castigado dos veces por un mismo hecho. No pueden recaer dos sanciones sobre el mismo sujeto por la misma infracción, puesto que tal proceder constituiría un exceso del poder sancionador contrario a las garantías propias del Estado de derecho". Así, no se puede imponer una doble sanción por identidad de sujeto, objeto y fundamento.

En esa línea, el Tribunal Constitucional ha indicado que para saber si estamos o no ante la presencia del referido principio de non bis in ídem, se debe verificar la concurrencia de tres presupuestos:

[40] EXP. N°1583-2007-PA/TC, fundamento 10.

> i) Identidad de la persona perseguida (*eadem persona*), lo que significa que la persona física o jurídica a la cual se le persigue tenga que ser necesariamente la misma.
> ii) Identidad del objeto de persecución (*eadem res*), que se refiere a la estricta identidad entre los hechos que sirvieron de fundamento para el inicio tanto en la anterior como en la nueva investigación, es decir, se debe tratar de la misma conducta material, sin que se tenga en cuenta para ello su calidad legal.
> iii) Identidad de la causa de persecución (*eadem causa petendi*), lo que significa que el fundamento jurídico que sirve de respaldo a la persecución tenga que ser el mismo tanto en la anterior como en la nueva investigación, proceso o procedimiento.[41]

En ese sentido, en aquellos casos que se verifique una identidad en el sujeto, objeto y fundamento, se podría alegar que se ha configurado la citada prohibición y, por lo tanto, no podría iniciarse un doble procedimiento, así como la aplicación de una doble sanción administrativa. Por el contrario, si en un caso no concurre la triple identidad, corresponderá la tramitación de dos procedimientos e imponer una o más sanciones por las conductas infractoras que se hayan configurado.

Ahora bien, aterrizando a la consulta realizada, ello no implicaría una vulneración del citado principio; pudiéndose iniciar ambos procedimientos sancionadores, ya que si bien podría existir una identidad en el sujeto (mismo proveedor) y en el objeto (no solicitar el consentimiento del consumidor); no se presentaría una identidad en el fundamento, es decir, en el fundamento jurídico pues los bienes jurídicos tutelados son distintos.

Al respecto, desde el punto de vista protección al consumidor, como se ha mencionado precedentemente, los proveedores tienen la obligación de no realizar prácticas que mermen la libertad de elección de los consumidores.

En ese sentido, el Código de Consumo tutela el derecho que tienen los consumidores que se encuentran directa o indirectamente expuestos o comprendidos dentro de una relación de consumo o, en una etapa preliminar a esta, a elegir libremente los productos o servicios que se les ofrecen en el mercado, dependiendo de los intereses y necesidades que tengan, basándose en su autonomía privada. De esta forma, el bien jurídico protegido es el derecho a la libertad de elección del consumidor aplicable a las relaciones de consumo que se celebren con los consumidores.

Por su parte, desde el punto de vista en materia de protección de datos personales, como se ha indicado en el presente documento, la LPDP establece que todo tratamiento de datos personales requiere el consentimiento del titular de los datos personales; ello de conformidad con el principio del consentimiento. En esa línea, el referido consentimiento

[41] EXP. N° 02493-2012-PA/TC.

debe ser otorgado de manera previa, informada, expresa e inequívoca; de lo contrario podríamos estar ante el riesgo de un tratamiento de datos personales no autorizado por su titular; lo cual constituye una infracción grave de acuerdo a lo previsto en el mencionado numeral 2, inciso b del artículo 132° del Reglamento de la LPDP.

De este modo, se advierte que el bien jurídico tutelado por la normativa en materia de protección de datos personales es la autodeterminación informativa, es decir, el control que debe de tener una persona respecto de su información personal, siendo la única fuente de legitimación para el tratamiento de datos personales por parte de terceros proviene del consentimiento otorgado por el titular de dichos datos personales. Ello, con independencia de la existencia o no de un vínculo comercial o relación de consumo preliminar o en curso.

En ese sentido, si en el marco de un procedimiento administrativo sancionador, el Indecopi o la Autoridad de Datos Personales determinase que se ha incurrido en una infracción al numeral 1, inciso e del artículo 58° vinculado al envío de correos electrónicos sin contar con la autorización del consumidor o al numeral 2, inciso b del artículo 132° referido a tratar datos personales sin contar con el consentimiento de su titular, correspondientemente, dichas autoridades podrían ordenar adicionalmente a la imputación de responsabilidad administrativa, remitir los actuados a la otra autoridad (de consumo o de protección de datos personales, según sea el caso), para que investiguen los hechos pues cautelan bienes jurídicos diferentes siendo que las decisiones que adoptasen dichas autoridades contendría fundamentos jurídicos distintos; no resultando vinculantes entre ellas.

Lo mencionado ratifica la posición respecto a que no existe una duplicidad de procedimientos y sanciones por parte de autoridades distintas respecto de un mismo sujeto, hecho y fundamento.

En conclusión, el envío de comunicaciones promocionales por parte de una persona jurídica de derecho privado en calidad de proveedor o responsable del tratamiento de los datos personales, sin contar con el consentimiento de sus clientes, es una práctica que se encuentra prohibida por el Código de Consumo y, adicionalmente por la LPDP y su Reglamento.

En ese sentido, se podría generar el inicio de un procedimiento administrativo sancionador ante el Indecopi y ante la Autoridad de Datos Personales, lo cual no implicaría que se vulnere el principio de *Non bis in ídem* en la medida que si bien existiría una identidad en el sujeto (persona jurídica de derecho privado) y de hecho (envío de publicidad o promociones respecto de sus productos o servicios sin contar con el consentimiento), no existe una identidad en la causa o fundamento jurídico lo cual se distingue principalmente por el bien jurídico tutelado.

En esa línea, la informante despejó el referido cuestionamiento sobre la posible contingencia a la que podrían verse expuestas las empresas a las que les brinda asesoría en caso de que incumplan con solicitar el consentimiento para el envío de publicidad comercial a sus clientes; siendo que dicha eventual contingencia sería alta en la medida que se podrían iniciar dos potenciales procedimientos sancionadores: (i) por infracción a las normas de protección al consumidor, ya que el bien jurídico protegido es el derecho a la libertad de elección del consumidor; entendido como el derecho que tiene de elegir libremente entre los productos y servicios que se le ofrecen en el mercado en atención a sus intereses y necesidades; y, (ii) otro en materia de protección de datos personales; ya que el bien jurídico protegido en la autodeterminación informativa del titular de los datos personales; entendido como el control de la información que le concierne.

En virtud a lo expuesto en el presente capítulo, se puede advertir que la informante pudo absolver los primeros y principales cuestionamientos que surgieron por parte de las empresas de derecho privado a las cuales les brindó asesoría legal respecto a la interpretación y alcances de la normativa de protección de datos personales, así como su aplicación práctica e interpretación frente a otras normativas.

Las acciones realizadas por la informante permitieron que dichas empresas tengan una comprensión sobre el cumplimiento de sus obligaciones en calidad de titulares de los bancos de datos personales o responsables del tratamiento y, en consecuencia, no incurran en infracciones a la normativa de protección de datos personales, evitándose la imposición de multas.

Capítulo 4

La revolución del *Big Data* y sus implicancias con la privacidad

En relación con este último capítulo, y de acuerdo a lo mencionado al inicio del presente documento, la informante procederá a realizar algunas reflexiones sobre posibles limitaciones que aún presentaría la normativa en materia de protección de datos personales respecto a la reutilización de los datos personales en el contexto de la revolución tecnológica; específicamente para su tratamiento en proyectos de *Big Data*. Asimismo, se planteará una eventual solución referida a la aplicación del test de incompatibilidad que podría, en determinados casos, ayudar a superar algunas dificultades vinculadas al tratamiento de información en los citados proyectos de *Big Data*.

4.1 ¿Qué se entiende por *Big Data*?

Actualmente, nos encontramos en un contexto de globalización, donde las tecnologías de la información y de la comunicación nos han convertido en una sociedad hiperconectada al mundo digital. Cada segundo producimos una gran cantidad de información por la utilización de herramientas tecnológicas, las cuales se han incorporado a nuestra vida. Sobre este punto, el desarrollo de la tecnología informática "ha modificado nuestros hábitos y costumbres de ocio y laborales o profesionales, como consumidores, en nuestras relaciones como ciudadanos con las diferentes administraciones y en las relaciones con otras personas".[42]

En este sentido, no podemos negar el hecho que compartimos un volumen importante de información personal la cual se integra en el universo digital. Ello, ha provocado un aumento desmesurado en la cantidad de datos que se pueden obtener, almacenar, procesar y examinar por parte de organizaciones tanto públicas como privadas. En este contexto, surge el concepto del *Big Data*, el mismo que hace referencia precisamente a ese gran volumen de datos y el tratamiento que se le da.

Al respecto, el Grupo de Trabajo del artículo 29[43], en la Opinión 03/2013 señala que el *Big Data* se refiere "al crecimiento exponencial tanto en la disponibilidad como en el uso automatizado de la información: se refiere a gigantescas cantidades de información digital,

---

[42] GARRIGA, Ana. *Nuevos retos para la protección de datos personales. En la Era digital del Big Data y de la computación ubicua.* Editorial Dykinson. Madrid, 2016.

[43] El Grupo de Trabajo del artículo 29 es creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo el 24 de octubre de 1995 y constituye un órgano consultivo independiente integrado por la Autoridades de Protección de Datos de todos los estados miembros de la UE, el supervisor Europeo de Protección de Datos Personales y la Comisión Europea.

controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos".[44]

Asimismo, se ha indicado que el *Big Data* se define comúnmente haciendo referencia a sus características clave, las cuales con frecuencia se describen como volumen, velocidad y variedad. Lo significativo en el *Big Data* es la forma en la que se utilizan y analizan el gran volumen de datos. Así, el análisis de grandes cúmulos de datos incluye la aplicación de un análisis veloz y sofisticado en donde la información de individuos y de grupos humanos es obtenida de diversas fuentes. Para ello, se utilizan herramientas como la inteligencia artificial con el objetivo de procesar y analizar los datos obtenidos para predecir y anticipar los eventos futuros de esa manera.[45]

Por su parte, la AEPD, ha indicado que "con dicho término se hace referencia al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo".[46]

Como se puede advertir, no existe un concepto universalmente aceptado sobre *Big Data*, siendo que sus definiciones hacen referencia a sus características. Así, puede entenderse el *Big Data* como "el conjunto de tecnologías que permiten tratar cantidades masivas de datos personales provenientes de distintas fuentes a través del uso de algoritmos, con el objetivo de poder otorgarles una utilidad que proporcione valor. Es decir, el *Big Data* permite procesar datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad) dificultan su captura, gestión, procesamiento o análisis por parte de tecnologías y herramientas convencionales".[47]

En tal sentido, podemos concluir que el *Big Data* implica la utilización de tecnologías que tienen la capacidad de captar y analizar: (i) un gran volumen de datos; (ii) cuya velocidad de generación es muy alta; (iii) proveniente de una variedad de fuentes; (iv) que se obtendrá

---

[44] Opinion 03/2013 on Purpose Limitation. Recuperado de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[45] PATERSON, M., & MCDONAGH, M. "*Data Protection in an era of Big Data: The challenges posed by big personal data".* Monash University Law Review. Vol 44, N°1 2018. Recuperado de: https://bridges.monash.edu/articles/journal_contribution/Data_Protection_in_an_Era_of_Big_Data_The_Challenges_Posed_by_Big_Personal_Data/10066145/1

[46] Autoridad Española de Protección de Datos Personales (AEPD) Recuperado de: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

[47] MORALES, Alejandro. "*El Big Data y sus implicancias legales en la Protección de Datos Personales"* en Revista Digital Agnitio. 2017. Disponible en: https://agnitio.pe/articulo/el-big-data-y-sus-implicancias-legales-en-la-proteccion-de-datos-personales/

un valor en función a los objetivos de la organización que los gestione; y, (v) alimentándose de datos veraces; es decir, relevantes y verdaderos.

Cabe señalar que las finalidades que puede tener un proyecto de *Big Data* son variadas. Atendiendo a ello, algunos autores agrupan a los proyectos en categorías en función al objetivo principal que persiguen; conforme se muestra a continuación:

- Inteligencia comercial, la cual engloba a todos aquellos proyectos *Big Data* que persiguen un conocimiento profundo y predictivo de sus clientes. Estos proyectos buscan mejorar la experiencia del cliente, prevenir y evitar que el cliente corte la relación comercial. Asimismo, buscan generar patrones de comportamiento y segmentaciones avanzadas de clientes o la oferta personalizada de productos, servicios y precios.
- Fraude y riesgo: consistentes en la previsión y predicción de posibles actividades fraudulentas de clientes, proveedores o elementos externos (ciberseguridad o prevención de fallos de sistema).
- Eficiencia operativa: se busca optimizar los procesos productivos o de toma de decisiones, incluyendo proyectos asociados al Internet de las cosas, eficiencia en la gestión logística, optimización en la gestión de reclamaciones y devoluciones.
- Monetización: se persigue un beneficio económico directo, a través de la generación de nuevos negocios en entorno digital, apps, empresas *fintech*, intermediación en *e-commerce*, etc.[48]

Como se puede advertir, los usos de estas tecnologías aportan múltiples ventajas, sin embargo, también se genera un impacto en la privacidad. Ello, en la medida que el *Big Data* implica un tratamiento masivo de datos personales, pues se recopilan y analizan datos referentes a personas físicas.

En ese sentido, para garantizar que el uso del *Big Data* no vulnere la normativa en materia de protección de datos personales, se deben de respetar los principios reconocidos en la LPDP, específicamente, los principios de finalidad, proporcionalidad y consentimiento.

Ahora bien, los referidos principios de finalidad, proporcionalidad y consentimiento buscan brindar un nivel adecuado de protección a la información o datos personales de sus titulares; constituyendo también criterios interpretativos al momento de aplicar la normativa ante potenciales vacíos legales. Sin embargo, debemos advertir que los citados principios fueron desarrollados cuando el *Big Data* y las TICs no habían evolucionado al nivel en el que se encuentran actualmente; lo cual puede generar ciertas incompatibilidades entre el uso de la referida tecnología y el cumplimiento de los mencionados principios.

---

[48] PÉREZ, Carlos. "Aspectos Legales del *Big Data*". Revista Índice: Estadística y Sociedad, N° 68. Pág N° 18. 2016. Recuperado de: http://www.revistaindice.com/numero68/p18.pdf

4.2 Problemática actual: reutilización de datos personales

Como se ha indicado, en un contexto de sociedad de la información, el tratamiento masivo de los datos personales a través de la tecnología del *Big Data* puede proporcionar gran valor o utilidad.

"El *Big Data* ayudará a crear nuevas oportunidades de negocio e incluso nuevos mercados y nuevas categorías de empresas. Es de prever que muchas de estas nuevas empresas se sitúen en medio de los flujos de datos, para capturar y analizar la información sobre productos y servicios, proveedores y clientes, o preferencias de consumo".[49]

Estas nuevas oportunidades se generan como consecuencia de hallar nueva información; sin embargo, también se advierten riesgos vinculados a la privacidad de los titulares de los datos personales.

Así pues, la analítica *Big Data* implica la reutilización de datos que fueron obtenidos para una determinada finalidad, otorgándoles nuevas finalidades. Lo indicado colisiona con el principio de finalidad y con el deber de información, contemplados en la normativa de protección de datos personales; los cuales indican que se debe de señalar expresamente la(s) finalidad(es) del tratamiento a las que los datos serán utilizados de forma previa a su tratamiento; siendo que dichas finalidades deber haber sido expresadas con claridad, sin lugar a confusión; especificándose el objeto del tratamiento de los datos personales.

Sin embargo, el *Big Data* es utilizado precisamente para generar nueva información o reutilizar la existente; la cual podrá ser empleada para nuevas finalidades. En este escenario, desde el momento inicial de recopilación de los datos personales no se podría determinar las finalidades ulteriores para las cuales serían utilizados los datos personales; no pudiendo solicitarse el consentimiento como lo indica la LPDP.

Sobre el particular, el procedimiento de anonimización ha sido considerado como una alternativa satisfactoria para superar los inconvenientes que surgen entre utilización del *Big Data* y los principios de consentimiento, finalidad y el cumplimiento del deber de información. Ello, en la medida que el citado procedimiento consiste en el: "Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible".[50] En esa misma línea, el artículo 6° de la LPDP indica que una excepción al principio de finalidad es cuando se ha utilizado un procedimiento de

[49] GIL, Elena. *Big Data, privacidad y protección de datos*. Accésit. Agencia Estatal Boletín Oficial del Estado. Madrid, España. 2017. Págs. 31 y 32. Recuperado de: https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

[50] Artículo 2, numeral 14 de la LPDP. Sobre el particular, un ejemplo de anonimización es la utilización de algoritmos de cifrado.

anonimización y, adicionalmente, el numeral 8 del artículo 14° de la LPDP, precisa que no se requiere solicitar el consentimiento "Cuando se hubiera aplicado un procedimiento de anonimización o disociación".[51]

De este modo, cuando los datos personales han pasado por un procedimiento de anonimización, no se requiere solicitar al titular de dichos datos su consentimiento para su tratamiento respecto de otras finalidades que no fueron establecidas inicialmente; ello en la medida que no sería identificado.

Cabe señalar que un procedimiento de anonimización fracasará en la medida que sea posible identificar al titular del dato personal; lo cual cada vez es más fácil de que suceda por la cantidad de información que maneja un proyecto de *Big Data*. Sobre este punto, la Federal Trade Commission de Estados Unidos ha indicado que: "hay pruebas significativas que demuestran que los avances tecnológicos y la capacidad de combinar diferentes datos puede conducir a la identificación de un consumidor, ordenador o dispositivo, incluso si los datos individuales no constituyen datos de identificación personal".[52]

Por su parte, la AEPD ha indicado que ninguna técnica de anonimización podrá garantizar en términos absolutos la imposibilidad de la reidentificación, ya que existirá siempre un índice de probabilidad de reidentificación el cual se debe intentar atenuar mediante la correspondiente gestión de riesgos.[53]

En ese sentido, para reducir la probabilidad de reidentificación de un conjunto de datos anonimizados, se debería aplicar el Principio de Proporcionalidad respecto de los datos personales que se tratarán en los proyectos de *Big Data*. Esto implicaría que solo se realice tratamiento de aquellos datos personales que sean pertinentes, adecuados y limitados en función a las finalidades que se quieren obtener; minimizándose la cantidad de datos tratados, lo cual podría dificultar la identificación de los titulares de los datos personales con las técnicas del el *Big Data*.

---

[51] Artículo 2, numeral 15 de la LPDP: "Procedimiento de disociación. Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible". Por ejemplo, cifrar la información personal mediante el uso de una clave, y;en caso se quiera descifrar la información se introduce nuevamente la clave.

[52] FEDERAL TRADE COMMISSION (FTC). "Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers" (2012). Pág. 20. Recuperado de: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[53] Orientaciones y garantías en los procedimientos de anonimización de datos personales elaborado por la Agencia Española de Protección de Datos Personales. Pág N° 8. Recuperado de: https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf

En otras palabras, “lo que se busca es que el grado de identificación del individuo esté restringido tanto por la cantidad como por la naturaleza de la información utilizada, ya que algunos detalles revelan más sobre la identidad de una persona que otros. Esto sumado al uso de las técnicas de anonimización y encriptación ayudan a proteger de mejor manera la identidad de los titulares de los datos personales”.[54]

De este modo, el principio de proporcionalidad contribuye a delimitar el universo de datos personales que pueden ser tratados para las finalidades del proyecto a ejecutarse; y, en consecuencia, será más efectivo el procedimiento de anonimización; ya que se aplicará respecto de una menor cantidad de datos personales; dificultando el riesgo de reidentificación y de este modo manteniéndose como una alternativa viable para evitar el conflicto que puede generar la reutilización de datos -propio del *Big Data*-, con la normativa de protección de datos personales.

Ahora bien, debemos mencionar que las técnicas de anonimización siempre van a restringir las formas en las que se pueden utilizar un conjunto de datos. Así, existen casos donde la aplicación de procedimientos de anonimización no constituyen la solución definitiva en la medida que algunos proyectos de *Big Data* requieren la identificación de los titulares de los datos personales para lograr sus objetivos comerciales.

Por ejemplo, un proyecto de *Big Data* de un hipermercado podría estar orientado a predecir mejor qué productos tendrán mayor demanda en una determinada temporada; analizando los patrones de consumo de los clientes. En este supuesto la información se puede manejar de forma anónima. Sin embargo, pensemos en un supuesto donde el mismo hipermercado ofrece a sus consumidores ofertas personalizadas (mediante cupones de descuento) de productos que compran de forma habitual. En este supuesto no sería posible la anonimización, ya que se requieren los datos personales del titular para ofrecerle descuentos personalizados.

Otro ejemplo sería el análisis de *Big Data* realizado por Netflix, la empresa utiliza algoritmos para analizar grandes cantidades de información de los usuarios para determinar el contenido de sus propias producciones y cómo serán distribuidas a efectos de lograr un éxito garantizado. En estos casos, los datos personales pueden ser anonimizados, sin embargo, la misma empresa, según las preferencias de cada usuario, le recomienda qué series, programas, documentales ver, siendo una información que no podría ser gestionada de forma anónima.

---

[54] MORALES, Alejandro. *“El impacto de la inteligencia artificial en el Derecho” en Revista* Advocatus. 2019. Recuperado de: https://revistas.ulima.edu.pe/index.php/Advocatus/article/view/5117/4930

En este sentido, dependiendo de la finalidad del proyecto de *Big Data*, la anonimización podrá considerarse una solución para poder reutilizar los datos obtenidos para una finalidad primaria y darle una finalidad secundaria; sin embargo; en otros casos; no resultará viable esta técnica. Es en este escenario donde se presenta la dificultad de cumplir con la normativa de protección de datos personales.

Así pues, resulta complejo, por un lado, imponerles a las organizaciones que utilizan tecnologías de *Big Data*, especificar de forma previa los fines para los que utilizarán los datos personales y obtener el correspondiente consentimiento por parte de los titulares de los datos personales y; por otro lado, imponerles a las referidas organizaciones que, una vez definidos los usos secundarios, soliciten el consentimiento a cada individuo, lo cual "entrañaría unos costes y unos recursos imposibles de asumir para las empresas, con lo que muchos de estos usos secundarios, y el consiguiente valor que supondrían, quedarían en saco roto".[55]

En atención a lo expuesto, en el siguiente acápite, plantearemos una eventual solución para superar esta situación de riesgo de incumplimiento de la LPDP respecto a la utilización del *Big Data* cuando la información no puede ser anonimizada.

4.3 Aplicación del test de incompatibilidad y los aspectos que deben valorarse para su aplicación

Con la finalidad de superar la situación antes descrita, las autoridades europeas en materia de protección de datos personales, recomiendan someter un proyecto de *Big Data* a un test de incompatibilidad y, si el mismo se supera, el uso del *Big Data* sería acorde con la normativa en materia de protección de datos personales, lo cual, implicaría que no se tenga que solicitar nuevamente el consentimiento para las finalidades ulteriores. De lo contrario, deberá sujetarse a la información y consentimiento previos, verificándose que los datos tratados guarden proporcionalidad con las nuevas finalidades.

Ahora bien, el referido test de incompatibilidad se supera con éxito si se cumplen algunas de las siguientes condiciones[56]:

- Que las finalidades del tratamiento de datos del proyecto *Big Data* se ajusten a lo informado a los interesados en el momento inicial de recabar sus datos; o bien
- Que las finalidades del tratamiento de datos del proyecto *Big Data* sean razonablemente previsibles para los interesados, aun no habiendo sido explícitamente informados en el momento de obtener sus datos; o bien
- El tratamiento de datos resultante del proyecto *Big Data* está justificado por otras causas de legitimación previstas en la normativa de privacidad (como son, por

[55] GIL, Elena. *Big Data, privacidad y protección…* ob. cit. Pág. 133.
[56] PÉREZ, Carlos. *Aspectos legales del Big Data*. Recuperado de: http://www.revistaindice.com/numero68/p18.pdf

ejemplo, el interés legítimo del responsable del tratamiento[57], el cumplimiento de obligaciones legales, contractuales[58], o en atención al interés vital de los interesados).[59]

[57] Sobre el interés legítimo, el artículo 6 del RGPD señala en su numeral f que el tratamiento de los datos personales es lícito "cuando sea necesario para satisfacer el interés legítimo perseguido por el responsable del tratamiento o por un tercero; siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales; en particular cuando el interesado sea un niño".
Asimismo, el RGPD indica en su considerando N° 47 que "Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior".
Cabe señalar que el RGPD menciona algunos ejemplos como prevención del fraude, mercadotecnia directa, transferencia en el mismo grupo empresarial para fines administrativos internos, transmisión a la autoridad competente en casos de actos delictivos o amenazas para la seguridad.
Finalmente, el Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos personales en virtud del artículo 7 de la Directiva 95/46/CE, aprobado el 09 de abril de 2014 por el Grupo de Trabajo del Artículo 29. Recuperado de: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf; establece los factores a tomar en cuenta para realizar una prueba de sopesamiento entre el interés legítimo del responsable o un tercero, y los intereses o los derechos fundamentales del interesado. Ello determinará si el interés legítimo del responsable puede utilizarse como fundamento.
Los factores son los siguientes:

"(i) que exista un interés legítimo del responsable o del tercero que alega dicho interés: para que prevalezca el interés legítimo del responsable el tratamiento, este debe ser necesario y proporcionado. Por ejemplo, un medio periodístico publica una noticia sobre gastos de un funcionario o, el tratamiento de datos con fines de investigación médica (aquí no es solo un interés particular sino de la comunidad en general). También existen otros intereses legítimos como el contexto de una relación contractual.
(ii) el impacto que dicho tratamiento tenga con el interesado: se analiza las repercusiones en los intereses o libertades del interesado. Las consecuencias positivas o negativas que se derivarán del tratamiento. Por ejemplo, que el tratamiento pueda dar lugar a la exclusión de personas o a su discriminación.
(iii) la naturaleza de los datos y la forma del tratamiento: evaluar si el tratamiento afecta a datos sensibles ya que estos pertenecen a categorías especiales de datos. Por ejemplo, el uso de datos biométricos para el acceso a zonas de alto riesgo de un laboratorio. Sobre la forma en que se tratan los datos. Por ejemplo, si los datos se han revelado al público o se han puesto a disposición de un gran número de personas.
(iv) expectativas razonables de los interesados: en relación al uso y la revelación de los datos. Por ejemplo, se analiza la posición del responsable (un abogado o médico); la naturaleza de la relación o del servicio prestado (servicios de *cloud computing* para gestión documental del personal) o obligaciones contractuales que pueden dar lugar a expectativas razonables de limitaciones más estrictas sobre su uso ulterior.
(v) posición del responsable del tratamiento y el interesado: si el responsable del tratamiento de los datos es una persona o una pequeña organización, una gran empresa multinacional o un organismo del sector público, y de las circunstancias específicas, su posición puede ser más o menos dominante respecto del interesado. Una empresa multinacional puede, por ejemplo, tener más recursos y poder de negociación que el interesado individual y, por tanto, puede encontrarse en una mejor posición

Por su parte, la Comisión Europea -órgano ejecutivo, políticamente independiente de la Unión Europea-, ha indicado que los datos personales pueden ser utilizados para otra finalidad que no ha sido prevista inicialmente cuando dicha finalidad responda a (i) un interés legítimo; (ii) se realice para el cumplimiento de un contrato; o (iii) para satisfacer intereses vitales.[60]

Como se puede observar lo indicado por la Comisión Europea se subsume dentro del punto N° 3 del mencionado test de incompatibilidad referido a las causas que legitimarían el tratamiento de datos personales en proyectos de *Big Data*.

Ahora bien, la Comisión Europea añade que si bien existen las referidas causas de legitimación que implicarían utilizar los datos personales para otros fines; este nuevo fin debe ser compatible con el fin original.

Así, a efectos de verificar si existe compatibilidad, la Comisión Europa señala que deben valorarse los siguientes aspectos: (i) relación entre el fin inicial y el nuevo o futuro fin; (ii) el contexto en que se recopilaron los datos. Por ejemplo, si hay una relación entre la empresa que recopila la información y el titular de los datos personales; (iii) el tipo y la naturaleza de los datos, (iv) las posibles consecuencias del tratamiento ulterior; es decir, evaluar si habría una afectación a la persona; (v) la existencia de garantías adecuadas, tales como técnicas de cifrado o de seudonimización.

Lo indicado por la Comisión Europea respecto a la compatibilidad tiene como base lo señalado en el considerando N° 50 del RGPD, el cual indica que a efectos de determinar la referida compatibilidad "debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las

---

para imponer al interesado lo que cree que corresponde a su "interés legítimo". También sería pertinente considerar si el interesado es un niño94 o pertenece de otro modo a algún segmento más vulnerable de la población que requiera protección especial, como, por ejemplo, los enfermos mentales, los solicitantes de asilo o las personas mayores.

El análisis de estos factores no es impedir cualquier impacto negativo sobre el interesado; sino impedir un impacto desproporcionado. Asimismo, el responsable puede utilizar garantías adicionales para limitar un impacto indebido como la minimización de datos, tecnologías de protección de la intimidad, aumento de transparencia, etc".

[58] Por ejemplo, para el desarrollo de contratos en una relación comercial, laboral entre el interesado (titular de los datos) y el responsable y sea necesario para su mantenimiento o cumplimiento.

[59] Por ejemplo, una situación de emergencia de salud.

[60] Portal web de la Unión Europea. Recuperado de: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_es

consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista".

Finalmente, sobre la compatibilidad de fines ulteriores respecto de los iniciales, el Grupo de Trabajo del artículo 29 en la Opinión 03/2013, indica que los siguientes factores son clave para evaluar la compatibilidad entre fines[61]:

- La relación entre los fines para los que se han recogido los datos y los fines del tratamiento posterior: puede haber situaciones en las que el tratamiento posterior estaba más o menos implícito en los fines iniciales, o se asumía como un paso lógico; así como situaciones donde solo existe un vínculo parcial o incluso inexistente con los fines originales. Mientras mayor sea la distancia entre los fines iniciales y los fines del tratamiento posterior; más problemática será la evaluación de compatibilidad.
- El contexto en el que se recogieron los datos y las expectativas razonables de los interesados en cuanto a su uso posterior: se refiere a la relación entre el responsable del tratamiento y el titular de los datos personales. En general, cuánto más inesperado o sorprendente sea el uso posterior; más probable será que se considere incompatible. La evaluación de la compatibilidad deberá ser más estricta si el titular de los datos personales no tuvo suficiente libertad de elección (por ejemplo, una relación contractual) o si los términos del consentimiento fueron pocos específicos. Cuánto más específico y restrictivo sea el contexto de la recogida de datos personales; más limitaciones habrá en cuanto a su uso para finalidades posteriores (por ejemplo, obligaciones contractuales que podrían dar lugar a expectativas razonables de una confidencialidad más estricta en cuanto a su posterior uso). Si el tratamiento posterior se basó en disposiciones legales, la seguridad jurídica y previsibilidad en general podrían sugerir que el uso posterior es adecuado; incluso si el titular de los datos personales no ha sido consciente de todas las consecuencias que su tratamiento puede implicar.
- La naturaleza de los datos y el impacto del tratamiento ulterior en los titulares de los datos personales: se debe evaluar si el tratamiento posterior involucra datos sensibles (como el caso de datos biométricos, información genética, pues este tipo de datos

[61] Dictamen 03/2013 sobre los límites de las finalidades aprobado el 02 de abril del 2013 por el Grupo de Trabajo del artículo 29. Recuperado de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

requieren protección especial). Cuanto más sensible sea la información involucrada, más estrecho será el alcance para el uso compatible. Respecto al impacto, se deben evaluar las consecuencias positivas como las negativas; es decir, si las finalidades ulteriores podrían conducir a una exclusión o discriminación de las personas o si los datos serán tratados por un responsable del tratamiento diferente con consecuencias desconocidas. Cuanto más negativas o inciertas sean las repercusiones del tratamiento posterior, más improbable es que se considere un uso compatible. La disponibilidad de métodos alternativos para alcanzar los objetivos perseguidos por el responsable del tratamiento, con un impacto menos negativo para el interesado, tendría que ser ciertamente una consideración relevante en este contexto.

- Las salvaguardias aplicadas por el responsable del tratamiento para garantizar un tratamiento justo y evitar cualquier impacto indebido sobre los titulares de los datos personales: medidas técnicas como la anonimización parcial o total, seudonimización, separación funcional[62].

Cabe señalar que el numeral 4 del artículo 6° del RGPD ha incorporado a la norma estos criterios para aquellos casos donde se requiere determinar si el tratamiento de datos personales para otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales[63].

De este modo, los factores mencionados ponen en manifiesto algunos criterios que pueden tomarse en consideración para analizar la compatibilidad y determinar si las

[62] El artículo 4.5 del RGPD define la seudonimización como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable" Por ejemplo, sustituir el nombre de una persona por un código o un identificador numérico; de este modo se cambian los datos por seudónimos.

[63] Artículo 6. 4 del RGPD Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

finalidades ulteriores son acordes y pueden armonizarse con las finalidades iniciales que motivaron la recopilación de los datos personales; lo cual podría generar que no se requiera el consentimiento del titular de los datos personales.

Asimismo, algunos de los factores mencionados para evaluar la compatibilidad podrían también ser tomados en consideración para evaluar si se supera la condición N° 2 del Test de Incompatibilidad referido a que las finalidades del tratamiento de datos del proyecto *Big Data* sean razonablemente previsibles para los interesados (titulares de los datos personales), ello en la medida que esa razonabilidad se podrá analizar, verificando diversos criterios tales como la relación entre las finalidades, la naturaleza de los datos que se están tratando o el contexto de su recolección.

Sobre las salvaguardias, la informante considera que más que factores a ser tomados en cuenta para evaluar si se supera alguna de las condiciones del Test de Incompatibilidad; deben constituirse como técnicas que todo proyecto de *Big Data* debe contemplar para asegurar un mayor grado de protección de la información personal. Por ejemplo, garantías jurídicas tales como acuerdos de confidencialidad con cláusulas contractuales que garanticen la privacidad de la información; compromisos de mantener la anonimización, disociación o seudonimización de la información suscritos con los posibles destinatarios de la misma, así como de no realizar ninguna acción para reidentificarla, o auditorias de uso de la información anonimizada.[64]

Sobre el particular, si bien la utilización del citado test de incompatibilidad constituye una medida que podría contribuir a viabilizar algunos proyectos de *Big Data*, en la medida que se superen alguna de sus condiciones, los citados proyectos deben implementar por un lado la privacidad desde el diseño[65] de la arquitectura de la tecnología; sistemas y procedimientos operativos para asegurar un mayor grado de protección de la privacidad (por ejemplo, uso de seudónimos para sustituir la identificación personal o cifrado para codificar mensajes para que solo las personas autorizadas puedan leerlo) y, por el otro lado, la

[64] Código de Buenas Prácticas en Protección de Datos para proyectos *Big Data*. Agencia Española de Protección de Datos Personales. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

[65] Artículo 25° del RGPD: "1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados".

privacidad por defecto[66], la cual comporta que la tecnología esté configurada para que las opciones que por defecto son establecidas por fábrica, sean las más protectoras de la privacidad[67] (por ejemplo, solo se traten los datos necesarios, un plazo de conservación que no se entienda más allá de la finalidad, accesibilidad limitada).

De este modo, el valor creado a través del uso de tecnologías; tendrán siempre en consideración la protección de los titulares de los datos personales. Las medidas de protección de los datos desde el diseño y por defecto se encuentran directamente relacionadas con el principio de responsabilidad proactiva, el cual se encuentra recogido el numeral 2 del artículo 5° del RGPD[68], y se define como: "la necesidad de que el responsable del tratamiento de datos personales aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de los datos es conforme con el Reglamento"[69].

Lo indicado, aplicándolo a proyectos de *Big Data*; implicará que las organizaciones que gestionan estos proyectos estén en la capacidad de determinar qué datos personales tratarán, las finalidades que se buscan alcanzar, las medidas tecnológicas que se utilizarán para proteger los datos personales y todos los aspectos que se vinculen al tratamiento de los datos personales a efectos de tener un panorama claro sobre los potenciales riesgos y disponer de las medidas adecuadas para el respeto de toda la normativa en materia de protección de datos personales.

No podemos ser ajenos a la revolución tecnológica del siglo XXI. Nos encontramos en un entorno digital donde tecnologías como el *Big Data* traen múltiples beneficios a nuestra sociedad. Por ello, en aquellos casos donde nuestra normativa de protección de datos personales nos plantee limitaciones, debemos buscar soluciones que busquen armonizar posibles incompatibilidades, garantizando el respeto al derecho fundamental a la protección de datos personales.

---

[66] "Artículo 25° del RGPD: 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

[67] GIL, Elena. *Big Data, privacidad y protección…* ob. cit. Pág134.

[68] 2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva)"

[69] Agencia Española de Protección de Datos Personales. Recuperado de: https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva

En conclusión, la informante considera que el test de incompatibilidad podría ser una alternativa viable para que determinados proyectos de *Big Data* puedan utilizar datos -que fueron obtenidos para una primera finalidad-, para finalidades ulteriores a las que motivaron su recopilación, cuando no sea posible aplicar procedimientos de anonimización o disociación.

Para ello, en cada proyecto de *Big Data*, se tendrían que evaluar los factores mencionados a efectos de terminar si el titular de los datos personales podría considerar razonablemente previsibles las finalidades ulteriores del proyecto de *Big Data* o si existen causas de legitimación o intereses vitales del titular de los datos personales involucrados que puedan justificar la utilización de su información personal para finalidades adicionales. Adicionalmente, todo proyecto de *Big Data* debe adoptar medidas de privacidad desde el diseño, y por defecto, aplicables con anterioridad al inicio del tratamiento y cuando se esté desarrollando; ello en el marco de garantizar una observancia a la normativa de protección de datos personales, protegiendo así la privacidad de las personas.

Conclusiones

Primera. El derecho a la autodeterminación informativa, mayormente conocido como el derecho a la protección de los datos personales, se encuentra recogido en la Constitución Política del Perú; siendo que luego de dieciocho (18) años de consagrado este derecho en nuestra Constitución. Su desarrollo y regulación se alcanzó con la aprobación de la LPDP y, dos (2) años más tarde, con la publicación de su reglamento. La normativa descrita tiene como objetivo garantizar el derecho fundamental a la protección de los datos personales, reconociendo que toda persona natural tiene el derecho de controlar su información personal y definir el acceso que le puede brindar a terceros respecto de esta. En ese sentido, la normativa regula su adecuado tratamiento y efectivo cumplimiento por parte de aquellas personas naturales o jurídicas públicas o privadas que realicen tratamiento de datos personales.

Segunda. Las disposiciones de la normativa de protección de datos personales entraron en plena vigencia en el año 2015. Precisamente, desde dicho año la informante se desempeñó como asesora legal especializada en protección de datos personales de diversas empresas del sector privado dedicadas a distintos rubros. Es importante mencionar que la presente regulación es transversal a todas las industrias en la medida que efectúen tratamiento de datos personales.

Tercera. La informante en su calidad de asesora legal tuvo la oportunidad de identificar los primeros y principales cuestionamientos que le plantearon las empresas a las cuales les brindaba asesoría, respecto al deber de información y obtención del consentimiento, concretamente, sobre su interpretación, alcances, aplicación práctica y compatibilidad con otras normativas. Así, la informante realizó un análisis jurídico de la normativa aplicable; lo cual permitió poder absolver los cuestionamientos planteados; logrando que las empresas de derecho privado cuya asesoría requirieron, comprendan cómo cumplir con sus obligaciones en calidad de titulares de los bancos de datos personales o responsables del tratamiento y, en consecuencia, no incurran en infracciones a la normativa de protección de datos personales; evitándose la imposición de multas elevadas.

Cuarta. Si bien la normativa de protección de datos personales ha sufrido algunas modificaciones con la finalidad de ser reforzada y fortalecida a efectos de proteger de forma más efectiva a los titulares de los datos personales frente al uso indebido de su información; actualmente la evolución y desarrollo tecnológico que estamos enfrentando como sociedad, conlleva a que el cumplimiento de la normativa presente algunas limitaciones, sobre todo, respecto al tratamiento y reutilización de información personal en proyectos de *Big Data*.

Quinta. Tomando en consideración que no podemos ser ajenos a la revolución tecnológica del siglo XXI, donde tecnologías como el *Big Data* traen múltiples beneficios a nuestra sociedad, una alternativa que podría ser viable para armonizar posibles incompatibilidades, garantizando el respeto al derecho fundamental a la protección de datos personales, sería la aplicación del test de incompatibilidad para determinados proyectos de *Big Data*. Ello, con el objetivo de utilizar datos -que fueron obtenidos para una primera finalidad-, para finalidades ulteriores a las que motivaron su recopilación, cuando no sea posible aplicar procedimientos de anonimización o disociación, no teniendo que solicitarse nuevamente el consentimiento informado y previo a los titulares de los datos personales para utilizar su información para nuevas finalidades. Sin embargo, dependerá del análisis de cada caso, o proyecto en concreto, para determinar si podría superarse alguna de las condiciones establecidas en el mencionado test. Cuando el mismo no pueda ser utilizado, se deberá cumplir con las obligaciones exigidas en la normativa vinculadas a la obtención del consentimiento.

Lista de abreviaturas

AEPD	Agencia Española de Protección de Datos Personales.
ANPDP	Autoridad Nacional de Protección de Datos Personales.
ANTAIP	Autoridad Nacional de Transparencia y Acceso a la Información Pública.
ANTAIPDP	Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.
ARCO	Acceso, Rectificación, Cancelación y Oposición.
DGPDP	Dirección General de Protección de Datos personales.
DL1353	Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública. Fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
LPDP	Ley de Protección de Datos Personales.
RDPD	Reglamento General de Protección de Datos.

UNIVERSITAS STUDIORUM PIURENSIS

Lista de referencias

Agencia Española de Protección de Datos Personales. Recuperado de: https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/3-principios-relativos-al-tratamiento/FAQ-0208-que-es-el-prinipio-de-responsabilidad-proactiva

Autoridad Española de Protección de Datos Personales (AEPD) Recuperado de: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

CASTILLO, Luis, *Comentarios al Código Procesal Constitucional*, 2ª edición, Palestra Editores, Lima, 2006 (1053 al 1068).

Código de Buenas Prácticas en Protección de Datos para proyectos *Big Data*. Autoridad Española de Protección de Datos Personales. Recuperado de: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

Dictamen 03/2013 sobre los límites de las finalidades; aprobado el 02 de abril del 2013 por el Grupo de Trabajo del Artículo 29. Recuperado de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos personales en virtud del artículo 7 de la Directiva 95/46/CE, aprobado el 09 de abril de 2014 por el Grupo de Trabajo del Artículo 29. Recuperado de: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

Exposición de Motivos del Decreto Legislativo N° 1353. Recuperado de https://www.congreso.gob.pe/Docs/comisiones2016/ConstitucionReglamento/files/dl_1353_(1).pdf

FEDERAL TRADE COMMISSION (FTC). "Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers" (2012). Pág. 20. Disponible en: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

GARRIGA, Ana. "*Nuevos retos para la protección de datos personales. En la Era digital del Big Data y de la computación ubicua"*. Editorial Dykinson, Madrid, 2016.

GIL, Elena. *Big Data, privacidad y protección de datos*. Accésit. Agencia Estatal Boletín Oficial del Estado. Madrid, España. 2017. Págs. 31 y 32. Recuperado de: https://www.aepd.es/sites/default/files/2019-10/big-data.pdf

LINARES, Sebastián. “En contenido constitucional del derecho fundamental a la autodeterminación informativa en el Derecho Constitucional Peruano”. Recuperado de: https://pirhua.udep.edu.pe/handle/11042/4163

MORALES, Alejandro. “El *Big Data* y sus implicancias legales en la Protección de Datos Personales” en Revista Digital Agnitio. 2017. Disponible en: https://agnitio.pe/articulo/el-big-data-y-sus-implicancias-legales-en-la-proteccion-de-datos-personales/

Opinion 03/2013 on Purpose Limitation. Recuperado de: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Orientaciones y garantías en los procedimientos de anonimización de datos personales elaborado por la Agencia Española de Protección de Datos Personales. Pág N° 8. Di Recuperado de: https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf

PATERSON, M., & MCDONAGH, M. Data Protection in an era of *Big Data*: The challenges posed by big personal data. Monash University Law Review. Vol 44, N°1 2018. Recuperado de: https://bridges.monash.edu/articles/journal_contribution/Data_Protection_in_an_Era_of_Big_Data_The_Challenges_Posed_by_Big_Personal_Data/10066145/1

PÉREZ, Carlos. “Aspectos Legales del *Big Data*”. Revista Índice: Estadística y Sociedad, N° 68. Pág N° 18. 2016. Recuperado de: http://www.revistaindice.com/numero68/p18.pdf

Perú. Ministerio de Justicia y Derechos Humanos (2022). *Organización. Autoridad Nacional de Protección de Datos Personales*. Recuperado de https://www.gob.pe/institucion/anpd/organizacion

Portal web de la Unión Europea. Recuperado de: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_es

Proyecto de Ley N° 7870 / 2020-PE; Proyecto de ley que crea la Autoridad Nacional Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de: https://cdn.www.gob.pe/uploads/document/file/1939689/OFICIO%20N°%20337-2021-PR.pdf.pdf

RUBIO, Marcial y otros. *Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional: análisis de los artículos 1,2 y 3 de la Constitución.* Fondo Editorial de la Pontificia Universidad Católica del Perú, Lima, 2003.

Documentos legales

Decreto Legislativo N° 1390 que modifica el Código de Protección y Defensa del Consumidor.

Decreto Supremo 003-2013-JUS, Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

Decreto Supremo, N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General

Directiva Administrativa N°294-MINSA/2020/OGTI, "Directiva Administrativa que establece el tratamiento de los datos personales relacionados con la salud o datos personales en salud"

Directiva N° 005-2009/COD-Indecopi, Directiva de Operación y Funcionamiento del Registro de Números Telefónicos y direcciones de correo electrónico excluidos de ser destinatarios de publicidad masiva registro "Gracias…No insista"

El Reglamento (UE) 2016/670 del Parlamento Europeo y del Consejo, del 27 de abril de 2016.

EXP. N°02493-2012-PA/TC.

EXP. N°1583-2007-PA/TC.

EXP. N°4739-2007-PHD/TC.

Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado "SPAM"

Ley N° 29571, Código de Protección y Defensa de Consumidor.

Ley N°29733, Ley de Protección de Datos Personales.

Ley N°31301, Nuevo Código Procesal Constitucional.

Oficio N°137-2015-JUS/DGPDP con fecha 04 de marzo de 2015.

Oficio N°140-2014-JUS/DGPDP con fecha 21 de marzo de 2014.

Oficio N°167-2017-JUS/DGPDP con fecha 03 de abril de 2017.

Oficio N°35-2020-JUS/DGPDP con fecha 22 de julio del 2020.

Oficio N°873-2013-JUS/DGPDP con fecha 18 de noviembre de 2013.

Opinión Consultiva N°032-2021-JUS/DGTAIPD con fecha 17 de agosto de 2021

Opinión Consultiva N°56-2020-JUS/DGTAIPD con fecha 18 de diciembre de 2020.

Reglamento de la Ley N°28493, que regula el envío de correo electrónico comercial no solicitado (SPAM), aprobado por Decreto Supremo N° 031-2005-MTC.