

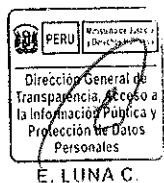
EXPOSICIÓN DE MOTIVOS

I. INTRODUCCIÓN

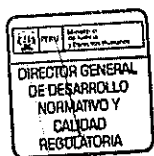
El avance de la tecnología que se ha dado en los últimos años se ha visto acelerada por la pandemia generada por la COVID-19, lo cual permitió un incremento exponencial de las tecnologías digitales y su uso por parte la ciudadanía que tuvo que consumir los servicios y productos de manera digital, además de las organizaciones del sector privado y entidades públicas que tuvieron que digitalizar los procesos que previamente los realizaban de manera presencial.

En ese contexto, si bien el uso de las tecnologías digitales trae múltiples beneficios para la sociedad puesto que permiten, entre otros, mejorar la prestación de servicios o generar nuevos, el desarrollo de actividades productivas, educacionales o de salud, la competitividad y el acceso a la información y el desarrollo, con ello se coadyuva al fortaleciendo del ecosistema digital y el desarrollo de una economía digital en nuestro país, también representa un aumento exponencial de recopilación y uso de datos, entre ellos datos personales. De manera general, en el año 2017 el flujo de datos a través de las redes de internet era de más de 45.000 GB (gigabytes) por segundo y para el año 2022 se estimaba 150.700 GB por segundo¹.

Conforme a la normativa peruana de protección de datos personales, los datos personales son cualquier información que identifica o hace identificable a una persona natural². Asimismo, la normativa indica que esos datos pueden tener el carácter sensible³, cuando se refieran a un aspecto íntimo de la persona, tales como, sus preferencias personales, información de salud, datos genéticos, opiniones o convicción políticas, entre otros. Así, en el mundo digital, los datos personales son el recurso o activo estratégico que impulsa las actividades esenciales, comerciales y que contribuyen nuevos avances científicos o uso de tecnologías digitales.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

En línea con lo expuesto en los párrafos precedentes, la Organización de las Naciones Unidas, mediante Resolución aprobada por la Asamblea General sobre las tecnologías de la información y comunicaciones para el desarrollo⁴, señaló que los derechos de las personas también deben protegerse en internet, y que no sólo debería considerarse como una visión para el desarrollo económico y la propagación de las tecnologías y las comunicaciones, sino también de avances para el ámbito de los derechos humanos y las libertades fundamentales. Además de ello, en la Resolución sobre el derecho a la privacidad en la era digital⁵, indicó que el rápido desarrollo tecnológico permite que todas las personas puedan hacer uso de las tecnologías de la información, lo que incrementa el riesgo que los gobiernos, las empresas y personas puedan llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o transgresión de los derechos humanos, en particular del derecho a la privacidad.

Aunado al aumento exponencial de las tecnologías digitales, se debe observar que la aceleración del comercio electrónico representa un incremento considerable de flujo transfronterizo de datos personales, ya que los proveedores pueden encontrarse fuera

¹ Conferencia de Naciones Unidas sobre Comercio y Desarrollo. El valor y el papel de los datos en el comercio electrónico y la economía digital y sus implicancias para el comercio y el desarrollo inclusivos. En: https://unctad.org/system/files/official-document/tdb_ede3d2_es.pdf

² Artículo 2, inciso 4 de la Ley N.° 29733, Ley de Protección de Datos Personales.

³ Artículo 2, inciso 5 de la Ley N.° 29733, Ley de Protección de Datos Personales.

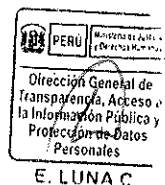
⁴ Resolución A/RES/71/212 https://www.iri.edu.ar/wp-content/uploads/2017/08/A2017CoopDod006_AG71212.pdf

⁵ Resolución A/RES/75/176 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/79/PDF/N2037179.pdf?OpenElement>

del territorio peruano, siendo necesario que se cuente con una regulación robusta que permita generar la confianza entre los usuarios y las empresas. Así también, se debe fortalecer el marco normativo a fin de que se pueda otorgar adecuadas garantías que salvaguarden los datos a terceros países que no cuenten con un nivel adecuado de datos personales, y así se facilite la circulación de los datos personales y mejore la economía digital y la vida social en el país.

En el Perú, la normativa de protección de datos personales data del año 2011 – Ley N.º 29733, y su reglamento en el año 2013, aprobado por Decreto Supremo N.º 003-2013-JUS, las mismas que fueron modificadas en el año 2017, a través del Decreto Legislativo N.º 1353, Decreto Legislativo 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, y su Reglamento aprobado por Decreto Supremo N.º 019-2017-JUS. Dichas normas modificatorias, si bien consideraron disposiciones respecto a las definiciones de los sujetos obligados al cumplimiento de las disposiciones en materia de protección de datos, obligaciones, limitaciones para el consentimiento para el tratamiento de datos, así como los relacionados a las tipificaciones administrativas, no se consideraron los riesgos asociados al incremento del uso de la tecnología en la era digital, lo cual representa mayores riesgos para los peruanos.

En ese sentido, debido a los avances mencionados y los riesgos en el entorno digital, resulta necesario establecer un nuevo reglamento más sólido que eleve los estándares regulatorios con el fin primario de salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital, especialmente en materia de protección de datos personales, garantizando que las personas naturales puedan tener el control de su información personal. Para ello, la propuesta normativa tiene en cuenta que el derecho a la protección de datos no es un derecho absoluto, sino que requiere un equilibrio y ponderación con otros derechos humanos, en observancia de los principios de proporcionalidad, necesidad y legalidad.

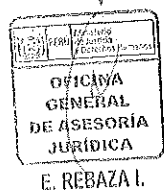


II. FUNDAMENTO TÉCNICO DE LA PROPUESTA NORMATIVA

2.1 ANÁLISIS DEL ESTADO SITUACIONAL

De acuerdo con la información reportada por el Instituto Nacional de Estadística e Informática (INEI) se observa que en el Perú⁶, respecto al trimestre julio - setiembre del 2022, el 74,2% de la población de 6 y más años de edad del país usa Internet. Así, se indica que, respecto a similar trimestre de 2021, se observa una disminución de 2,0 puntos porcentuales al pasar de 76,2% a 74,2%. Asimismo, al compararlo con lo registrado en similar trimestre del año 2020, se observa un incremento de 3,8% y con relación al trimestre del año 2019 (prepandemia), se incrementó en 14,0 puntos porcentuales.

Así también, se resaltó que el 95,0% de la población de 19 a 24 años, el 88,8% de 12 a 18 años y el 87,1% de 25 a 40 años son los mayores usuarios de Internet. Entre los niños de 6 a 11 años usan Internet el 59,5%. En la población de 60 y más años solo usa Internet el 36,4%.



⁶<https://cdn.www.gob.pe/uploads/document/file/4001765/informe%20Técnico%3A%20TIC%20III%20Trimestre%202022.pdf?v=1672262394>

Perú: Población de 6 años y más de edad que hace uso de Internet, según grupos de edad

Trimestre: Julio-Agosto-Septiembre 2019, 2020, 2021 y 2022

(Porcentaje del total de población de 6 años y más de edad de cada grupo de edad)

Grupos de edad	Jul-Ago-Sept 2019	Jul-Ago-Sept 2020	Jul-Ago-Sept 2021	Jul-Ago-Sept 2022 P/	Variación absoluta (Puntos porcentuales)		
					2022/2019	2022/2020	2022/2021
Total	60,2	70,4	76,2	74,2	14,0	3,8	-2,0 **
6 a 11 años	41,1	69,8	82,4	59,5	18,4	-10,3	-22,9 ***
12 a 18 años	77,4	85,8	92,9	88,8	11,4	3,0	-4,1 ***
19 a 24 años	88,5	90,9	93,7	95,0	6,5	4,1	1,3
25 a 40 años	72,6	79,5	85,9	87,1	14,5	7,6	1,2
41 a 59 años	51,7	60,4	65,9	70,5	18,8	10,1	4,6 ***
60 y más	23,2	33,4	34,3	36,4	13,2	3,0	2,1

* Existe diferencia significativa, con un nivel de confianza del 90%.

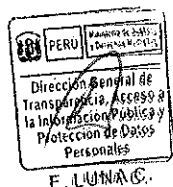
** La diferencia es altamente significativa, con un nivel de confianza del 95%.

*** La diferencia es muy altamente significativa, con un nivel de confianza del 99%.

P/ Preliminar.

Fuente: Instituto Nacional de Estadística e Informática - Encuesta Nacional de Hogares.

El mismo informe del INEI indica, que en cuanto a las actividades que realiza la población usuaria de internet, el 92,9% de la población de 6 y más años de edad navega en Internet para comunicarse, 88,1% utiliza Internet para realizar actividades de entretenimiento como juegos de videos y obtener películas o música y el 78,9% recurre a Internet para obtener información.



Perú: Población de 6 años y más de edad por sexo y grupos de edad, según tipo de actividad que realiza en Internet

Trimestre: Julio-Agosto-Septiembre 2022 P/

(Porcentaje sobre el total de usuarios de Internet)

Actividades	Total	Sexo		Grupos de edad	
		Hombre	Mujer	6 a 24 años	25 y más años
Comunicarse (e-mail, chat, etc)	92,9	92,5	93,3	84,9	98,3
Obtener información	78,9	80,0	77,7	82,0	76,9
Actividades de Entretenimiento (juego de video, obtener películas, música, etc).	88,1	89,1	87,0	89,6	87,0

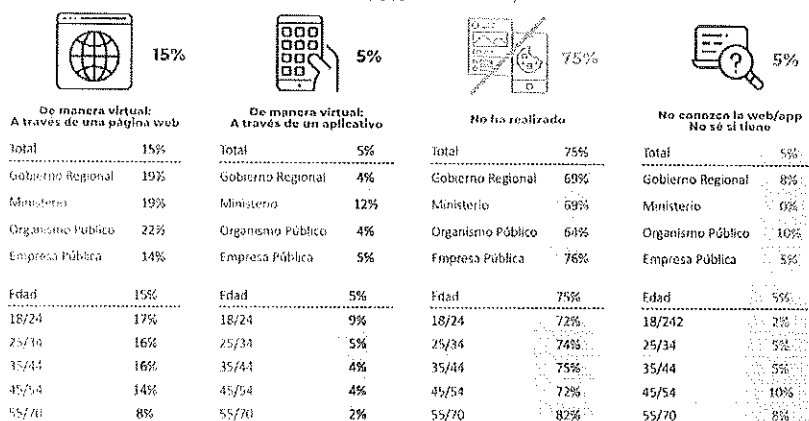
P/ Preliminar.

Fuente: Instituto Nacional de Estadística e Informática - Encuesta Nacional de Hogares.

En la misma línea, la Encuesta de satisfacción ciudadana a nivel regional, realizada por Datum Internacional en el 2021⁷, se muestra información sobre la percepción de la ciudadanía en cuanto a su acceso al internet para realizar gestiones o trámite con entidades públicas y se señala que 8 de cada 10 personas no ha realizado trámites de manera virtual en entidades públicas durante el periodo de pandemia por el COVID 19 (75% no lo hizo y 5% no conoce de páginas web o aplicativos de las entidades).

⁷ Cfr. <https://cdn.www.gob.pe/uploads/document/file/3792943/Encuesta%20Regional%202021.pdf.pdf?v=1666800634>

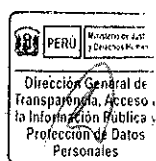
¿Durante la pandemia de la COVID-19, ¿ha realizado gestiones/trámites a través de la página web y/o aplicaciones (app) de entidades públicas?



Total 100% (Base: 410 personas)

Fuente: Datum Internacional

En cuanto a los motivos por los que no realizaron trámites en forma virtual fueron que “no confían en que la gestión se lleve a cabo efectivamente” (duda relevante entre los jóvenes de 18 a 34 años), “lo complicado de su manejo” (respuesta que prevalece entre las personas mayores de 45 años) y otra respuesta importante fue **“temor que se puedan filtrar los datos personales”**.



E. LUNA C

¿Cuál es la principal razón por la que no ha realizado gestiones/trámites a través de la página web o aplicaciones (app) de entidades públicas?

entre quienes no han realizado gestiones/trámites en entidades públicas a través de la página web o app - por tipo de entidad -

	Total	Gobierno Regional	Ministerio	Organismo Público	Empresa Pública
No confío que se haga el trámite	25%	24%	12%	26%	25%
No fue necesario	24%	25%	32%	23%	24%
Es muy complicado su manejo	22%	24%	26%	17%	22%
No es seguro, pueden filtrarse mis datos	19%	13%	2%	7%	19%
No conozco las aplicaciones, no sé usar	2%	4%	28%	7%	2%
Otro	8%	10%	0%	2%	0%
Total	100% (194)	100% (54)	100% (93)	100% (53)	100% (77)

Total 100% (Base: 410 personas que no realizaron gestiones/trámites en entidades públicas a través de la página web o app)

Fuente: Datum Internacional

Concordante con lo anterior, la estadística de DATUM muestra que en cuanto al motivo por el que desconfían de la entidad para realizar trámites en línea, es porque no es seguro y hay estafas.



G. VALDIVIESO R



E. REBAZA I.

¿Cuál es el principal motivo por el que desconfía en esta entidad?
 ¿cómo quieren desconfiar en la entidad
 por entidades

	Total	Gobierno Regional	Ministerio	Organismo Público	Empresa Pública
No es seguro, hay estafas, documentos se pierden	29%	19%	5%	19%	30%
Mala atención, mal servicio	18%	12%	91%	0%	18%
No dan solución a mi reclamo, demora en la solución	12%	20%	1%	23%	17%
No confío, me mintieron	10%	6%	1%	9%	11%
No brindaron información, orientación incorrecta	9%	7%	0%	14%	9%
Demora en la atención, hay colas	6%	9%	1%	12%	6%
No le gusta la modalidad virtual	4%	0%	0%	0%	5%
No hay facilidades para los trámites, son engorrosos	4%	3%	1%	10%	4%
Total	100%				

Base: 463 que desconfían en la entidad

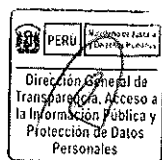
Fuente: Datum Internacional

Conforme se advierte, la población peruana viene incrementando su presencia en el entorno digital, sobre todo dicha población es cada vez más joven, por ello resulta importante se fortalezcan las medidas preventivas que generen obligaciones para aquellos que recolectan y usan los datos personales a fin de evitar riesgos para los mismos. Así también, toda la población, y en especial los niños y jóvenes deben tomar conciencia, que al momento que acceden a internet otorgan muchos datos y que es su responsabilidad de cuidarla y saber para qué se están entregando, ya que dichos datos ya representan un valor en el entorno digital.

Además, es importante mencionar la Resolución de la Organización de la Naciones Unidas adoptada el 02 de julio de 2018, sobre la Promoción, protección y disfrute de los derechos humanos en internet, mediante la cual reafirma la importancia de la protección y garantías para ejercicio de los derechos humanos en internet, ya que señala su preocupación por la recolección, procesamiento y utilización arbitrarias o ilícitas de los datos personales en internet y que puede constituir una violación de los derechos humanos, por ello: *"Exhorta a los Estados a hacer frente a los problemas de seguridad en Internet de conformidad con sus obligaciones internacionales de derechos humanos para garantizar la protección en línea de los derechos humanos, en particular la libertad de opinión y de expresión, la libertad de asociación y la privacidad, especialmente por conducto de instituciones nacionales democráticas y transparentes, sobre la base del estado de derecho, y de un modo que garantice la libertad y la seguridad en Internet para que esta siga siendo una fuerza dinámica que genere desarrollo económico, social y cultural"*.

2.2 DESCRIPCIÓN DEL PROBLEMA PÚBLICO

A nivel internacional, el informe de la Oficina del Alto Comisionado de la Organización de las Naciones Unidas para los Derechos Humanos sobre la privacidad en la era digital, advierte las amenazas que enfrenta la intimidad de las personas por el uso de las nuevas herramientas tecnológicas, por lo se exhorta el control a través de una regulación eficaz.⁸ Así también, la resolución aprobada por la Asamblea general de la Organización de las Naciones Unidas del 16 de diciembre de 2020, señala que las violaciones y transgresiones al derecho a la privacidad en la era digital pueden afectar a todas las



E. LUNA C.



G. VALDIVIESO R.

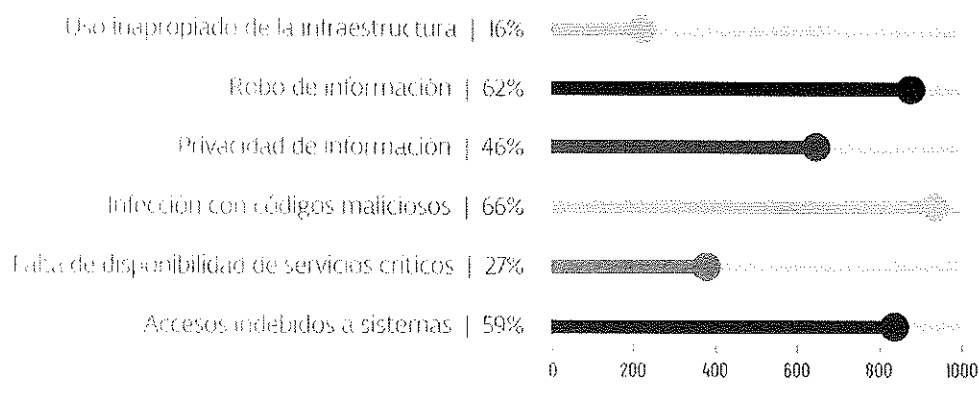


E. REBAZA I.

⁸ Cfr. <https://digitallibrary.un.org/record/1298042>

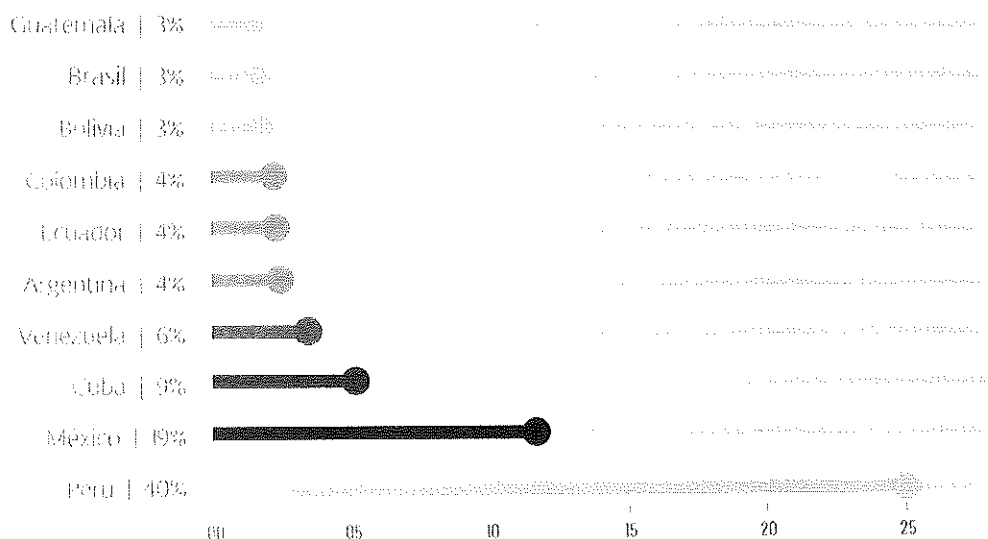
personas y tener repercusiones particulares en las mujeres, así como niños, sobre todo en las niñas y las personas vulnerables y marginadas.⁹

Es importante mencionar, que, durante el 2022, conforme al ESET Security Report en Latinoamérica¹⁰, se ha indicado que el Perú (18%), es el país que tiene mayor cantidad de incidentes de seguridad, seguido de México (17%), Argentina (11%) y Ecuador (9%). Además, se informó que la segunda preocupación en materia de ciberseguridad, es el robo de información con 62%.

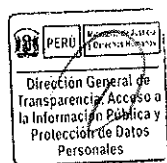


Fuente: Eset Report

Así también, el Reporte muestra que dentro de las nuevas incidencias de seguridad se encuentran los "spyware", que es una incidencia relacionada a robo de datos y el espionaje, siendo en Latinoamérica, Perú el país más afectado con 40% de las detecciones, y le sigue a México el 19% y el resto de los países con menos del 10% de malware espía detectado.



Fuente: Eset Report



E. LUNA C.



G. VALDIVIESO R.



E. REBAZA I.

⁹ <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/371/79/PDF/N2037179.pdf?OpenElement>

¹⁰ <https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf>

En el ámbito nacional, el Centro Nacional de Seguridad Digital, creado por el Decreto de Urgencia N.º 007-2020 que crea el Marco de Confianza Digital, mediante Comunicado N.º 007-2022-PCM/SGTD dio cuenta de la filtración de datos contenido en bancos de datos personales de titularidad de RENIEC. Así, la Autoridad Nacional de Protección de Datos Personales inició las acciones de fiscalización, con el fin de determinar si existen indicios razonables para el inicio de un procedimiento sancionador contra quienes resulten responsables de obtener en forma irregular y difundir datos personales de ciudadanos. Además, la Autoridad detectó que se estarían utilizando las cuentas asignadas a diversas entidades públicas para comercializar los datos de identificación de las personas, por lo que se estarían vulnerando los principios de consentimiento y finalidad, al margen de la naturaleza delictiva de estas acciones. Se indicó que los hallazgos se pondrán en conocimiento de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú y de las demás instancias competentes.¹¹

Sin embargo, debido a que la obligación de comunicar los incidentes de seguridad que involucren datos personales solo corresponde a las entidades públicas, y a determinados proveedores de servicios digitales, la Autoridad Nacional de Protección de Datos del Ministerio de Justicia y Derechos Humanos, no ha tomado conocimiento de otros incidentes de seguridad que se han generado, lo que cual representa un riesgo ya que no permite que se pueda restituir de alguna forma el daño generado, sobre todo cuando existen reportes de seguridad que muestran al Perú como uno de los países con mayor cantidad de incidentes de seguridad.

Conforme se advierte, hoy en día, la mayor cantidad de incidencias de seguridad se encuentran relacionadas con el robo de información personal, por lo que es necesario que se produzcan modificaciones al reglamento de protección de datos respecto a las medidas mínimas que se deben implementar sobre seguridad digital de datos personales, así como establecer, para determinados casos, la figura del Oficial de Datos Personales, quien permitirá asegurar el cumplimiento de la normativa de protección de datos al interior de la organización o entidad pública. Si bien el rol del Oficial de Datos Personales ya fue creado a través del Reglamento del Decreto Legislativo N.º 1412, aprobado por Decreto Supremo N.º 029-2021-PCM, su ámbito de aplicación solo corresponde para las entidades de la Administración Pública, existiendo así un vacío en la regulación.



E. LUNA C.



G. VALDIVIESO R.



E. REBAZA I.

Por otro lado, con la aceleración de la tecnología y el uso de nuevos servicios digitales, se han planteado nuevos retos para la protección de datos personales, ya que la recopilación y el intercambio de datos para comprar o vender productos o servicios se ha visto rápidamente aumentada. Muestra de ello, es el sector de comercio electrónico en el Perú (*ecommerce*), ya que según la publicación realizada por ECOMMERCE NEWS¹², que recoge el informe de la Cámara Peruana de Comercio Electrónico (CAPECE), se indica que, al cierre del año 2021, el 41.8% de peruanos (13.9 millones) realizaron sus compras online por primera vez, a comparación del año 2019, previo a la pandemia, que era el 18.6% (6 millones).

Así, estos avances requieren un marco normativo más sólido y coherente con la rápida recopilación de millones de datos personales de peruanos, a decir de aclarar en el nuevo reglamento otros tipos de datos personales que son recopilados como los identificadores en línea (dirección IP o identificadores de dispositivos móviles, entre otros) o los datos de localización, además de actualizar principios que guíen el actuar de los responsables del tratamiento de datos personales, como los de transparencia y responsabilidad

¹¹ <https://www.gob.pe/institucion/minjus/noticias/608291-autoridad-nacional-de-proteccion-de-datos-personales-inicia-investigacion-y-advierte-que-filtracion-de-datos-es-infraccion-muy-grave>

¹² Ver: <https://www.ecommercenews.pe/ecommerce-insights/2022/crecimiento-del-comercio-electronico-en-peru.html>

proactiva. Aunado a ello, se debe establecer disposiciones claras sobre el tratamiento de datos para fines de marketing y prospección comercial sin consentimiento válido que realizan las empresas.

En línea con lo expuesto, la aparición de nuevas apps que ofrecen nuevos servicios y el uso intensivo de redes sociales, generan nuevos retos debido a que los datos personales son transferidos de una forma más rápida a países fuera del territorio peruano, así como la difusión de datos personales que realizan las personas a una mayor escala, muestra de ellos es el resultado del Digital 2022 Global Overview Report¹³ en el que se hace visible el impacto de los dispositivos móviles, las apps y la publicidad en los usuarios peruanos. Así, el Reporte señala que 21.89 millones de personas son usuarios activos de internet desde cualquier dispositivo electrónico (smartphone, laptop, consola de video juego, TV, entre otro), también que el 83.8% de la población total del Perú es usuaria activa en redes sociales, y que el 48.2% de los usuarios son mujeres y el 51.8% son hombres.

De acuerdo con ello, el avance de las nuevas tecnologías y el uso de nuevos servicios digitales por parte de los peruanos, requiere de un marco normativo más sólido y coherente con instrumentos normativos internacionales como los Principios Actualizados de la Organización de Estados Americanos, el Reglamento de Protección de Datos Personales, el Convenio 108+, que permitan generar confianza en el entorno digital y así también se desarrolle la economía digital dentro del país y con otros países.

Finalmente, el Perú se encuentra en proceso de evaluación para adhesión a la Organización para la Cooperación y el Desarrollo Económico (OCDE), por ende, el proyecto de Reglamento recoge las recomendaciones que la organización ha dispuesto para sus países miembros en materia de protección de datos. A decir, de las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, lo que genera contar una legislación actualizada en materia de protección de datos, elevando al país a mayores niveles adecuados de protección de datos, promoviendo la economía digital y la expansión de mercados globales con un tratamiento adecuado de datos personales.

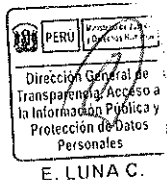
III. CONTENIDO

A continuación, se desarrolla el sustento de los principales aspectos desarrollados en el nuevo Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales:

3.1. Definiciones

En el artículo de definiciones, se incorporan nuevos términos que permiten un mejor entendimiento de las disposiciones en el nuevo Reglamento, a decir de: "Elaboración de perfiles", "Fines de tránsito", "Incidente de seguridad de datos personales", "Oficial de datos personales", "Representante" y "Tratamiento".

Las nuevas tecnologías (inteligencia artificial, internet de las cosas, macrodatos, entre otros) y los servicios digitales que se brindan a los ciudadanos de manera más rápida y personalizada en sectores como financiero, de salud, seguros, publicidad, turismo, entre otros, ha generado un nuevo tratamiento de datos personales, denominado "Elaboración de perfiles", el cual permite evaluar de manera constante y específica aspectos de una persona natural como sus preferencias personales, situación económica, intereses, localización, hábitos de la persona, entre otros que contribuyan a la toma de decisiones.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

¹³ <https://branch.com.co/marketing-digital/estadisticas-de-la-situacion-digital-de-peru-en-el-2021-2022/>

Así, esta nueva forma de tratamiento plantea nuevos retos para el derecho a la protección de datos personales, que requiere de garantías adecuadas, las mismas que han sido incorporadas en el nuevo Reglamento.

En cuanto a la denominación "Fines de tránsito", la finalidad de su incorporación es cubrir el vacío del reglamento anterior, a efectos de que pueda interpretarse de manera adecuada la excepción al ámbito de aplicación territorial establecida en el inciso 6 del párrafo 5.1 del artículo V del nuevo Reglamento.

Por su parte, se incorporan las definiciones de "Oficial de datos personales" y de "Incidente de seguridad de datos personales", que son términos que van a permitir dar mayor claridad en el cumplimiento de las obligaciones establecidas al responsable de tratamiento, y encargado de tratamiento, cuando corresponda. De esta forma, sus alcances son desarrollados en el punto 3.5 del presente apartado.

Además, se incluye la definición de "Representante", si bien no es una figura nueva, ya que la misma se encontraba establecida en el anterior reglamento, en el que se establecía de manera general que el responsable debía proveer los medios que resulten necesarios para el cumplimiento de lo que dispone la Ley y su reglamento y designará un representante. El problema de la disposición anterior es que no se establecía quién era el representante ni en qué supuestos específicos debía nombrarse, siendo estos los asuntos que busca solucionar el nuevo Reglamento.

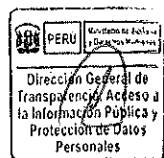
De esta forma, el representante puede ser una persona natural o jurídica designada de manera expresa por el responsable, titular o encargado para fines del tratamiento de datos personales, de conformidad con los párrafos 5.2, 5.3 y 5.4 del artículo V del presente reglamento. El representante, es el punto de contacto con la Autoridad Nacional de Protección de Datos Personales y debe atender las consultas o requerimientos de información que le realiza, así como las realizadas por los titulares de datos personales.

Por último, respecto a las nuevas incorporaciones, se añade la definición de "Tratamiento", en el sentido general de: "Cualquier operación o procedimiento técnico, automatizado o no, que se efectúe sobre datos personales o conjunto de datos personales", ello debido a que se requiere una definición amplia que pueda comprender los nuevos procedimientos técnicos que surgen aparejados de la innovación tecnológica, tales como las empresas que realizan estudios o análisis de comportamientos a través de las "cookies".

En el artículo de definiciones también se precisan términos ya existentes, entre los que se encuentran: "Responsable de tratamiento" y "Encargado de tratamiento".

El régimen de protección de datos personales implica la existencia de categorías jurídicas necesarias para la atribución de las responsabilidades por el cumplimiento de las obligaciones, deberes y garantías vinculadas a su normativa. En ese sentido, se precisa la definición del "Responsable del tratamiento", como aquella persona que determina las finalidades y medios del tratamiento, independientemente de la existencia de un banco de datos personales. Y la de "Encargado de tratamiento", como la persona natural, jurídica o entidad pública que actúa por orden del responsable de tratamiento.

Debe tenerse en cuenta, por ejemplo, que existen situaciones en las que determinadas organizaciones elaboran productos o servicios que al desarrollarlos o diseñarlos, si bien no existe un banco de datos personales, se presenta una responsabilidad al momento de realizar tratamiento de datos para los diseños y desarrollos mencionados, lo cual implica que dichas organizaciones asuman un rol como responsables del tratamiento.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

3.2. Excepciones al ámbito de aplicación

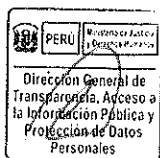
El anterior reglamento estableció dos supuestos de excepción material a la aplicación de las disposiciones contenidas en la Ley y su reglamento, sin embargo, la casuística presentada a la Autoridad Nacional de Protección de Datos Personales y la interpretación de las disposiciones contenidas en la Ley, permiten que el nuevo Reglamento precise excepciones adicionales:

- a) Tratamiento de datos personales de los representantes o apoderados de una persona jurídica:

Tanto el inciso 4, artículo 2 de la Ley N.º 29733, Ley de Protección de Datos Personales como el inciso 4 del artículo 2 del anterior reglamento, establecen que los datos personales es toda información que identifica o hace identificable a una persona natural, siendo que su alcance no incluye a las personas jurídicas; postura que ha sido desarrollada por la ANPD en opiniones consultivas como la OC N.º 35-2020-JUS/DGTAIPD, la consulta atendida mediante el Oficio N.º 873-2013-JUS/DGPDP de fecha 18 de noviembre de 2013 y el Oficio N.º 140-2014-JUS/DGPDP de fecha 21 de marzo de 2014, las mismas que se encuentran publicadas en el sitio web del Ministerio de Justicia y Derechos Humanos.

Conforme al criterio establecido en la absolución de las consultas mencionados, los datos personales de los representantes de una persona jurídica, al ser inscritos en el registro correspondiente, pasan a formar parte de la persona jurídica; por tanto, cuando una persona natural actúa como representante de una persona jurídica, aquellos datos personales, tales como los nombres, apellidos, número de documento de identidad, etc., cuyo tratamiento resulta necesario para el ejercicio de la representación, serán considerados como datos de la persona jurídica, y en consecuencia su tratamiento no se encontrará bajo los alcances de la LPDP y su Reglamento.

Conforme a lo expuesto, el nuevo Reglamento establece de forma expresa la excepción de los datos personales de una persona natural cuando actúa en representación de una persona jurídica, solo y tanto se realice con ese fin específico de representación de la persona jurídica.



E. LUNA C.

- b) Tratamiento de personas fallecidas:

Como precepto general, se entiende que toda persona natural es sujeto de derechos y que cuando fallece se convierte en un objeto de derecho.

El artículo 1 del Código Civil señala que: "La persona humana es sujeto de derecho desde su nacimiento. La vida humana comienza con la concepción. El concebido es sujeto de derecho para todo cuanto le favorece. La atribución de derechos patrimoniales está condicionada a que nazca vivo." Asimismo, el artículo 61 de la misma norma legal, señala que: "La muerte pone fin a la persona."

En esa línea el Tribunal Constitucional, se ha pronunciado en la Sentencia N.º 0256-2003-HC/TC señalando que: "(...) Sucede que la vida es la condición necesaria para que pueda titularizarse un derecho fundamental y, entre ellos, la libertad locomotora. Por tanto, no pudiendo los difuntos ser titulares de derechos fundamentales, no podrían resultar lesionados de los mismos."

Por tanto, entendiendo que el inciso 16 del artículo 2 de la Ley N.º 29733, Ley de Protección de Datos Personales define al "titular de datos personales" como la



G. VALDIVIESO P.



E. REBAZA I.

persona natural a quien le corresponde los datos personales debe concluirse que una vez que esta persona fallece no le corresponde el derecho a la protección de datos personales, por lo que el tratamiento de datos personales de fallecidos se encontraría fuera del ámbito de la normativa de protección de datos personales.

Así también, de la evaluación de la referencia internacional en materia de protección de datos personales, el Reglamento General de Protección de Datos (en adelante, RGPD), referente internacional en materia de protección de datos personales, establece de forma expresa que el Reglamento no es aplicable a la protección de las personas fallecidas.

Asimismo, la Ley de España también excluye del ámbito de aplicación, sin embargo, habilita que determinadas personas por razones familiares o de hecho puedan acceder a información de la persona muerta y pedir acceso, rectificación o supresión.

En la misma línea, el proyecto de Ley de Chile especifica: "En caso de fallecimiento del titular de datos, los derechos que reconoce esta ley pueden ser ejercidos por sus herederos."

Por tanto, el nuevo Reglamento a fin de cubrir el vacío de la norma, establece de forma expresa que el ámbito de aplicación de la normativa excluye al tratamiento de datos personales de fallecidos, sin embargo, habilita el ejercicio de determinados derechos por parte de familiares directos u otros con interés legítimo subjetivo¹⁴, salvo que, en vida, el titular, lo haya prohibido expresamente. Dicha habilitación tiene por finalidad que se pueda proteger la memoria o buena reputación del fallecido, ya que por datos erróneos o inexactos pueden generar perjuicio o daño a sus familiares.

- c) Se precisa que la finalidad sea vigente respecto a las competencias asignadas por ley a determinadas entidades públicas



El inciso 2 del artículo 4 del anterior reglamento, establecía que las entidades públicas que realicen tratamiento de datos personales en cumplimiento de las siguientes funciones: a) defensa nacional, b) seguridad pública, y c) desarrollo de actividades en materia penal para la investigación y represión del delito, se encontrarían fuera del ámbito de aplicación de la normativa de protección de datos personales.

Sin embargo, su inaplicación no puede darse de forma amplia, ya que las entidades públicas pueden mantener una finalidad actual o vigente para tratar los datos, pero cuando dicho período se cumple, y tienen la obligación de dejar evidencia histórica o acreditar sus actuaciones, valiéndose de documentos que pueden ser almacenados a través de medios físicos o informáticos, si se encuentran dentro del ámbito de aplicación de la norma.

Por ello, dichas entidades públicas deben perseguir garantizar la disponibilidad e integridad de su documentación en cualquier soporte, con la finalidad de asegurar su gestión, recuperación y conservación, y con el objeto de que, de ser necesaria, esta sea utilizada de acuerdo con las competencias, funciones y fines de la administración pública que los conserva.



14

El Tribunal Constitucional ha tenido una comprensión amplia del término "familia" al momento de determinar a los sujetos legitimados para acceder a los datos de una persona fallecida, condicionado ello a la existencia de un "interés legítimo subjetivo". Cfr. Tribunal Constitucional. Sentencia recaída en el Expediente N.º 02369-2013-PHD/TC, de fecha 8 de junio de 2015, fj. 14.

En este sentido, el nuevo Reglamento precisa que los datos personales contenidos o destinados a ser contenidos en bancos de datos de las entidades de la administración pública, debe tener una finalidad vigente para el cumplimiento de las funciones señaladas, y cuando dicha actividad cumpla su finalidad o cuando realicen cualquier otro tratamiento si se encuentran dentro del marco de aplicación de la LPDP y su reglamento, y en atención a ello, estos tratamientos deben realizarse en estricto respeto a los principios de finalidad, proporcionalidad, calidad, seguridad y disponibilidad de recurso, que fundamentan el pleno ejercicio del derecho de protección de datos personales.

3.3. Ámbito de aplicación territorial

El anterior reglamento, establecía dos supuestos de aplicación territorial (principio de territorialidad), siendo estos:

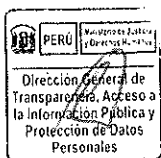
- Que el tratamiento de datos personales sea efectuado por un titular de banco de datos o quien resulte responsable establecido en territorio peruano.
- Que el tratamiento de datos sea efectuado por un encargado de tratamiento, a cuenta de un titular de banco de datos o quien resulte responsable establecido en territorio peruano.

Además, agregó criterios adicionales¹⁵ para la aplicación de la jurisdicción peruana en materia de protección de datos personales:

- Cuando el titular del banco de datos personales o quien resulte responsable no se encuentre en territorio peruano, pero le es aplicable la legislación por disposición contractual o del derecho internacional.
- Cuando el titular del banco de datos personales o quien resulte responsable no se encuentre en territorio peruano, pero utilice medios en dicho territorio, salvo sea con fines de tránsito.

En cuanto a lo que se refiere a medios, la Autoridad Nacional de Protección de Datos Personales (Opinión Consultiva N.º 56-2020-JUS/DGTAIPD) sostiene que se entenderá que se utiliza medios situados en territorio peruano, cuando por ejemplo, un motor de búsqueda realiza una operación técnica consistente en visitar las páginas web ubicadas en servidores peruanos, registra e indexa la información extraída utilizando dicho medio a fin de realizar tratamiento de los datos fuera del control de los titulares de los datos personales.¹⁶

Del análisis situacional, realizado en el punto IV de la presente Exposición de Motivos, del avance de la tecnología y su creciente uso por parte de los peruanos, se evidencia el tratamiento de datos personales más allá del territorio peruano genera riesgos respecto a la capacidad de las personas de ejercer su derecho a la protección de datos personales, y de forma específica, para protegerse contra uso o transferencia ilícita de sus datos. Por ello, resulta fundamental que se pueda establecer supuestos adicionales



E. LUNA C.



G. VALDIVIESO R.



E. REBAZA I.

¹⁵ A fin de establecer supuesto adicionales, se ha evaluado las más recientes normas emitidas a nivel internacional, así como la doctrina que ha sido emitida sobre la materia, tales como Reglamento General de Protección de Datos, N.º 2016/679, los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio N.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001 -ambos aprobados por Ley N.º 19.030 de 27 de diciembre de 2012-, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018.

¹⁶ Así también se ha pronunciado a través de las siguientes resoluciones Ver: Resoluciones Directorales 1853-2018-JUS/DGTAIPD-DPDP y 84-2019-JUS/DGTAIPD en <https://www.minjus.gob.pe/wp-content/uploads/2020/08/Exp.-7-2018-RD-1853-2018-DPDP.pdf> y <https://www.minjus.gob.pe/wp-content/uploads/2020/08/Exp.-07-2018-RD-84-2019-DGTAIPD.pdf>.

que permitan aclarar determinados criterios en los que será aplicable la jurisdicción peruana en materia de protección de datos personales:

- Si el responsable de tratamiento de datos no se encuentra en territorio peruano, pero realiza actividades relacionadas a la oferta de bienes o servicios dirigidos a los titulares de datos personales ubicados en territorio peruano.
- Si el responsable del tratamiento de datos no se encuentra en territorio peruano, pero realizan actividades realizadas al análisis de comportamiento de los titulares de datos personales ubicados en territorio peruano, así como el tratamiento que incluye la elaboración de perfiles que busquen predeterminedar conductas, preferencias, hábitos o similares.

Es importante mencionar, que, para la evaluación de las actividades relacionadas a la oferta de bienes o servicios dirigidos a los titulares de los datos personales ubicados en territorio peruano, se evaluarán elementos de convicción como el uso del idioma español, la referencia del pago en moneda nacional y la provisión de servicios conexos brindados en territorio peruano, como la publicidad o marketing.

Sobre el tratamiento realizado por el responsable del tratamiento o titular del banco de datos cuando se encuentran fuera del territorio peruano, es importante mencionar, el rol sustancial que tiene la figura del "Representante". El anterior reglamento, ya establecía la designación del representante, de manera específica señalada en el segundo párrafo del artículo 5 que:

"(...)

Para estos efectos, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que imponen la Ley y el presente reglamento y designará un representante o implementará los mecanismos suficientes para estar en posibilidades de cumplir de manera efectiva, en territorio peruano, con las obligaciones que impone la legislación peruana.

(...) (subrayado y negrita es nuestra)



E. LUNA C.

Hoy en día existen millones de datos personales son entregados diariamente para la provisión de productos y servicios y muchas de ellas son empresas extranjeras que tratan los datos personales de las personas que residen en territorio peruano; sin embargo, dichas empresas no cuentan con un representante en territorio peruano que permita cumplir de manera efectiva con las obligaciones que impone el régimen jurídico de protección de datos personales.



G. VALDIVIESO P.

Por tal motivo, es necesario aclarar la obligación de designar al representante, ya que el anterior reglamento no establecía quien era ese representante, y tampoco en que supuestos específicos debía designarse, así también fue establecido de manera facultativa, ya que se señaló que lo designará o implementará mecanismos suficientes para cumplir de manera efectiva en territorio peruano con la legislación en materia de protección de datos.

Así, el nuevo Reglamento propone dar mayor visibilidad a la obligación de designar al representante en territorio peruano, a fin de que exista un punto de contacto con la Autoridad Nacional de Protección de Datos Personales, y además atienda las solicitudes de los titulares de los datos personales. Y a su vez, brinda flexibilidad al determinar que el representante podrá ubicarse fuera del territorio peruano, siempre que el mismo pueda estar acreditado para atender procesalmente toda gestión de comunicación realizada por la Autoridad Nacional de Protección de Datos, así como solicitudes de los



E. REBAZA I.

titulares de los datos, denuncias o similares que se deriven de los procedimientos administrativos.

3.4. Principios para el tratamiento de datos personales

La Ley N.º 29733, Ley de Protección de Datos y su reglamento, establecen 8 principios rectores en materia de protección de datos personales, siendo los siguientes: legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición de recurso, nivel de protección adecuado.

Si bien dichos principios son estándares en países de Iberoamérica, los mismos ya han sido actualizados, incorporándose nuevos principios que permiten afrontar las tecnologías emergentes como inteligencia artificial o *big data*, entre otros que son utilizadas por las entidades públicas y personas jurídicas que recopilan y tratan grandes cantidades de datos personales.

A fin de incorporar los principios específicos de protección de datos personales en el nuevo Reglamento, se ha evaluado las más recientes normas emitidas a nivel internacional, así como la doctrina y el *soft law*, que han sido emitidos sobre la materia, tales como los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales de la Organización de Estados Americano en el año 2021, el Reglamento General de Protección de Datos, N.º 2016/679, los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio N.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001 -ambos aprobados por Ley N.º 19.030 de 27 de diciembre de 2012-, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, y las Directrices sobre Protección de la Privacidad y Flujos Transfronterizo de Datos Personales de la OCDE.

Estos principios, adicionalmente a los ya establecidos en la Ley N.º 29733, se agregan al marco teórico de interpretación de toda la regulación sobre el tratamiento de datos personales, estos son: principio de transparencia y principio de responsabilidad proactiva.



E. LUNA C.

- Principio de responsabilidad proactiva:

La implementación de nuevas disposiciones para un adecuado tratamiento de datos personales requiere, además, de un equilibrio de la ética y un nivel de responsabilidad directa por parte de aquellos que recopilan, procesan, usan y gestionan datos personales.



G. VALDIVIESO P.

La responsabilidad proactiva tiene por finalidad que el titular del banco de datos o quien resulte responsable actúe de forma diligente y anticipada frente al tratamiento de datos personales que realice.

En atención al principio se aplicarán las medidas técnicas y organizativas a fin de garantizar el respeto efectivo de la implementación de la normativa de datos personales y también la forma de demostrar su cumplimiento ante las Autoridades de Datos Personales.



E. REBAZA I.

Así, un enfoque contemporáneo de la responsabilidad proactiva es la incorporación de la privacidad en el diseño y arquitectura de los sistemas, así

como en cada etapa del diseño de los productos. El enfoque de privacidad proactiva debe ser parte integral del producto o servicio ya que se puede minimizar los riesgos asociados a las personas.

Es importante mencionar que, en las disposiciones emitidas respecto a gobierno digital a nivel nacional, que resulta aplicable a las entidades de la Administración Pública, sí se ha previsto como un principio en el marco de gobernanza digital a la privacidad desde el diseño como un enfoque al momento de diseñar servicios digitales a favor de la ciudadanía.¹⁷

Conforme a ello, Ann Cavoukian, Comisionado de información y Privacidad de Ontario, señaló que este enfoque se puede lograr a través de 7 principios fundacionales:

- Proactivo, no reactivo; preventivo no correctivo, que está caracterizado por anticipar los riesgos a los derechos y libertades antes que ocurra un daño a las personas;
- Privacidad como configuración predeterminada, quiere decir que no es necesario una acción, sino que esta intrínseca en el sistema
- Privacidad incrustada en el diseño, quiere decir que la privacidad es parte integral del sistema y no disminuye su funcionalidad;
- Funcionalidad total, permite demostrar que es posible mantener privacidad y seguridad al mismo tiempo; v) Seguridad de extremo a extremo, significa que garantiza una protección segura del ciclo de vida de la información, de inicio a fin
- Visibilidad y transparencia, significa que todos los involucrados permanecen transparentes y visibles a los usuarios;
- Respeto por la privacidad de los usuarios, significa que las personas son el enfoque del diseño



E. LUNA C.

Por tanto, la incorporación del principio de responsabilidad proactiva representa un aspecto novedoso y relevante para el tratamiento de datos personales, ya que permite elevar el estándar de protección de datos en el país, debido de que incentiva que los titulares de bancos de datos o responsables de tratamiento adopten de oficio y de forma anticipada determinadas medidas técnicas y organizativas que puedan evitar los efectos o riesgos que se generarían a los titulares de los datos personales.

Principio de transparencia:

En la normativa de protección de datos personales (LPDP y su Reglamento), la transparencia no se encuentra recogido de forma expresa, sin embargo su esencia se encuentra recogido en el contenido del derecho de información (artículo 18 de la Ley 29733) que lo reconoce como un derecho que tiene el titular del dato personal de que se le informe sobre los alcances del tratamiento de sus datos, sin embargo ello ha generado muchos cuestionamientos en los procedimientos administrativos a cargo de la Autoridad Nacional de Protección de Datos Personales, a través de los cuales señalan que el derecho de información requiere necesariamente una acción por parte del titular del dato personal a fin de que el responsable le informe sobre sus datos y no es un deber por parte del responsable del tratamiento o encargado.



G. VALDIVIESO P.



E. REBAZA I.

¹⁷ Artículo 5, inciso 5.3 del Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital.

Al respecto, la Autoridad Nacional de Protección de Datos se ha pronunciado en resoluciones que resuelven procedimiento sancionador, señalando que el derecho de información recogido en el artículo 18 de la LPDP, tiene una doble acepción que implica un derecho-deber de información, y que no necesariamente debe existir un medio a través del cual se materialice el derecho sino que este debe entenderse como la obligación del responsable del tratamiento de proveer toda la información al titular de los datos sobre el alcance del tratamiento de sus datos.

Así, este derecho implica que toda persona titular de sus datos personales debe poder conocer con qué finalidad se están recopilando sus datos, así como a quien se transferirán y la forma como puede ejercer sus derechos frente al tratamiento que se realiza, así como otras circunstancias y condiciones respecto al tratamiento de sus datos. Por ello, toda información sobre las condiciones del tratamiento de los datos personales debe ser fácilmente identificable y accesible, lo que exige emplear un lenguaje sencillo y claro que permita al ciudadano tomar una decisión basada en información idónea y veraz.

En esta línea, resulta necesario explicitar el principio de transparencia a efectos de fortalecer la obligatoriedad de que el tratamiento de datos personales deba ser informado de manera clara, fácil de entender y accesible al titular de los datos personales. Este principio busca que el titular del dato personal tome conocimiento de los riesgos que puede suponer el tratamiento de sus datos, así como los derechos que puede hacer valer respecto a los datos personales.

La determinación de la transparencia del tratamiento de los datos como principio rector representará una disposición de observancia obligatoria por parte de los responsables del tratamiento, y ya no será entendido como un derecho que tiene que ser ejercido a través de una solicitud (acción material).

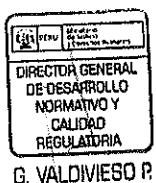
3.5. Obligaciones para el responsable de tratamiento y encargado

El nuevo Reglamento incorpora el Capítulo V referido a las obligaciones del titular del banco de datos o responsable del tratamiento, y del encargado de tratamiento, cuando corresponda.

A fin de incorporar las nuevas obligaciones de protección de datos personales en el nuevo Reglamento, se ha evaluado las más recientes normas emitidas a nivel internacional, así como la doctrina y el *soft law*, que han sido emitidos sobre la materia, tales como los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales de la Organización de Estados Americano en el año 2021, el Reglamento General de Protección de Datos, N.º 2016/679, los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio N.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001 -ambos aprobados por Ley N.º 19.030 de 27 de diciembre de 2012-, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, y las Directrices sobre Protección de la Privacidad y Flujos Transfronterizo de Datos Personales de la OCDE.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

- a) Obligación de designar a un Oficial de Datos Personales en las entidades públicas y privadas

El artículo 68, inciso 68.6 del Reglamento del Decreto Legislativo N.º 1412, Decreto que aprueba la Ley de Gobierno Digital, aprobado por Decreto Supremo N.º 029-2021-PCM, establece la obligación de que las entidades públicas designen a un Oficial de Datos Personales, quien es el enlace con la Autoridad Nacional de Protección de Datos Personales y sigue sus Directivas y Lineamientos.

La Ley N.º 29733, Ley de Protección de Datos Personales ni el anterior reglamento establecen la obligación de contar con la figura del Oficial de Datos Personales. Sin embargo, el artículo 28 de la Ley N.º 29733, Ley de Protección de Datos Personales, establece que el Titular y encargado de tratamiento tienen otras obligaciones establecidas en el Reglamento, por lo que se advierte una habilitación legal expresa, que permite el establecimiento de nuevas obligaciones.

Así, el nuevo Reglamento a efectos de garantizar de manera proactiva un tratamiento adecuado de datos personales, establece la obligación de designar el rol del Oficial de Datos Personales, el mismo que será también aplicable para determinadas organizaciones del sector privado. Los supuestos para su designación son los siguientes:

- El tratamiento lo lleve a cabo una autoridad u organismo público, de conformidad con lo establecido en el inciso 69.6 del artículo 68 del Reglamento del Decreto Legislativo N.º 1412, Ley de Gobierno Digital, aprobado por Decreto Supremo N.º 029-2021-PCM.
- El titular del banco de datos o del responsable del tratamiento o el encargado de tratamiento realicen actividades que consistan en operaciones de tratamiento que, debido a su naturaleza, alcance y/o fines, requieran una observación habitual, sistemática y continua de titulares de datos personales de forma masiva o gran escala; o
- El titular del banco de datos o responsable de tratamiento o del encargado realicen como actividades principales aquellas que consistan en el tratamiento de datos sensibles.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

Además, el nuevo Reglamento establece las funciones principales que debe cumplir el (ODP), entre las que se encuentran:

- Informar y asesorar al titular del banco de datos personales o al responsable del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud de la Ley, el presente Reglamento y de otras disposiciones de protección de datos;
- Supervisar el cumplimiento de lo dispuesto en la Ley, el presente Reglamento y de otras disposiciones de protección de datos y en las políticas del titular del banco de datos o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la sensibilización y formación del personal que participa en las operaciones de tratamiento, y las auditorías que se realicen;
- Ofrecer el asesoramiento que se le solicite acerca del cumplimiento de las disposiciones sobre protección de datos personales.
- Cooperar con la Autoridad Nacional de Protección de Datos Personales para el desempeño de sus fines y atribuciones.
- Actuar como punto de contacto de la Autoridad Nacional de Protección de Datos Personales para cuestiones relativas al tratamiento de datos personales.

b) Reportar los incidentes de seguridad que afecten datos personales

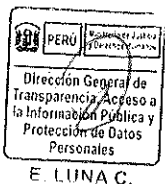
Conforme al Reglamento del Decreto Legislativo N.º 1412, Decreto que aprueba la Ley de Gobierno Digital, aprobado por Decreto Supremo N.º 029-2021-PCM, el artículo 108 establece la obligación de que las entidades públicas comunican y colaboran con la Autoridad Nacional de Protección de Datos Personales ante la identificación de incidentes de seguridad digital cuando involucren datos personales, dentro del plazo de 48 horas a partir de la toma de conocimiento de la brecha de seguridad.

Asimismo, el artículo 9 del Decreto de Urgencia señala específicamente que los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos deben reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.

Conforme se advierte de la norma descrita en el párrafo precedente, la obligación de comunicar los incidentes de seguridad respecto al sector privado se centra en determinados sectores, excluyendo a otros responsables de tratamiento que realizan tratamiento de grandes volúmenes de datos como los motores de búsqueda o aquellos que realizan análisis comportamental o de publicidad personalizada o aquellos que son considerados encargados de tratamiento de datos personales y que deben comunicarlo al responsable del tratamiento.

Los datos personales representan uno de los activos estratégicos más importantes de una organización, lo cual conlleva que se generen situaciones de riesgo, siendo uno de ellos, el incidente de seguridad que pueda generar daños materiales o inmateriales a las personas naturales, como la pérdida de control de sus datos personales o la restricción de otros derechos como la discriminación, suplantación de identidad, pérdidas financieras, estafa, daño a la imagen o reputación, o cualquier otro daño económico o social.

Por ello, resulta fundamental se establezca que cuando un responsable de tratamiento tome conocimiento que se ha producido un incidente de seguridad de datos personales lo reporte ante la Autoridad Nacional de Protección de Datos Personales. Así también la obligación de que el encargado de tratamiento lo comunique al responsable de tratamiento.



c) Evaluación de impacto del tratamiento de datos personales

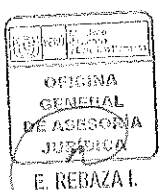
Es un mecanismo de responsabilidad proactiva que faculta a los responsables del tratamiento de datos realizar, de forma previa al tratamiento de datos, un análisis o evaluación del impacto o riesgos que implicará el tratamiento de esos datos.

Dicha evaluación permite de manera anticipada evaluar los potenciales riesgos a los que se encuentran expuestos los datos personales, a fin de establecer las salvaguardas para reducirlos hasta un nivel de riesgo que sea aceptable.

La Autoridad Nacional de Protección de Datos Personales elabora lineamientos o guías orientativas sobre el contenido del documento denominado Evaluación de Impacto en el tratamiento de datos personales.

La Evaluación de impacto del tratamiento de datos personales se podrá realizar especialmente en los siguientes supuestos:

- Cuando se traten datos sensibles;



- Cuando se traten datos con fines de crear perfiles personales;
 - Cuando se traten datos de personas en especial situación de vulnerabilidad, como menores o personas con discapacidad;
 - Cuando se traten grandes volúmenes de datos;
 - Cuando se realicen transferencias de datos a países que no cuentan con un nivel adecuado de protección de datos ni se otorgan las garantías adecuadas; u,
- otros que determine la Autoridad Nacional de Protección de Datos Personales mediante resolución.

3.6. Derechos de los Titulares de los Datos Personales: el derecho de acceso y la portabilidad de los datos personales

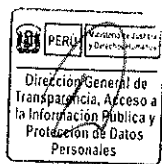
La normativa de protección de datos personales establece derechos para dar protección a los titulares frente al tratamiento de sus datos: derecho de información, derecho de acceso, derecho de rectificación, derecho de cancelación o supresión, derecho de tratamiento objetivo. Sin embargo, los nuevos retos debido al avance de la tecnología, la globalización de los mercados digitales, los nuevos servicios digitales que promueven el intercambio a gran velocidad de los datos, requieren ser evaluados y adaptados a efectos de fortalecer el régimen jurídico de protección de datos sin afectar los derechos y libertades de otros.

La evaluación precitada debe enfocarse en el derecho de acceso establecido en el artículo 19 de la Ley N.º 29733 que establece: *"El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos."*

Así, de forma complementaria a lo establecido en la Ley N.º 29733, en el Reglamento de la Ley¹⁸, se establece que: *"El titular tiene derecho a obtener del titular del banco de datos personales o responsables del tratamiento la información relativa a sus datos, así como las condiciones y generalidades del tratamiento de los mismos"*. Asimismo, se agrega que la forma en que la información puede ser entregada a los titulares de los datos es a través de los siguientes medios¹⁹:

- Visualización en sitio
- Escrito, copia, fotocopia o facsímil
- Transmisión electrónica la respuesta siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información.
- Cualquier otra forma o medio que sea adecuado a la configuración o implantación material del banco de datos personales o a la naturaleza del tratamiento, establecido por el titular del banco de datos personales o responsable del tratamiento.

Asimismo, el tercer párrafo del mencionado artículo 70 del Reglamento señala que, independientemente de la forma en la que se entregue la información, esta debe ser en un formato claro, legible e inteligible, sin utilizar claves o códigos que requieran de dispositivos mecánicos para su adecuada comprensión.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

¹⁸ Artículo 61 del Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales, aprobado por Decreto Supremo N.º 003-2013-JUS

¹⁹ Artículo 62 del Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales, aprobado por Decreto Supremo N.º 003-2013-JUS

Conforme a los artículos expuestos, el derecho de acceso se ve limitado ante el avance de la tecnología, ya que si bien la información puede ser obtenida a través de distintas formas como la transmisión electrónica o cualquier otra que sea adecuada a la implantación material del banco de datos personales, no se garantiza que esta pueda ser transmitida a través de medios reutilizables a fin de que otras instituciones públicas o privadas puedan hacer uso de ellas para otras finalidades a solicitud del propio titular de los datos personales²⁰.

Al respecto, se debe tener en cuenta lo mencionado por el Tribunal Constitucional en la STC N.º 693-2012-PHD/TC, a efectos de determinar si el derecho de acceso permite la reutilización de la información obtenida por parte de titular de los datos personales, así se señala:

*"(...) el derecho a la autodeterminación informativa también supone **que una persona pueda hacer uso de la información privada que existe sobre ella, ya sea que la información se encuentre almacenada o en disposición de entidades públicas, o sea de carácter privado.** En ese sentido, parece razonable afirmar que una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si ésta se encuentra disponible en una entidad pública o privada."* (subrayado y resaltado es nuestro)

De acuerdo con lo mencionado por el Tribunal Constitucional, el derecho de acceso no solo implica la acción material de presentar una solicitud requiriendo la información sobre el tratamiento de sus datos personales, sino que garantiza además el derecho de que dicha persona pueda hacer uso de esa información que solicita al responsable del tratamiento, sea público o privado.

El ejercicio del derecho de acceso en los términos redactados actualmente en la Ley y su Reglamento no permite que se cumpla el contenido esencial de dicho derecho que implica que sea usado por el titular de los datos personales, ya que la entrega de la información en formato electrónico no significa que se entregue en formatos estructurados, abiertos, fácilmente procesables y reutilizables por otros responsables de tratamiento.

En atención a ello, el presente Reglamento busca cubrir la deficiencia regulatoria respecto de las limitaciones del ejercicio del derecho de acceso debido al actual avance de la tecnología, incluyendo de manera expresa la portabilidad como una manifestación del contenido en el derecho de acceso²¹.

Así también, la Red Iberoamericana de Protección de Datos se ha pronunciado²² sobre que la "regulación del tratamiento de datos personales debe aplicarse al margen de los procedimientos, metodologías o mecanismos que se utilicen para recolectar, usar o tratar los datos personales", señalando que la aplicación del principio de neutralidad tecnológica en el tratamiento de datos, implica "que la



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

²⁰ Bolaños Vainstein, G. G. (2022). *La incorporación del derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano* [Tesis para optar el título profesional de Abogado, Universidad de Lima]. p. 72 Repositorio Institucional de la Universidad de Lima. <https://hdl.handle.net/20.500.12724/15999>

²¹ Sobre el derecho continente, el Tribunal Constitucional se ha pronunciado en diversa jurisprudencia, señalando que es un derecho que comprende diversas garantías y reglas, las cuales son a su vez derechos parte de un gran derecho con una estructura compleja o compuesta. STC N.º 00579-2013-PA/TC. <https://www.tc.gob.pe/jurisprudencia/2014/00579-2013-AA.html>

²² Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube. <https://www.redipd.org/sites/default/files/2021-06/recomendaciones-tratamiento-datos-personales-servicios-nube.pdf>

regulación sobre el tratamiento de datos personales es neutral tecnológica y temáticamente”, es decir, que “aplica a cualquier tratamiento de datos, con independencia de las técnicas, procesos o tecnologías actuales o futuras que se utilicen para dicho efecto”.

En línea con lo expuesto, el contenido del derecho de acceso permite una función habilitadora de la portabilidad, a efectos de brindar un impacto práctico a dicho derecho que se encuentre acorde con el avance de las nuevas tecnologías y la economía digital, a fin de que los datos puedan ser transmitidos y usados fácilmente por otros responsables de tratamiento.

La expresa inclusión de la portabilidad, como manifestación de derecho de acceso, genera un impacto positivo como país, ya que contribuye al nivel adecuado de protección de datos, además de haber sido recogido en otros instrumentos internacionales referentes en la materia como: los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales de la Organización de Estados Americano en el año 2021, el Reglamento General de Protección de Datos, N.º 2016/679, y los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017.

De esta forma, el nuevo Reglamento incluye en el régimen jurídico de protección de datos personales, la portabilidad de los datos como manifestación del derecho de acceso, que refuerza el control de los datos que le conciernen a una persona natural, otorgándoles mayor poder, en el sentido de que pueden copiar, mover o transferir sus datos de un entorno de tecnología de la información a otro.

La portabilidad de los datos personales

La portabilidad de datos personales subyace al derecho de acceso siendo una “expresión” o “actualización” del fenómeno de digitalización frente a las limitaciones del derecho de acceso en entornos digitales²³. En ese sentido, como manifestación del derecho de acceso, la portabilidad permite que, cuando el tratamiento se realice por medios automatizados y sea técnicamente posible, el titular de los datos pueda solicitar al responsable de tratamiento o titular de banco de datos que transmita sus datos a otro responsable o titular de banco de datos²⁴.

La portabilidad implica la facilidad de transferencia sin necesidad de volver a ingresar la data y su posterior posibilidad de reutilización; la necesidad de formatos o estándares comunes o, al menos, compatibles; su indiscutible asociación al tratamiento automatizado de datos personales; su vinculación a la interoperabilidad; la necesidad de generar consensos y colaboración entre agentes del mercado para poder materializar la portabilidad de datos; e, implicancias económicas que deben ser estudiadas²⁵.



²³ Ibid. p. 214 Repositorio institucional de la Universidad de Lima. <https://hdl.handle.net/20.500.12724/15999>

²⁴ Sobre el particular, el Reglamento General de Protección de Datos, Reglamento (UE) 2016/679 del Parlamento y del Consejo de la Unión Europea, incorpora el derecho a la portabilidad de los datos. Asimismo, el Grupo de Trabajo del Artículo 29, actualmente el Comité Europeo de Protección de datos, publicó unas Directrices sobre el derecho a la portabilidad de los datos, WP 242 rev.01, revisadas y adoptadas el 5 de abril de 2017, en las que se mencionaba que este derecho ofrece a los interesados una forma sencilla de gestionar y reutilizar por sí mismos sus datos personales. Disponible en: <https://bit.ly/3t13fz4>

²⁵ Bolaños Vainstein, G. G. (2022). *La incorporación del derecho a la portabilidad de datos personales en el ordenamiento jurídico peruano* [Tesis para optar el título profesional de Abogado, Universidad de Lima]. p. 86 Repositorio institucional de la Universidad de Lima. <https://hdl.handle.net/20.500.12724/15999>

Asimismo, la portabilidad no es una figura jurídica ajena al régimen peruano, pues en el sector de las telecomunicaciones se reconoce la portabilidad numérica, lo cual se traduce en el derecho de los usuarios de los servicios de telecomunicaciones de conservar su número de teléfono, aun cuando cambie de empresa operadora de servicio móvil o fijo²⁶.

La portabilidad de los datos se encuentra relacionada al derecho de acceso a la protección de los datos personales (artículo 19 de la Ley N.º 29733, Ley de Protección de Datos Personales) ya que permite recibir los datos que sobre sí mismo le haya dado al responsable de tratamiento o titular de banco de datos y poder transmitirlo a otro responsable o titular.

En sentido similar a lo antes mencionado, se pronunció el Grupo de Trabajo del Artículo 29, al señalar expresamente que el: *"derecho a la portabilidad de los datos, estrechamente relacionado con el derecho de acceso, aunque diferente de este en muchos aspectos."*

Sobre el particular, la inclusión expresa de la portabilidad como una manifestación actualizada del derecho de acceso en respuesta a las necesidades tecnológicas presentes, permite que los titulares de los datos puedan reutilizar su información para sus propios fines en diferentes servicios, lo que promueve la libre circulación de información y facilita la transmisión entre distintos proveedores de servicios. Así, este derecho contiene sus propias particularidades, estableciéndose que puede ser ejercido cuando se produzcan alguna de las siguientes condiciones:

- El tratamiento esté basado en el consentimiento o en una relación contractual en la que el titular del dato es parte.
- El tratamiento se ejerza mediante medios automatizados.

Finalmente, el nuevo reglamento prevé de forma expresa que la portabilidad no se aplica al tratamiento necesario para el cumplimiento de las competencias o funciones conferidas a las entidades públicas.



E. LUNA C.

3.7. Registro Nacional de Protección de Datos Personales

Respecto a los procedimientos de inscripción, modificación y eliminación de bancos de datos personales de administración pública o privada en el Registro Nacional de Protección de Datos Personales, con el objetivo de lograr mayores niveles de cumplimiento de la LPDP y su Reglamento, resulta necesario simplificar y reducir las cargas de los administrados en los procedimientos mencionados. Con ese objetivo, el Proyecto de Reglamento de la Ley 29733 propone eliminar la exigencia de un pago por derecho de tramitación, de modo tal que este tipo de trámites sean gratuitos.

Esto último se ha propuesto en la convicción que todos los procedimientos administrativos deben sustentarse en el principio de simplicidad ya señalado, el cual tiene como finalidad cautelar el derecho de los administrados de acceder a lo solicitado reduciendo los costos en los que debe incurrir (en términos de tiempo, dinero y esfuerzo), para fomentar el desarrollo económico.



G. VALDIVIESO R.



E. REBAZA I.

²⁶ Conforme a la Ley N° 28999, Ley de portabilidad numérica en los servicios móviles; y la Ley N° 29956, Ley que establece el derecho de portabilidad numérica en los servicios de telefonía fija, establece el derecho del usuario de telefonía fija de conservar su número telefónico aun cuando cambie de empresa operador.

Es preciso señalar que, en el caso de los procedimientos de modificación y cancelación de bancos de datos, buscando la celeridad y simplicidad del procedimiento, en la solicitud vía formulario, únicamente, se debe consignar los datos a modificar, y en el caso de cancelación deberá indicarse el destino de los datos del banco a cancelarse, no siendo necesario consignar nuevamente la totalidad de los datos que fueron materia de inscripción.

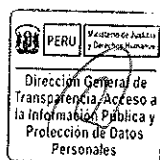
Debe advertirse que según el economista senior de la División de Política Regulatoria de la OCDE, Manuel Gerardo Flores Romero²⁷ los efectos de una regulación restrictiva son la afectación del crecimiento económico y bienestar social, entorpeciendo el emprendimiento e innovación, lo que afecta la competencia y la productividad.

3.8. Tratamientos especiales de datos personales

Protección del tratamiento de datos de menores

En principio, el tratamiento de los datos personales de un menor de edad se considera lícito cuando se obtenga el consentimiento de al menos uno de los titulares de la patria potestad o tutores, según corresponda. Asimismo, en el caso de datos personales de mayores de catorce y menores de dieciocho años, para realizar tratamiento de datos personales, dicho menor puede otorgar consentimiento válidamente, siempre que la información proporcionada haya sido expresada en un lenguaje comprensible por ellos, salvo en los casos que la ley establezca una disposición distinta al respecto.

En ningún caso, el consentimiento para el tratamiento de datos personales de menores de edad puede otorgarse para que accedan a actividades, vinculadas con bienes o servicios que están restringidos para mayores de edad.



E. LUNA C.

Ahora bien, en razón de la aceleración tecnológica y las actividades de menores a través de medios digitales, se está generando una alta exposición de imágenes o información de menores en las redes sociales o páginas web, por lo que resulta necesario visibilizar la importancia de la protección de los datos de menores en este ámbito.

De este modo, se enfatiza que es obligación de los titulares de bancos de datos personales, o de quien resulte responsable del tratamiento de datos de menores garantizar la protección del interés superior del niño y de sus derechos, en especial en la publicación o difusión de sus datos personales a través de servicios digitales.



G. VALDIVIESO P.

Asimismo, en sintonía con lo previamente señalado, se prevé que cuando la publicación o difusión de los datos personales de mayores de catorce y menores de dieciocho años se realice a través de las redes sociales o servicios equivalentes, corresponde contar con el consentimiento de dicho menor o, alternativamente, con el consentimiento de uno de los titulares de la patria potestad o tutores.



E. REDAZA I.

27

Flores Romero, Manuel Gerardo (junio 2016), *Calidad Regulatoria y Modernización de la Gestión Pública*. III Seminario Internacional de Modernización de la Gestión Pública "Camino Hacia la Buena Gobernanza", Lima, Perú, disponible en: <https://smartreg.pe/reportes/OCDE%20Calidad%20regulatoria%20y%20modernizacion%20publica%20en%20el%20Peru%202016.pdf>

3.9. Flujo transfronterizo de datos personales

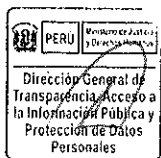
El nuevo funcionamiento de los servicios digitales dentro del mercado interior ha generado el aumento de flujos transfronterizos de datos personales, convirtiéndose los datos personales en el recurso fundamental de la sociedad de la información. Por un lado, el intercambio de los datos fuera del territorio peruano resulta positivo porque permite nuevos y mejores servicios, así como hallazgos e investigación científica; y, por otro lado, existen mayores riesgos ya que es más difícil el control del destino y el uso que se dará a los datos personales.

Por ello, el nuevo Reglamento incorpora un marco más claro y garantista que asegura que los datos personales tendrán una protección equiparable a la establecida en la normativa peruana, sin generar trabas a la economía y libre mercado.

Así, se explicita mayor participación a la Autoridad Nacional de Protección de Datos Personales, a fin de que se determine qué países ofrecen un nivel de protección adecuado en materia de protección de datos, siguiendo determinados criterios como:

- Revisión del marco jurídico legal general.
- La existencia de principios para el tratamiento de los datos personales.
- La existencia de normas que reconozcan y garanticen los derechos de los titulares de datos y que puedan disponer de vías para ejercer sus derechos.
- Se debe contar con una autoridad encargada de la supervisión y la determinación de responsabilidades en caso de infracciones.

Además, la Autoridad Nacional de Protección de Datos emitirá modelos de cláusulas contractuales a fin de que los receptores asuman las obligaciones que corresponden al titular del banco de datos o responsable del tratamiento, y se establezca los derechos y libertades de los titulares de los datos personales y las obligaciones de los responsables.



E. LUNA C.

Por último, el titular del banco de datos o responsable del tratamiento cuenta con la facultad de solicitar opinión a la Autoridad Nacional de Protección de Datos Personales a fin de que se determine que la transferencia se realiza acorde al régimen de protección de datos personales.

3.10. Régimen sancionador y tipificación de infracciones

Potestad de la Autoridad Nacional de Protección de Datos Personales para incorporar las infracciones en el Proyecto de Reglamento

Por el principio de tipicidad regulado en el numeral 4 del artículo 248 del TUO de la Ley 27444, las disposiciones reglamentarias de desarrollo solamente pueden "especificar o graduar" aquellas normas dirigidas a identificar las conductas (infracciones) o determinar sanciones, sin constituir nuevas conductas sancionables a las previstas legalmente, salvo los casos en que la "ley o Decreto Legislativo" permita tipificar infracciones por norma reglamentaria.

El artículo 38 de la Ley N.º 29733, Ley de Protección de Datos Personales, modificada por la Cuarta Disposición Complementaria Modificatoria del Decreto



G. VALDIVIESO R.



E. REBAZA I.

Legislativo²⁸ N.º 1353, establece que las infracciones se clasifican en leves, graves y muy graves, y permite que las infracciones sean tipificadas vía reglamentaria.

Así también, el artículo 39 de la LPDP²⁹, prevé lo referente a las sanciones a aplicar en relación con la gravedad de las conductas infractoras, de acuerdo con el siguiente texto:

“Artículo 39. Sanciones administrativas

En caso de violación de las normas de esta Ley o de su reglamento, la Autoridad Nacional de Protección de Datos Personales puede aplicar las siguientes multas:

1. Las infracciones leves son sancionadas con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco unidades impositivas tributarias (UIT).

2. Las infracciones graves son sancionadas con multa desde más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT).

3. Las infracciones muy graves son sancionadas con multa desde más de cincuenta unidades impositivas tributarias (UIT) hasta cien unidades impositivas tributarias (UIT).

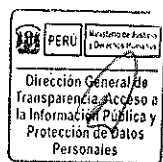
(...)

La Autoridad Nacional de Protección de Datos Personales determina la infracción cometida y el monto de la multa imponible mediante resolución debidamente motivada. Para la graduación del monto de las multas, se toman en cuenta los criterios establecidos en el artículo 230, numeral 3), de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces. (...)

En ese contexto, la LPDP ha facultado de manera expresa para que a través del Reglamento se pueda especificar o graduar aquellas disposiciones dirigidas a identificar las conductas o determinar las sanciones, pues el artículo 38 de la LPDP determina que, vía reglamentaria, las infracciones puedan ser tipificadas considerando que las obligaciones que deben cumplir los administrados se encuentren previstas en la LPDP.

Esta figura constituye la reserva de ley relativa que también ha sido reconocida en el ámbito de la jurisprudencia del Tribunal Constitucional en la sentencia del 10 de noviembre de 2015 (caso Ley Universitaria) y la decisión de su Pleno en la Sentencia 201/2022 del 15 de junio de 2022 (análisis de constitucionalidad del inciso 4 del artículo 248 del TUO de la Ley 27444).

Precisamente, la habilitación legal para que el Proyecto de Reglamento pueda tipificar las infracciones es acorde a los criterios del Tribunal Constitucional a través de su sentencia del 10 de noviembre de 2015 (Pleno Jurisdiccional) recaída en los Expedientes N.º 0014-2014-P1/TC, 0016-2014-P1/TC, 0019-2014-P1/TC y



E. LUNA C.



G. VALDIVIESO P.

28

Decreto Legislativo 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.

29

Ley Nro. 29733, Ley de Protección de Datos Personales

(...)

“Artículo 38.- Tipificación de infracciones

Las infracciones se clasifican en leves, graves y muy graves, las cuales son tipificadas vía reglamentaria, de acuerdo a lo establecido en el numeral 4) del artículo 230 de la Ley N° 27444, Ley del Procedimiento Administrativo General, mediante Decreto Supremo con el voto aprobatorio del Consejo de Ministros.

(...)



E. REBAZA I.

0007- 2015-PI/TC (caso Ley Universitaria³⁰) que indica los siguientes aspectos referidos al principio de legalidad y reserva de ley relativa:

"(...) 180. En esta materia aplica entonces aquella reserva de ley relativa. Por ende, no resulta inconstitucional que se derive al reglamento la tipificación de las infracciones, en tanto se ha fijado en la ley las conductas sancionables y la escala y los tipos de sanción. 181. Por último, cabe añadir que, si se regula una actividad con miras a garantizar la calidad del servicio público, resulta necesario dotar al organismo supervisor de las herramientas necesarias para corregir las infracciones que se adviertan en su ámbito."

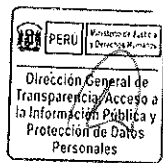
Dicho criterio fue confirmado Tribunal Constitucional a través de su sentencia del 25 de abril de 2018 (Pleno Jurisdiccional) recaída en el Expediente N.º 0020-2015-PI/TC (Caso Potestad Sancionadora de la Contraloría General de la República³¹) que indica lo siguiente respecto a la potestad reglamentaria del Poder Ejecutivo:

46. Por tanto, al desarrollar normas con rango de ley, los reglamentos no pueden desnaturalizarlas creando infracciones sin una debida base legal. Admitir lo contrario implicaría aceptar una desviación de la potestad reglamentaria y vaciar de contenido los principios de legalidad y tipicidad que guardan una estrecha relación con el derecho fundamental al debido proceso.

Y, a través de los fundamentos 20 al 25 de la Sentencia 201/2022 del 15 de junio de 2022 (análisis de constitucionalidad del inciso 4 del artículo 248 del TUP de la Ley 27444³²), recaída en el Expediente N.º 0002-2021-PI/TC, el Tribunal Constitucional aclara que la habilitación legal para tipificar infracciones a través de un dispositivo reglamentario no vulnera el principio de tipicidad en el ámbito del procedimiento administrativo sancionador, en tanto resulta admisible que, en ocasiones, los reglamentos especifiquen o gradúen infracciones previstas de manera expresa en la ley; siempre que las conductas prohibidas cuenten con una adecuada base legal, o que no se desarrollen disposiciones legales generales o imprecisas que terminen creando infracciones nuevas subrepticamente.

En ese contexto, cumpliendo con lo señalado por el Tribunal Constitucional, la tipificación de las conductas prohibidas o infracciones relacionadas al incumplimiento del derecho deber de información, el principio deber de seguridad y, otras disposiciones establecidas en la LPDP, así como el TUP de la Ley 27444, incluidas en el presente Proyecto de Reglamento cuentan con una adecuada base legal que respalda su tipificación; y, asimismo, la gravedad de cada conducta infractora también se encuentra delimitada por la escala y tipo de sanción conforme al artículo 39 de la LPDP.

La Autoridad Nacional de Protección de Datos Personales se encuentra comprometida con el cumplimiento de los principios de legalidad y tipicidad que resguardar el legítimo ejercicio de la potestad sancionadora y, en ese sentido, se ha procurado que la tipificación de las infracciones incorporadas al Proyecto de



E. LUNA C.



G. VALDIVIESO R.



E. REDAZA L.

30 Sentencia del Tribunal Constitucional del 10 de noviembre de 2015 (Caso Ley Universitaria) disponible en el siguiente enlace: <https://www.tc.gob.pe/jurisprudencia/2015/00014-2014-AI%2000016-2014-AI%2000019-2014-AI%2000007-2015-AI.pdf>

31 Sentencia del Tribunal Constitucional del 25 de abril de 2018 (Caso Potestad Sancionadora de la Contraloría General de la República) disponible en el siguiente enlace: <https://tc.gob.pe/jurisprudencia/2019/00020-2015-AI.pdf>

32 Pleno Sentencia del Tribunal Constitucional del 15 de junio de 2022 (Caso del cuestionamiento de los procesos de decisión en el ámbito de la administración pública - análisis de constitucionalidad del inciso 4 del artículo 248 del TUP de la Ley 27444) disponible en el siguiente enlace: <https://www.tc.gob.pe/jurisprudencia/2022/00002-2021-AI.pdf>

Reglamento cumpla con los principios del ámbito del procedimiento administrativo sancionador, a fin de resguardar los derechos de los administrados, respetando las características esenciales de las conductas antijurídicas que pueden desprenderse del incumplimiento de las obligaciones establecidas en la LPDP y evitando que la tipificación incluya conceptos indeterminados o imprecisos que no se encuentren delimitados en la LPDP.

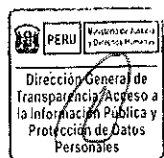
En esa línea, a través del Proyecto de Reglamento se elimina la infracción regulada actualmente en el literal f, numeral 2 del artículo 132 del actual Reglamento que establece como infracción leve: *f) Dar tratamiento a los datos personales contraviniendo las disposiciones de la Ley y su Reglamento*; debido a que contiene un enunciado genérico e indeterminado que no permite delimitar de forma adecuada la conducta prohibitiva; por lo cual, podría ocasionar una transgresión al principio de tipicidad.

En ese mismo sentido, el numeral 1 del artículo 141 del Proyecto de Reglamento modifica una infracción administrativa grave que actualmente se encuentra establecida en el actual Reglamento de la LPDP, tipificándola de la siguiente forma: *No atender, impedir u obstaculizar el ejercicio material de los derechos titular de datos personales*.

Así entonces, a través del Proyecto de Reglamento se corrige la redacción de la infracción tipificada con la finalidad de aclarar el sentido del dispositivo legal respecto a las conductas "no atención", "impedimento" "obstaculización" descritas, para que estas deben ser entendidas e interpretadas en el contexto de la existencia de una solicitud del titular del dato personal; es decir, dentro del ejercicio de sus derechos reconocidos en el Título III de la Ley 29733 (artículos 19, 20, 22 y 24 de la LPDP). Por lo tanto, en línea con el criterio del Tribunal Constitucional, se ha corregido los alcances de la descripción típica referida "el ejercicio de los derechos", la cual en el texto anterior no delimitaba de forma adecuada la conducta prohibitiva y generaba diversas interpretaciones.

Tipificación de infracciones por el cumplimiento de las condiciones establecidas en el artículo 18 de la Ley N.º 29733, Ley de Protección de Datos Personales

El artículo 18 de la Ley N.º 29733, Ley de Protección de Datos Personales³³ contempla el derecho-deber de información por el cual el titular del banco de datos



E. LUNA C.

33

Ley Nro. 29733, Ley de Protección de Datos Personales (...)

"Artículo 18.- Derecho de información del titular de datos personales

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.

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 el caso que el titular del banco de datos establezca vinculación con un encargado de tratamiento de manera posterior al consentimiento, el accionar del encargado queda bajo responsabilidad del Titular del Banco de Datos, debiendo establecer un mecanismo de información personalizado para el titular de los datos personales sobre dicho nuevo encargado de tratamiento.



G. VALDIVIESO R.



E. REBAZA I.

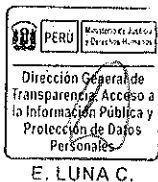
personales o responsable del tratamiento debe informar al titular de dichos datos (de forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación) sobre las condiciones de tratamiento de sus datos, las cuales son las siguientes:

- la finalidad para la que sus datos personales serán tratados;
- quienes son o pueden ser los destinatarios de dichos datos personales;
- 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;
- la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

El artículo 18 de la LPDP desarrolla las características del derecho-deber de información y las condiciones que deben ser informadas al titular de datos personales; de este modo, dicha disposición legal determina el contenido prescriptivo esencial cuyo incumplimiento debe ser contemplado para el planteamiento de las conductas infractoras previstas en el inciso 5 del artículo 140 y el inciso 2 del artículo 141 del Proyecto del Reglamento.

Así, con el objetivo de asegurar el cumplimiento del derecho-deber de informar de acuerdo a lo contemplado en el artículo 18 de la LPDP, en el Proyecto de Reglamento se incorporan las siguientes 2 infracciones administrativas específicas:

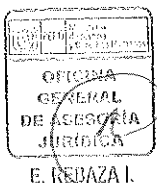
- **Infracción Leve** - Inciso 5 del artículo 140 del Proyecto del Reglamento: *"Informar de forma incompleta de dos o menos de dos condiciones del tratamiento de los datos personales señaladas en el artículo 18 de la Ley."*
- **Infracción Grave** - Inciso 2 del artículo 141 del Proyecto del Reglamento: *"No cumplir con el deber de informar o informar de forma incompleta de tres a más condiciones del tratamiento de los datos personales a los titulares de datos personales, de acuerdo con lo establecido en el artículo 18 de la Ley."*



Resulta relevante que el incumplimiento del derecho-deber de informar las condiciones del tratamiento de los datos personales (cuya obligatoriedad se encuentra contemplada en el artículo 18 de la LPDP) sea contemplado como infracciones administrativas, pues ello genera incentivos para los sujetos obligados coadyuvando a garantizar el derecho que tienen los titulares de datos personales de acceder a información clara sobre la forma en que otros utilizan o administra sus datos personales (finalidad, destinatarios, transferencia, la posibilidad de ejercer los derechos que la ley le concede, entre otros).

Lo anterior, además, guarda concordancia con el principio de transparencia incorporado en el artículo VI del nuevo Reglamento, el cual establece el deber de garantizar que el titular de datos personales tome conocimiento de manera previa de los alcances, riesgos y derechos que puede hacer valer ante el tratamiento de sus datos.

Si con posterioridad al consentimiento se produce la transferencia de datos personales por fusión, adquisición de cartera, o supuestos similares, el nuevo titular del banco de datos debe establecer un mecanismo de información eficaz para el titular de los datos personales sobre dicho nuevo encargado de tratamiento".



En ese sentido, a través del inciso 5 del artículo 140 y el inciso 2 del artículo 141 del Proyecto de Reglamento se especifica y gradúa el incumplimiento de las obligaciones relativas al derecho-deber de informar previstas en el artículo 18 de la LPDP estableciendo que el grado de reproche de la conducta se determinará en atención a la cantidad de condiciones que no se haya cumplido con informar al titular del dato personal pudiéndose tratar de una infracción leve o grave, conforme a lo delimitado por la escala y tipo de sanción establecida en el artículo 39 de la LPDP.

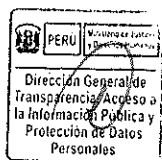
Tipificación de infracciones por el incumplimiento del principio – deber de seguridad, contenido en la Ley de Protección de Datos Personales (LPDP)

El artículo 9 de la LPDP contempla el principio de seguridad, a través del cual el titular del banco de datos personales y el encargado de su tratamiento, se encuentran obligados a adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales; asimismo, las medidas de seguridad deben ser apropiadas y acordes con el tratamiento a efectuar y con la categoría de datos personales de que se trate.

Por otro lado, el artículo 16 de la LPDP señala que, para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado; asimismo, señala que queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.

Por otra parte, conforme al artículo 3 de la LPDP, existe la obligación de brindar una especial protección cuando el tratamiento involucre datos personales sensibles, esto es, aquellos que se encuentran constituidos por los datos biométricos 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 o a la vida sexual.

En virtud de las obligaciones señaladas, en el Proyecto de Reglamento se incorporan las siguientes infracciones administrativas:



E. LUNA C.

Infracción Grave - Inciso 4 del artículo 141 del Proyecto del Reglamento: *"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia, y generando con ello un perjuicio al titular del dato personal o una exposición no autorizada de sus datos personales."*



G. VALDIVIESO R.

Infracción Muy Grave - Inciso 4 del artículo 142 del Proyecto del Reglamento: *"Realizar tratamiento de datos personales sensibles incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia, y generando con ello un perjuicio al titular del dato personal sensible o una exposición no autorizada de sus datos personales sensibles."*



E. REBAZA I.

Como se advierte, las previsiones legales contempladas en los artículos 3, 9 y 16 de la LPDP precitados fijan el contenido esencial que debe considerarse para tipificar las conductas sancionables incorporadas en el inciso 4 del artículo 140 y el inciso 4 del artículo 142 del Proyecto del Reglamento; es decir, la obligación legal de adoptar medidas de seguridad para el tratamiento de los datos personales, en especial de los datos sensibles, con la finalidad de evitar un perjuicio al titular de los datos personales por su alteración, pérdida, tratamiento o acceso no autorizado.

A efectos del cumplimiento de las obligaciones legales establecidas en los artículos 3, 9 y 16 de la LPDP, en el inciso 4 del artículo 140 y el inciso 4 del artículo 142 del Proyecto del Reglamento se precisa las infracciones a considerar por el incumplimiento de tales disposiciones vinculadas al principio de seguridad, considerando un mayor reproche jurídico si estas involucran datos personales de carácter sensible cuando existió algún perjuicio al titular de los datos por las circunstancias del artículo 16 de la LPDP.

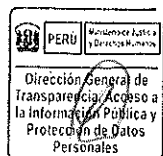
Por otro lado, el literal e) del inciso 9.1 del artículo 9 del Decreto de Urgencia N.º 007-2020³⁴ establece que las entidades de la administración pública y los proveedores de los servicios digitales deben reportar y colaborar con la autoridad de la protección de datos personales cuando se verifique un incidente de seguridad digital que involucre datos personales. Asimismo, conforme al artículo 108 del Reglamento del Decreto Legislativo N.º 1412, Ley de Gobierno Digital³⁵, aprobado por Decreto Supremo N.º 029-2021-PCM, existe la obligación normativa de que las entidades públicas comuniquen y colaboren con la Autoridad Nacional de Protección de Datos Personales ante la identificación de incidentes de seguridad digital cuando involucren datos, dentro del plazo de 48 horas a partir de la toma de conocimiento de la brecha de seguridad.

En virtud de las obligaciones señaladas, en el Proyecto de Reglamento se incorpora la siguiente infracción administrativa:

Infracción Grave - Inciso 12 del artículo 141 del Proyecto del Reglamento: *"No comunicar a la Autoridad Nacional de Protección de Datos Personales el incidente de seguridad cuando se genere exposición de datos personales y/o datos sensibles o cuando exista un alto riesgo para los derechos y libertades de las personas naturales."*

Como se aprecia, en el inciso 12 del artículo 141 del Proyecto del Reglamento se incluye la infracción administrativa vinculada al incumplimiento de comunicar a la Autoridad Nacional de Protección de Datos Personales el incidente de seguridad, particularmente en aquellos supuestos en los que se genere exposición de datos personales o sensibles, o cuando exista un alto riesgo para los derechos y libertades de las personas naturales.

Sobre el contenido de la definición de un incidente de seguridad, el Grupo de Trabajo de Artículo 29, en su Dictamen 03/2014 sobre la notificación de violación



E. LUNA C. 34

Decreto de Urgencia N.º 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento
(...)

Artículo 9. Obligaciones del Proveedor de servicios digitales

9.1 Las entidades de la administración pública, los proveedores de servicios digitales del sector financiero, servicios básicos (energía eléctrica, agua y gas), salud y transporte de personas, proveedores de servicios de internet, proveedores de actividades críticas y de servicios educativos, deben:

(...)

e) Reportar y colaborar con la autoridad de la protección de datos personales cuando verifiquen un incidente de seguridad digital que involucre datos personales.

Reglamento del Decreto Legislativo N.º 1412, Ley de Gobierno Digital, aprobado por Decreto Supremo N.º 029-2021-PCM
(...)

Artículo 108.- Incidentes de Seguridad Digital relativos a Datos Personales

Las entidades públicas comunican y colaboran con la Autoridad Nacional de Protección de Datos Personales ante la identificación de incidentes de seguridad digital que hayan afectado los datos personales, comunicándose en un plazo máximo de 48 horas, a partir de la toma de conocimiento de la brecha de seguridad.



G. VALDIVIESO P. 35



E. REDAZA I.

de datos personales³⁶, explicó que las violaciones pueden clasificarse con arreglo a los siguientes tres conocidos principios de seguridad de la información:

- Violación de la confidencialidad: cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos. Violación de la integridad: cuando se produce una alteración no autorizada o accidental de los datos personales.
- Violación de la disponibilidad: cuando se produce una pérdida de acceso accidental o no autorizada a los datos personales, o la destrucción de los mismos.

Se debe tener en cuenta la importancia de la acciones para revertir la vulneración de seguridad y la inmediata comunicación a la Autoridad, a efectos de evitar efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales, tales como la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos sujetos a secreto profesional.

En atención a ello, considerando los efectos del incidente de seguridad de datos personales, y a efectos de coadyuvar con la eficacia de la fiscalización en materia de protección de datos personales, resulta de vital importancia que la Autoridad Nacional de Protección de Datos Personales esté informada sobre la vulneración de seguridad, a fin de garantizar la protección de datos personales de los titulares afectados.

La obligación de comunicar a la Autoridad tiene el objetivo de que se tome conocimiento de la existencia del incidente de seguridad, lo cual no implica que necesariamente despliegue alguna acción que incida en la fiscalización en materia de protección de datos personales, sin perjuicio de existir determinados supuestos en los que sea necesario la apertura de acciones de fiscalización a efectos de verificar si el incidente se derivó por un incumplimiento de las medidas de seguridad de datos personales a las que el responsable de tratamiento se encontraba obligado.

En ese contexto, se recurre a la colaboración reglamentaria para precisar en el artículo 35 del Proyecto de Reglamento que esta obligación corresponde a todo responsable del tratamiento de datos personales, debiendo notificar a la Autoridad Nacional de Protección de Datos Personales dentro de las 48 horas posteriores a haber tenido constancia de un incidente de seguridad que afecte a datos personales, detallando en los artículos 35, 36 y 37 el contenido de la información que debe ser notificada a la autoridad, la obligación de documentar incidentes de seguridad y las obligaciones del encargado del tratamiento de datos personales ante un incidente de seguridad.

Asimismo, conforme a la potestad para tipificar infracciones vía reglamentaria, resulta necesario incluir un dispositivo reglamentario que sancione "*No comunicar a la Autoridad Nacional de Protección de Datos Personales el incidente de seguridad cuando se genere exposición de datos personales y/o datos sensibles o cuando exista un alto riesgo para los derechos y libertades de las personas naturales*", el cual tiene sustento legal en lo establecido en los artículos 3, 9 y 16 de la LPDP y la normativa antes mencionada sobre la comunicación de incidentes de seguridad.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA L.

³⁶ Dictamen 03/2014 sobre la notificación de violación de datos personales: <https://ec.europa.eu/newsroom/article29/items/612052>

Incorporación de infracciones por el incumplimiento de obligaciones de los administrados vinculadas al adecuado ejercicio de las funciones otorgadas a la Autoridad Nacional de Protección de Datos Personales

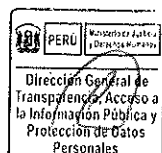
Conforme a lo establecido en el inciso 19 del artículo 33 de la LPDP, la Autoridad Nacional de Protección de Datos Personales se encuentra encargada de supervisar la sujeción del tratamiento de los datos personales que efectúen el titular y el encargado del banco de datos personales a las disposiciones técnicas que ella emita y, en caso de contravención, disponer las acciones que correspondan.

Asimismo, conforme al inciso 17 y 20 del mismo artículo 33 de la LPDP, la Autoridad Nacional de Protección de Datos Personales debe velar por el cumplimiento de la legislación vinculada con la protección de datos personales y por el respeto de sus principios rectores; y, se encuentra facultada a iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su Reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento.

Ahora bien, para el ejercicio de la actividad de fiscalización y las otras funciones a cargo de la Autoridad Nacional de Protección de Datos Personales, es indispensable la colaboración de los administrados y todo participe del procedimiento, en virtud del principio de buena conducta procedimental³⁷ establecido en el Artículo IV del Título Preliminar del TUO de la Ley 27444, quienes deben cooperar y/o colaborar con la autoridad para verificar el cumplimiento de las obligaciones vinculadas con la protección de datos personales y el respeto de sus principios rectores de la LPDP y su Reglamento.

Precisamente, conforme al numeral 2 del artículo 67 del TUO de la Ley 27444³⁸, todo administrado tiene el deber de cooperar y/o colaborar con la autoridad; y, se

37



E. LUNA C.

Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N.º 004-2019-JUS

(...)

TÍTULO PRELIMINAR

Artículo IV.- Principios del procedimiento administrativo

1. El procedimiento administrativo se sustenta fundamentalmente en los siguientes principios, sin perjuicio de la vigencia de otros principios generales del Derecho Administrativo:

(...)

1.8. Principio de buena fe procedimental. - La autoridad administrativa, los administrados, sus representantes o abogados y, en general, todos los partícipes del procedimiento, realizan sus respectivos actos procedimentales guiados por el respeto mutuo, la colaboración y la buena fe. La autoridad administrativa no puede actuar contra sus propios actos, salvo los supuestos de revisión de oficio contemplados en la presente Ley.

Ninguna regulación del procedimiento administrativo puede interpretarse de modo tal que ampare alguna conducta contra la buena fe procedimental.

(...)

38



G. VALDIVIESO R.

Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N.º 004-2019-JUS

(...)

Artículo 67.- Deberes generales de los administrados en el procedimiento

Los administrados respecto del procedimiento administrativo, así como quienes participen en él, tienen los siguientes deberes generales:

1. Abstenerse de formular pretensiones o articulaciones ilegales, de declarar hechos contrarios a la verdad o no confirmados como si fueran fehacientes, de solicitar actuaciones meramente dilatorias, o de cualquier otro modo afectar el principio de conducta procedimental
2. Prestar su colaboración para el pertinente esclarecimiento de los hechos
3. Proporcionar a la autoridad cualquier información dirigida a identificar a otros administrados no comparecientes con interés legítimo en el procedimiento.



E. REBAZA I.

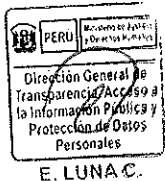
encuentra obligados a cumplir con los requerimientos que efectúe la autoridad para el esclarecimiento de los hechos, de lo contrario, su conducta eventualmente constituirá una obstrucción en las labores de la Autoridad Nacional de Protección de Datos Personales.

A través del Decreto Legislativo 1272³⁹, se incorporó disposiciones relacionadas a la actividad administrativa de fiscalización de la administración pública, las cuales también son aplicables a los procedimientos de todas las entidades en los tres niveles de gobierno, estableciendo garantías mínimas para los administrados fiscalizados, así como los deberes y reglas básicas que se deben cumplir para un ejercicio proporcionado y adecuado de la potestad fiscalizadora.

Asimismo, el inciso 2 del artículo 243 del TUO de la Ley 27444 establece la obligación del administrado fiscalizado en permitir el acceso de los funcionarios, servidores y terceros fiscalizadores, a sus dependencias, instalaciones, bienes y/o equipos, de administración directa o no, sin perjuicio de su derecho fundamental a la inviolabilidad del domicilio cuando corresponda, en el marco de un procedimiento de fiscalización.

Por su parte, el artículo 240 en concordancia con el inciso 1 del artículo 243 del TUO de la Ley 27444⁴⁰, establece las obligaciones del administrado fiscalizado en brindar todas las facilidades para que la autoridad pueda ejecutar inspecciones, con o sin previa notificación, en los locales y/o bienes de las personas naturales o jurídicas objeto de las acciones de fiscalización; así como brindar toda la información o documentación requerida por la autoridad en el marco de un procedimiento de fiscalización.

En complemento de lo anterior, la obligación del administrado de facilitar información y documentos necesarios en el entorno de acciones de fiscalización o un procedimiento sancionador, resulta fundamental para un proporcionado y adecuado ejercicio de la función fiscalizadora; y, también para que la Autoridad Nacional de Protección de Datos Personales, en ejercicio de sus funciones



39

4. *Comprobar previamente a su presentación ante la entidad, la autenticidad de la documentación sucedánea y de cualquier otra información que se ampare en la presunción de veracidad.*
(Subrayado añadido)

Decreto Legislativo que modifica la Ley N.º 27444, Ley del Procedimiento Administrativo General y deroga la Ley N.º 29060, Ley del Silencio Administrativo, publicado el 21 de diciembre de 2016.

40

Texto Único Ordenado de la Ley Nro. 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nro. 004-2019-JUS
(...)

Artículo 243.- Deberes de los administrados fiscalizados

Son deberes de los administrados fiscalizados:

1. Realizar o brindar todas las facilidades para ejecutar las facultades listadas en el artículo 240.

(...)

Artículo 240.- Facultades de las entidades que realizan actividad de fiscalización

(...)

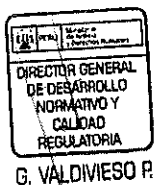
240.2 La Administración Pública en el ejercicio de la actividad de fiscalización está facultada para realizar lo siguiente:

1. Requerir al administrado objeto de la fiscalización, la exhibición o presentación de todo tipo de documentación, expedientes, archivos u otra información necesaria, respetando el principio de legalidad.

El acceso a la información que pueda afectar la intimidad personal o familiar, así como las materias protegidas por el secreto bancario, tributario, comercial e industrial y la protección de datos personales, se rige por lo dispuesto en la Constitución Política del Perú y las leyes especiales.

(...)

3. Realizar inspecciones, con o sin previa notificación, en los locales y/o bienes de las personas naturales o jurídicas objeto de las acciones de fiscalización, respetando el derecho fundamental a la inviolabilidad del domicilio cuando corresponda.



G. VALDIVIESO R.



E. REBAZA I.

establecidas en los incisos 19 y 20, aplique de forma razonable las sanciones administrativas correspondientes y ordene de manera oportuna las medidas cautelares o correctivas que fije el Reglamento de la LPDP.

Al respecto, justamente el inciso 2 del artículo 68 del TUO de la Ley 27444 establece la obligación del administrado respecto a los procedimientos investigatorios, a facilitar la información y documentos que conocieron y fueron razonablemente adecuados a los objetivos de la actuación para alcanzar la verdad material.

En virtud de esto último, el artículo 114 del Proyecto de Reglamento, al igual que el actual Reglamento de la LPDP dispone que debe dejarse constancia en el acta de fiscalización, del acto o los actos obstructivos del administrado fiscalizado y de su reiteración, de ser el caso, siendo actos obstructivos el negarse directamente a colaborar u demorar injustificadamente su colaboración, plantear cuestionamientos no razonables a la labor fiscalizadora, desatender las indicaciones de los fiscalizadores o cualquier otra conducta similar o equivalente.

En atención a las obligaciones legales contempladas en la normativa de la materia, en complemento con las disposiciones contempladas en el TUO de la Ley N.º 27444, en el proyecto de Reglamento se ha incorporado las siguientes infracciones administrativas:

- **Infracción Grave** - Inciso 8 del artículo 141 del Proyecto del Reglamento: *"Negar o demorar injustificadamente a la Autoridad Nacional de Protección de Datos Personales el ingreso a las instalaciones objeto de la fiscalización."*
- **Infracción Grave** - Inciso 9 del artículo 141 del Proyecto del Reglamento: *"Negarse injustificadamente a proporcionar a la Autoridad Nacional de Protección de Datos Personales la información o la documentación relativa al tratamiento de datos personales que esta le requiera en el marco de una fiscalización o procedimiento administrativo en curso."*

Infracción Muy Grave - Inciso 2 del artículo 142 del Proyecto del Reglamento: *"Suministrar documentos o información falsa o inexacta a la Autoridad Nacional de Protección de Datos Personales."*



Por lo expuesto, se aprecia que las infracciones incorporadas a través de los incisos 8 y 9 del artículo 141 e inciso 2 del artículo 142 del Proyecto del Reglamento han previsto prohibiciones que se desprenden, con un grado de certeza suficiente, a partir del propio texto legal de las disposiciones legales antes citadas, las cuales obligan al administrado en brindar las facilidades para la ejecución de inspecciones y facilitar la información requerida por la autoridad durante el desarrollo e acciones de fiscalización o en el marco de un procedimiento administrativo sancionador en curso.

Respecto a la tipificación de la infracción administrativa incorporada en el inciso 2 del artículo 142 del Proyecto del Reglamento, se debe precisar adicionalmente que esta disposición reglamentaria se encuentra sustentada en el deber del administrado de colaborar con la entidad para el esclarecimiento de los hechos, absteniéndose de declarar hechos contrarios a la verdad o no confirmados como si fueran fehacientes, o de cualquier otro modo afectar el principio de conducta procedimental, siendo que estas obligaciones, establecidas en los incisos 1 y 2



del artículo 67 del TUO de la Ley 27444⁴¹, constituyen las características esenciales de la conducta antijurídica tipificada.

Cabe precisar que la gravedad de las conductas tipificadas se encuentra dentro de lo delimitado por la escala y tipo de sanción establecida en el artículo 39 de la LPDP; y, resulta de importancia su incorporación, a fin de desincentivar aquellas conductas que puedan obstaculizar el ejercicio de las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras de la Autoridad Nacional de Protección de Datos Personales, reguladas en el artículo 33 de la LPDP.

Incorporación de infracciones por el incumplimiento de otras obligaciones establecidas en la LPDP

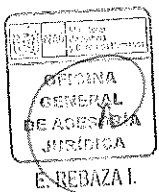
El numeral 2 artículo del artículo 34 de la LPDP establece la obligación de inscribir en el Registro Nacional de Protección de Datos Personales las comunicaciones de flujo transfronterizo de datos personales. Asimismo, es función de la Autoridad Nacional de Protección de Datos Personales supervisar el cumplimiento de las exigencias previstas en la LPDP, respecto al flujo transfronterizo de datos personales, conforme a lo establecido en el numeral 8 del artículo 33 de la LPDP.

En ese contexto, el inciso 8 del artículo 140 del Proyecto de Reglamento tipifica la siguiente infracción administrativa leve: *"No comunicar el flujo transfronterizo de datos personales a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para su inscripción en el Registro Nacional de Protección de Datos Personales."*

La infracción antes citada tiene como sustento la base legal establecida en el inciso 2 artículo del artículo 34 de la LPDP; y, asimismo, su incumplimiento constituye una infracción leve, de conformidad con el artículo 39 de la LPDP.

Por otro lado, el inciso 7 del artículo 140 del Proyecto de Reglamento incorpora la siguiente infracción administrativa leve: *"Atender fuera de plazo el ejercicio material de los derechos del titular de datos personales, cuando legalmente proceda"*.

La obligación legal del titular o el responsable de tratamiento de datos personales, respecto al ejercicio material de los derechos del titular de datos personales se desprenden del ejercicio de los derechos de acceso, rectificación, cancelación y oposición que se encuentran contenidos en los artículos 19, 20 y 22 del Título III de la Ley 29733⁴²; y, constituyen la norma sustantiva de obligatorio cumplimiento.



41

Texto Único Ordenado de la Ley Nro. 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nro. 004-2019-JUS

(...)

Artículo 67.- Deberes generales de los administrados en el procedimiento

Los administrados respecto del procedimiento administrativo, así como quienes participen en él, tienen los siguientes deberes generales:

1. Abstenerse de formular pretensiones o articulaciones ilegales, de declarar hechos contrarios a la verdad o no confirmados como si fueran fehacientes, de solicitar actuaciones meramente dilatorias, o de cualquier otro modo afectar el principio de conducta procedimental
2. Prestar su colaboración para el pertinente esclarecimiento de los hechos.

(...)

42

Texto Único Ordenado de la Ley Nro. 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo Nro. 004-2019-JUS

(...)

Artículo 19. Derecho de acceso del titular de datos personales

El titular de datos personales tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos

Además, el artículo 24 de la LPDP, establece que su ejercicio debe solicitarse ante el titular o encargado del tratamiento de datos personales, de manera previa a que se recurra ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data; por lo cual, se desprende la obligación del titular o encargado del tratamiento de datos personales de atender la solicitud del titular de los datos personales.

Asimismo, de forma complementaria a la norma sustantiva, en su artículo 81 del Proyecto de Reglamento, al igual que el actual Reglamento, se establece un plazo máximo para que el titular o el responsable de tratamiento de datos personales, resuelva la solicitud de tutela directa presentada por el titular de los datos personales en ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.

fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos.

Artículo 20. Derecho de actualización, inclusión, rectificación y supresión

El titular de datos personales tiene derecho a la actualización, inclusión, rectificación y supresión de sus datos personales materia de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento.

Si sus datos personales hubieran sido transferidos previamente, el encargado de tratamiento de datos personales debe comunicar la actualización, inclusión, rectificación o supresión a quienes se hayan transferido, en el caso que se mantenga el tratamiento por este último, quien debe también proceder a la actualización, inclusión, rectificación o supresión, según corresponda.

Durante el proceso de actualización, inclusión, rectificación o supresión de datos personales, el encargado de tratamiento de datos personales dispone su bloqueo, quedando impedido de permitir que terceros accedan a ellos. Dicho bloqueo no es aplicable a las entidades públicas que requieren de tal información para el adecuado ejercicio de sus competencias, según ley, las que deben informar que se encuentra en trámite cualquiera de los mencionados procesos.

La supresión de datos personales contenidos en bancos de datos personales de administración pública se sujeta a lo dispuesto en el artículo 21 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, o la que haga sus veces"

Artículo 22. Derecho de oposición

Siempre que, por ley, no se disponga lo contrario y cuando no hubiera prestado consentimiento, el titular de datos personales puede oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En caso de oposición justificada, el titular o el encargado de tratamiento de datos personales, según corresponda, debe proceder a su supresión, conforme a ley".

Artículo 24. Derecho a la tutela

En caso de que el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de los derechos establecidos en esta Ley, este puede recurrir ante la Autoridad Nacional de Protección de Datos Personales en vía de reclamación o al Poder Judicial para los efectos de la correspondiente acción de hábeas data.

El procedimiento a seguir ante la Autoridad Nacional de Protección de Datos Personales se sujeta a lo dispuesto en los artículos 219 y siguientes de la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces.

La resolución de la Autoridad Nacional de Protección de Datos Personales agota la vía administrativa y habilita la imposición de las sanciones administrativas previstas en el artículo 39. El reglamento determina las instancias correspondientes.

Contra las resoluciones de la Autoridad Nacional de Protección de Datos Personales procede la acción contencioso-administrativa.



E. LUNA C.



G. VALDIVIESO P.



E. REDAZA I.

Así entonces, se ha tipificado como infracción leve la conducta consistente en “atender fuera del plazo las solicitudes que se presentan para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición” en tanto su inobservancia constituye incumplimiento a las obligaciones contenidas Título III de la LPDP.

IV. ANÁLISIS DE IMPACTOS CUANTITATIVOS Y/O CUALITATIVOS

Desde el punto de vista cuantitativo, el presente Reglamento no irrogará costos adicionales a las entidades de la Administración Pública, puesto que se financia con el presupuesto del pliego presupuestario aprobado por las entidades de los tres niveles de gobierno, sin demandar recursos adicionales al tesoro público.

Desde el punto de vista cualitativo, el presente Reglamento, que regula diversos mecanismos y figuras para optimizar el ejercicio del derecho de protección de datos personales, tendrá un alto impacto positivo y resultará beneficioso para los titulares de los datos personales y la sociedad en general, toda vez que permitirá que el país cuente con un marco normativo actualizado y con un mayor nivel de protección de datos que procura adaptarse a nuevas formas de tratamiento, las cuales vienen siendo determinados por el avance de la tecnología y un entorno digital cada vez más creciente.

En esa línea, por ejemplo, mediante la incorporación expresa del término “elaboración de perfiles” en el Artículo II. “Definiciones” se busca afianzar el ámbito de aplicación y la competencia de la Autoridad Nacional en este tipo de supuestos que vienen siendo muy utilizados por el sector empresarial para fines de marketing, publicidad y comercio electrónico⁴³. De este modo, se fortalece el alcance de la tutela brindada por la Autoridad Nacional, lo cual redundará en favor del cumplimiento de las garantías de los titulares de datos personales.

Cabe precisar que la definición de la expresión “elaboración de perfiles” se encuentra prevista en diferentes documentos internacionales, como es el caso del Reglamento General de Protección de Datos⁴⁴, de modo tal que, al incorporarse como definición en el texto del presente Reglamento de la Ley N.º 29733, la regulación peruana se encuentre alineada con el estándar actual en documentos que rigen países que cuentan con niveles de protección adecuada en materia de protección de datos personales.

De otro lado, se ha procurado regular un vacío normativo respecto del tratamiento de los datos de las personas fallecidas, estableciendo que dicho supuesto se encuentra excluido del ámbito del presente Reglamento⁴⁵, sin que ello involucre desconocer que



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

⁴³ El uso del tratamiento “elaboración de perfiles” ha crecido en el Perú; así este tratamiento es utilizado por diferentes empresas, como por la empresa Enel X store que cuenta con el formulario web consentimiento para tratamiento de datos personales y elaboración de perfiles, el cual puede ser visualizado a través del siguiente enlace: <https://www.enelxstore.com/pe/es/legal/peru-lead-profiling-.html>

⁴⁴ El artículo 4, numeral 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos define la “elaboración de perfiles” como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

⁴⁵ Sobre el criterio de exclusión del tratamiento de personas fallecidas en los alcances de la LPDP y el actual Reglamento se ha emitido el Informe Jurídico N.º 020-2022-JUS/DGTAIPD de 4 de octubre de 2022 denominado “Opinión sobre el Proyecto de Ley N.º 2574/2021-CR que propone la “Ley que faculta al RENIEC a regular mediante procedimiento administrativo simplificado la rectificación de datos personales de personas fallecidas”. Véase: <https://cdn.www.gob.pe/uploads/document/file/4033553/Sobre%20el%20Proyecto%20de%20Ley%20N%C2%B02574/2021-CR%20que%20propone%20la%20E2%80%9CLey%20que%20faculta%20al%20RENIEC%20a%20regular%20mediante%20procedimiento%20administrativo%20simplificado%20la%20rectificaci%C3%B3n%20de%20datos%20personales%20de%20personas%20fallecidas%E2%80%9D.pdf?v=1673366741>

los familiares directos (cónyuge, hijos, padres, hermanos) u otra persona interés legítimo subjetivo, por razones familiares u otros análogos, puedan solicitar el acceso a los datos personales de la persona fallecida y, en su caso, su rectificación o supresión.

De este modo, se busca crear predictibilidad y seguridad jurídica para los administrados excluyendo de sus alcances el tratamiento de datos de personas fallecidas, pero regulando expresamente que sus familiares puedan solicitar el acceso a su información buscando resguardar la memoria o buena reputación del fallecido.

Asimismo, a efectos de consolidar el rol de la ANPD como autoridad garante en materia de protección de datos personales, el presente Reglamento también incorpora nuevas disposiciones relativas al ámbito de aplicación territorial, estableciendo expresamente que se encuentran dentro de su alcance aquellos casos en que el titular del banco de datos personales o quien resulte responsable del tratamiento (no ubicado en territorio peruano) realice actividades relacionadas a la "oferta de bienes y servicios" dirigidos a titulares de datos ubicados en territorio peruano.

Lo mismo aplicaría en el caso en que el titular del banco de datos personales o quien resulte responsable del tratamiento no se encuentre en territorio peruano, pero realiza actividades orientadas al "*análisis de comportamiento de los titulares de datos personales ubicados en territorio peruano*", así como la "*elaboración de perfiles*" que busquen predeterminar conductas, preferencias, hábitos o similares.

Resulta importante incluir expresamente en el ámbito territorial del Reglamento las actividades orientadas al "análisis de comportamiento de los titulares de datos personales ubicados en territorio peruano" así como la "elaboración de perfiles", a efectos de que las competencias desplegadas por la Autoridad no queden relegadas, sino que vayan aparejadas con las actuales prácticas comerciales y empresariales.

En la misma línea, considerando que existen empresas extranjeras que no cuentan con un representante en Perú encargado del cumplimiento de las obligaciones en materia de protección de datos, el presente Reglamento prevé que el titular del banco de datos o quien resulte responsable debe designar formalmente a un representante fuera del territorio peruano, lo cual traería consigo los siguientes beneficios:

- El representante, como punto de enlace entre la Autoridad Nacional y las empresas extranjeras, podrá velar por la implementación de la LPDP y su Reglamento dentro de la empresa a la cual pertenece y, en consecuencia, responderá cualquier requerimiento de la Autoridad.
- El representante deberá atender las solicitudes de los titulares de los datos personales efectuados a la empresa extranjera, con lo cual, se fortalecerá la protección de los datos personales de dichos titulares.
- El representante tendrá flexibilidad para ubicarse fuera del territorio peruano, siempre que el mismo pueda estar acreditado para atender procesalmente toda gestión de comunicación realizada por la Autoridad Nacional, así como solicitudes de los titulares de los datos, denuncias o similares que se deriven de los procedimientos administrativos.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZAL.

De otro lado, en el afán de optimizar el nivel de cumplimiento de los sujetos obligados por la normativa de protección de datos personales, mediante el presente Reglamento se ha incorporado el *Principio de Responsabilidad Proactiva* que prevé que en el tratamiento de datos personales se deben aplicar las medidas legales, técnicas y organizativas a fin de garantizar el cumplimiento efectivo de la normativa de datos

personales, y el titular del banco de datos personales o quien resulte responsable, debiendo este último ser capaz de demostrar su cumplimiento.

La incorporación del *Principio de Responsabilidad Proactiva*, permitirá elevar el estándar de protección de datos personales en el país al constituir un mandato para los titulares de bancos de datos o responsables de tratamiento que los obliga a adoptar, por sí mismos y de forma anticipada, medidas técnicas y organizativas para garantizar los derechos de los titulares de los datos personales, tomando activamente el control a efectos de evitar cualquier riesgo para los titulares de los datos personales.

Es claro que la dinámica de los servicios digitales⁴⁶ ha determinado el aumento de las transferencias internacionales o flujos transfronterizos de datos personales, obligando a la Autoridad Nacional a actualizar las disposiciones del Reglamento en dicha materia. En atención a ello, mediante el presente Reglamento se ha regulado otorgar mayor participación a la Autoridad Nacional de Protección de Datos Personales, estableciendo y haciendo predecibles las pautas a utilizar a fin de determinar el nivel de protección adecuado en materia de protección de datos de determinado país.

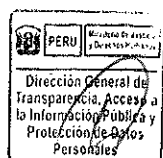
En la misma línea, en el presente Reglamento se establece la disposición relativa a que la ANPD emita Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales como un instrumento que permitirá superar las limitaciones en las actuales transferencias internacionales de datos y contribuirá a que éstas se realicen bajo condiciones que resguarden el derecho de los titulares de los datos, en armonía con la normativa en materia de protección de datos personales.

El uso de Cláusulas Contractuales Modelo tiene el potencial de coadyuvar a superar las limitaciones en las actuales transferencias de datos que se deriven de las diferencias en el nivel de protección entre los diferentes países, en consideración a que dichas cláusulas contribuyen a construir una convergencia a nivel contractual (entre privados) sin necesariamente requerir convergencia a nivel de país.

Asimismo, con el uso de las cláusulas contractuales se facilita el cumplimiento de los requisitos previstos en la ley de protección de datos del país exportador de datos personales para la transferencia de dichos datos a un tercer país que no haya sido reconocido con un nivel adecuado de protección, de modo tal que las garantías inicialmente otorgadas a los datos personales continúen con independencia del lugar donde estos datos se encuentren.

Con el uso de las cláusulas contractuales se permite que las empresas no tengan que negociar y pactar acuerdos en cada caso individual, con el coste económico que ello implica (por representación legal y tiempo), pues se puede utilizar el modelo de cláusulas aprobado por la Autoridad Nacional, sabiendo que, al implementarlas y cumplirlas, las empresas y entidades observan sus obligaciones legales en materia de transferencia internacional de datos personales con una solución sencilla y práctica.

En el presente Reglamento además se prevén disposiciones específicas para determinados tipos de tratamiento de datos personales, por ejemplo, se establece que cuando se trate de servicios digitales ofrecidos de forma directa a menores de edad y resulte necesario el consentimiento de los titulares de la patria potestad o tutores, el titular del banco de datos o responsable del tratamiento debe acreditar, conforme al artículo 9 del presente Reglamento, tal consentimiento considerando los medios



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

⁴⁶ Según la Cámara Peruana de Comercio Electrónico - CAPECE en el 2021⁴⁶, los compradores online ascienden a 13.9 millones, el tamaño del mercado online en Perú es de US\$ 9300 millones, la penetración del e-commerce en el consumo de tarjetas es de 45% y el volumen de las ventas online provienen de e-commerce retail 52%. <https://www.capece.org.pe/wp-content/uploads/2021/03/Observatorio-Ecommerce-Peru-2020-2021.pdf>

digitales disponibles para tal efecto. Mediante esta disposición se potencia la especial tutela y protección que requiere el tratamiento de datos personales de menores de edad, particularmente, cuando se trata de servicios digitales.

Del mismo modo, se regula la obligación de los titulares de bancos de datos personales, o de quien resulte responsable del tratamiento de datos de menores de garantizar la protección del interés superior del niño y de sus derechos fundamentales con particular énfasis en la publicación o difusión de sus datos personales a través de servicios digitales permitiendo fortalecer la tutela de los derechos de los menores de edad.

Asimismo, se incorpora en el Reglamento que, cuando los datos personales son tratados para fines de publicidad y prospección comercial (incluido la elaboración de perfiles) el titular de datos personales puede oponerse en cualquier momento al tratamiento de sus datos personales. De este modo, se busca fortalecer la tutela de los titulares de datos que no están de acuerdo con el tratamiento que se realiza sobre su información personal, sobre todo en entornos comerciales o de publicidad donde, en un afán lucrativo, estos podrían ser usados sin cumplir las garantías normativas.

Adicionalmente, el presente Reglamento incorpora como novedad una disposición relativa a la posibilidad de realizar la Evaluación de Impacto del Tratamiento de Datos Personales, como mecanismo de responsabilidad proactiva, que permite a los titulares de los bancos de datos personales o responsable del tratamiento realizar, de forma previa al tratamiento de datos, un análisis del impacto o riesgos que implicará el tratamiento sobre determinados datos.

El gran beneficio de la *Evaluación de impacto de tratamiento de datos personales* radica en que permite que, de manera anticipada, se identifique cualquier tipo de riesgo existente sobre los datos personales que administran y así poder adoptar medidas organizativas o de seguridad necesarias mitigar dichos riesgos y, de esa manera, evitar incurrir en incumplimientos normativos o infracciones administrativas y/o afectar el derecho de los titulares de datos que manejan.

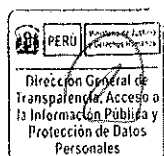
El cumplimiento de medidas de seguridad en el tratamiento de datos personales adquiere particular necesidad en el entorno corporativo, por tal motivo, en lo relativo a las medidas mínimas que se deben implementar sobre seguridad digital de datos personales, se ha incorporado al Reglamento la obligación de notificación de incidentes de seguridad, lo cual permitirá que, al tomar conocimiento del incidente, la ANPD efectúe el seguimiento del caso a efectos de promover la restitución del daño generado y requerir el cumplimiento de las medidas de seguridad que corresponda.

Lo anterior resulta particularmente relevante en países latinoamericanos como el Perú que, según señala el ESET Security Report en Latinoamérica⁴⁷, es uno de los países más afectados en Latinoamérica por incidencias de seguridad vinculadas a robo de datos y espionaje.

En relación con lo anterior y en la búsqueda de un adecuado cumplimiento de la normativa de protección de datos personales, el Reglamento incorpora, en el sector público y en algunos casos en el sector privado, la obligación de designar un Oficial de datos personales, como figura que permitirá asegurar el cumplimiento de la normativa de protección de datos al interior de la organización o entidad pública.

Se debe tener en cuenta que la designación de un ODP, no genera *per se* gastos o costos, por el contrario, genera beneficios, siendo estos:

⁴⁷ <https://www.welivesecurity.com/wp-content/uploads/2022/07/ESET-security-report-LATAM-2022.pdf>



E. LUNA C.



G. VALDIVIESO P.



E. RESAZA I.

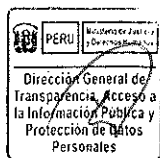
- Fortalece la imagen de la organización, ya que, valida un tratamiento adecuado de datos personales, y aporta valores de compromiso y ética sobre el uso de los datos personales.
- En la medida que promueve el cumplimiento del régimen jurídico de protección de datos personales puede implicar un impacto respecto la reducción de sanciones.
- Permite contar con una persona especializada para atender posibles riesgos o incidentes de seguridad de datos personales.
- Permite fortalecer la cultura la protección de datos al interior de la organización o entidad pública.

El presente Reglamento establece que el responsable del tratamiento de datos personales debe contar con un documento de seguridad el cual debe ser aprobado formalmente y contar con fecha cierta, siendo este la política de seguridad. Asimismo, este documento debe estar actualizado y contener como mínimo los procedimientos de gestión de accesos, la gestión de privilegios y la verificación periódica de los privilegios asignados, de modo tal que se promueve la prevención de riesgos de seguridad pudiendo evitar incluso sanciones que deriven de incumplimientos normativos.

La normativa vigente ha otorgado a la Autoridad Nacional potestad sancionadora como herramienta para garantizar el cumplimiento de las obligaciones vinculadas a la normativa de protección de datos personales.

En el nuevo Reglamento se propone tipificar como infracciones administrativas leve: *"Informar de forma incompleta de dos o menos de dos condiciones del tratamiento de los datos personales señaladas en el artículo 18 de la Ley"*; y, grave: *"No cumplir con el deber de informar o informar de forma incompleta de tres a más condiciones del tratamiento de los datos personales a los titulares de datos personales, de acuerdo con lo establecido en el artículo 18 de la Ley."*

La previsión de estos tipos infractores tendrá un impacto positivo al cubrir de manera expresa y taxativa el supuesto de incumplimiento del deber de informar contemplado en el artículo 18 de la LPDP, buscando fortalecer la seguridad jurídica y sobre todo el principio de predictibilidad, permitiéndole a los administrados conocer con claridad cuáles conductas consideradas como infracciones a efectos de regular su conducta en lo relativo al cumplimiento del deber de informar (artículo 18).



E. LUNA C.



G. VALDIVIESO P.



E. REDAZA I.

De otro lado, en aras de resolver el problema de interpretación existente respecto de la expresión "el ejercicio de los derechos" en el tipo infractor referido a *"no atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales"*, el presente Reglamento modifica la fórmula normativa precisando que dicha infracción se encuentra referida al ejercicio material de los derechos quedando así: *"No atender, impedir u obstaculizar el ejercicio material de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley N.º 29733 y su Reglamento"*.

De este modo, se genera predictibilidad y certeza en los administrados, en cuanto a cómo se determinará la responsabilidad derivada de esta infracción, pues la nueva fórmula: *"No atender, impedir u obstaculizar el ejercicio material de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley N.º 29733 y su Reglamento"* deja claro que esta infracción solo se utilizará al no atenderse, impedirse u obstaculizar el ejercicio material del derecho, esto es, cuando exista una solicitud de por medio y no solo por el mero incumplimiento del artículo 18 de la LPDP.

Asimismo, en los casos en que exista atención del ejercicio material de los derechos del

titular de datos personales, pero esta sea, demorada o extemporánea, no corresponderá la aplicación de la infracción grave precitada, sino de aquella contemplada en el inciso 7 del artículo 151 del Reglamento: *"Atender fuera de plazo el ejercicio material de los derechos del titular de datos personales, cuando legalmente proceda"* (infracción leve).

En lo relativo al incumplimiento de las medidas de seguridad, el presente Reglamento establece diferencias en el grado de reprochabilidad en atención al bien jurídico protegido. Así las cosas, realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa de la materia es imputado como infracción leve; sin embargo, en el caso de que tal incumplimiento genere perjuicio al titular del dato personal o exposición no autorizada de sus datos personales, corresponderá imputar una infracción grave. A su vez, si este tipo de tratamiento indebido estuvieran involucrados datos sensibles, la conducta del sujeto obligado debe imputarse como muy grave, conforme a lo establecido en el inciso 4 del artículo 153.

De este modo, se busca asegurar el cumplimiento del principio de seguridad a efectos de preservar la confidencialidad, disponibilidad e integridad de los datos de las personas; y de modo especial, en aquellos casos en los que la omisión de la medida de seguridad genere un perjuicio al titular del dato personal, la exposición no autorizada de sus datos o cuando se trate de datos sensibles (información relativa a datos genéticos o biométricos de la persona natural, 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).

Finalmente, en el presente Reglamento se incorpora como infracción grave la conducta consistente en: *"No comunicar a la Autoridad Nacional de Protección de Datos Personales el incidente de seguridad cuando se genere exposición o revelación de datos personales y/o datos sensibles o cuando exista un alto riesgo para los derechos y libertades de las personas naturales"*.

La incorporación de esta infracción grave al Reglamento resulta particularmente relevante a la luz de la información existente sobre incidentes de seguridad en el tratamiento de datos personales, de este modo, se busca generar incentivos para que, ante este tipo de incidentes, los administrados cumplan con comunicar dicha circunstancia a la Autoridad Nacional, más aún cuando se trata de casos en los que exista exposición o revelación de datos personales y/o datos sensibles o cuando exista un alto riesgo para los derechos y libertades de las personas naturales.

Resulta importante reforzar el cumplimiento de la comunicación de un incidente de seguridad a la Autoridad Nacional considerando que estas pueden tener efectos adversos considerables sobre la información de las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales, tales como la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos personales sujetos al secreto profesional.

En atención a la existencia de esta infracción y la posibilidad de una sanción por el incumplimiento de la obligación vinculada a los incidentes de seguridad, los administrados tendrán mayores incentivos para promover una constante supervisión más aún se genere exposición o revelación de datos personales y/o sensibles o cuando exista un alto riesgo para los derechos y libertades de las personas naturales.

La potestad sancionadora de la Autoridad Nacional se ha venido ejerciendo conforme al principio de legalidad, razonabilidad y con respeto del debido procedimiento, y en esa línea, el nuevo Reglamento contempla que la determinación de las multas se realiza



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

conforme a la Metodología para el cálculo de multas, aprobada por Resolución Ministerial N.º 0326-2020-JUS o norma que la sustituya. Esta especificación no se encontraba en el anterior Reglamento y lo que busca es brindar al administrado una herramienta normativa predecible y cierta, de acuerdo con la cual, se establecerán las multas en atención a criterios objetivos.

En suma, en cuanto a los principales beneficios de las principales disposiciones del nuevo Reglamento, podemos señalar lo siguiente:

a. Respetto a la ciudadanía:

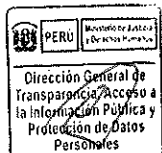
- Generar confianza al fortalecer las medidas que aseguren la protección de datos personales en el entorno digital, tanto las personas, como empresas y entidades públicas deben compartir la responsabilidad de salvaguardar el derecho a la protección de datos personales.
- Mayor confianza en el uso de canales digitales por parte de la ciudadanía, al establecer obligaciones al responsable de tratamiento de sus datos personales.
- Fortalecer el despliegue del proceso de transformación digital de manera sostenible, y confiables al fortalecer el marco regulatorio de datos personales.

b. Respetto a las entidades de la Administración Pública:

- Contar con disposiciones que permitan a las entidades públicas gestionar los riesgos de la privacidad de las personas.
- Fortalecer los roles para garantizar el adecuado uso de los datos personales, estableciendo como actor clave al Oficial de Datos Personales como el rol responsable de coordinar la gestión de un adecuado tratamiento de datos personales.

c. Respetto a las organizaciones privadas:

- Promover la interacción de los ciudadanos con los servicios digitales al establecer medidas para fortalecer un adecuado tratamiento de datos personales, lo cual impacta en el desarrollo de la economía y el libre flujo de datos.



E. LUNA C.

De acuerdo con lo expuesto, habiéndose revisado los beneficios que trae consigo las disposiciones más relevantes del presente Reglamento, podemos advertir que se trata de un documento normativo de alto impacto y beneficioso para los ciudadanos y sociedad en general, toda vez, que permitirá que el país cuente con un marco normativo más sólido y con un mayor nivel de protección de datos personales.



G. VALDIVIESO P.

Así, desde un análisis costo-beneficio, ciertamente los beneficios que generará la aprobación del nuevo Reglamento superan largamente los costos (presupuesto público) que implicaría su implementación; razón por la cual, resulta pertinente su aprobación.

V. ANÁLISIS DEL IMPACTO DE LA VIGENCIA DE LA NORMA EN LA LEGISLACIÓN NACIONAL

Análisis de constitucionalidad



E. REDAZA I.

Mediante los incisos 3 y 8 del artículo 118 de la Constitución Política del Perú, se reconoce la potestad del presidente de la República para dirigir la política general del gobierno y reglamentar las leyes sin transgredirlas ni desnaturalizarlas y dentro de tales límites dictar decretos y resoluciones.

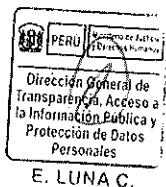
En esa línea, el inciso 6 del artículo 2 de la Constitución Política del Perú señala que, toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar.

Su desarrollo a nivel legislativo es realizado por la Ley N.º 29733, Ley de Protección de Datos Personales que, tiene por objeto garantizar el derecho a la protección de datos personales, previsto en el inciso 6 del artículo 2 de la Constitución Política del Perú.

Si bien la Ley N.º 29733, Ley de Protección de Datos Personales contempla los aspectos elementales y generales del derecho a la protección de los datos personales, dada su naturaleza de norma de desarrollo constitucional, no contiene reglas de detalle, operativas o precisas para tales efectos. Por ello, fue necesario complementar su articulado mediante un reglamento con la finalidad de asegurar su aplicación.

Así, el 22 de marzo de 2013, mediante Decreto Supremo N.º 003-2013-JUS se publicó el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales, cuyo objeto fue desarrollar la Ley N.º 29733 a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado.

Dicho reglamento, si bien consideró disposiciones respecto a las definiciones de los sujetos obligados al cumplimiento de las disposiciones en materia de protección de datos, obligaciones, limitaciones para el consentimiento para el tratamiento de datos, así como los relacionados a las tipificaciones administrativas, actualmente, no contiene disposiciones referidas a los riesgos asociados al incremento del uso de la tecnología en la era digital, lo cual representa mayores riesgos para los peruanos.

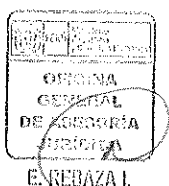


En ese sentido, debido a los avances y los riesgos en el entorno digital, resulta necesario establecer un nuevo reglamento que eleve los estándares regulatorios con el fin de salvaguardar los derechos fundamentales de las personas y ciudadanos en el entorno digital, especialmente en materia de protección de datos personales, garantizando que las personas naturales puedan tener el control de su información personal. Para ello, la propuesta normativa tiene en cuenta que el derecho a la protección de datos no es un derecho absoluto, sino que requiere un equilibrio y ponderación con otros derechos humanos, en observancia de los principios de proporcionalidad, necesidad y legalidad.



Así las cosas, desde el punto de vista constitucional, resulta válida la presente iniciativa reglamentaria, en tanto desarrolla aspectos concretos referidos al cumplimiento de las obligaciones de designar a un Oficial de Datos Personales en las entidades públicas y privadas, reportar los incidentes de seguridad que afecten datos personales, y, realizar la evaluación de impacto del tratamiento de datos personales.

Asimismo, permite reconocer la importancia y necesidad de la incorporación y regulación del derecho a la portabilidad de datos; así como garantizar la protección del tratamiento de datos de menores en internet. También busca desarrollar los alcances y preceptos para un nivel de protección adecuado en cuanto al flujo transfronterizo de datos personales. Del mismo modo, introduce nuevas y relevantes conductas infractoras que han sido incorporadas con la finalidad de asegurar el cumplimiento de la Ley de Protección de Datos Personales. Todas estas incorporaciones, no solo



guardan coherencia con la norma constitucional prevista en el inciso 6 del artículo 2 de la Constitución Política del Perú, sino que, permiten aplicarlas a los casos concretos.

En tal sentido, con el nuevo reglamento se cubriría de manera integral la ausencia de la regulación constitucional y legal sobre los vacíos normativos en cuanto a la protección de los datos personales, haciendo posible el ejercicio efectivo del derecho constitucional por sus titulares y el cumplimiento de las obligaciones que de ellas derivan para las entidades obligadas a satisfacer este derecho.

En consecuencia, de acuerdo con la Constitución Política del Perú, los ciudadanos tienen derecho a obtener protección frente a posibles abusos o riesgos derivados de la utilización de los datos, lo cual involucra contar con una norma reglamentaria que desarrolle los principios, garantías y mecanismos destinados a salvaguardar tal derecho, cuya aprobación es potestad del presidente de la República.

Análisis de legalidad

Los artículos I y VI del Título Preliminar de la Ley N.º 29158, Ley Orgánica del Poder Ejecutivo, establecen que los ministerios únicamente pueden ejercer las competencias que le han sido atribuidas a través de la Constitución Política del Perú y la Ley. Lo anterior se condice con lo establecido en el artículo 6 de la precitada Ley, cuando establece que el Poder Ejecutivo ejerce la función de "reglamentar leyes, evaluar su aplicación y supervisar su cumplimiento".

Asimismo, conforme a los incisos l) y r) del artículo 7 de la Ley N.º 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, son funciones específicas del Ministerio de Justicia y Derechos Humanos, estudiar y proponer la dación y reforma de la legislación, así como otras que se establezcan por ley.

Por su parte, la Ley N.º 29733, Ley de Protección de Datos Personales, publicada el 3 de julio de 2011, tiene por objeto garantizar el derecho a la protección de datos personales, previsto en el inciso 6 del artículo 2 de la Constitución Política del Perú. La mencionada norma legal, creó la Autoridad Nacional de Protección de Datos Personales como el órgano competente para realizar las acciones para el cumplimiento de la Ley N.º 29733 y su Reglamento aprobado por Decreto Supremo N.º 003-2013-JUS.

El 22 de marzo de 2013, mediante Decreto Supremo N.º 003-2013-JUS se publicó el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales, cuyo objeto fue desarrollar la Ley N.º 29733 a fin de garantizar el derecho fundamental a la protección de datos personales, regulando un adecuado tratamiento, tanto por las entidades públicas, como por las instituciones pertenecientes al sector privado.



E. LUNA C.



G. VALDIVIESO R.

Por Decreto Supremo N.º 013-2017-JUS, se aprobó el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, estableciendo que la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales es el órgano de línea del Despacho Viceministerial de Justicia del Ministerio de Justicia y Derechos Humanos que se encuentra a cargo de la Autoridad Nacional de Protección de Datos Personales.

Mediante Decreto Supremo N.º 019-2017-JUS se aprobó el Reglamento del Decreto Legislativo 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, el cual incorporó la nueva tipificación de infracciones a efectos de fortalecer la normativa de protección de datos personales.



E. REDAZA I.

Posteriormente, por Decreto Supremo N.º 004-2019-JUS, publicado el 25 de enero de 2019, se aprobó el Texto Único Ordenado de la Ley N.º 27444, Ley de Procedimiento Administrativo General, que incorporó modificaciones respecto a las actividades de fiscalización, los procedimientos administrativos sancionadores y procedimientos bilaterales de tutela, así como en lo referente a los plazos administrativos.

Mediante Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, se reguló, en el inciso 5.10 del artículo 5, como principio del Marco de Gobierno Digital, el nivel de protección adecuado de los datos personales estableciéndose que el tratamiento de datos personales debe realizarse conforme la Ley de Protección de Datos Personales y su Reglamento.

Asimismo, el inciso 18.8 del artículo 18 del Decreto Legislativo N.º 1412 dispone que las entidades de la administración pública deben garantizar que en el diseño y configuración de los servicios digitales se adopten medidas técnicas, organizativas y legales para la debida protección de los datos personales, además de que deben administrar los datos durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de protección de datos personales.

El Decreto Supremo N.º 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, especifica que el ciudadano digital tiene derecho fundamental a la protección de datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política.

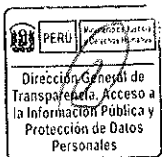
Como se aprecia, la normativa en materia de gobierno digital se encuentra acorde con la LPDP y sus disposiciones, reconociendo el derecho a la protección de datos personales, resultando compatible con la emisión del nuevo Reglamento de la LPDP.

Por otro lado, el Decreto de Urgencia N.º 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, tiene por objeto establecer las medidas para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones privadas en el territorio nacional. Dicha norma contempla como parte de su ámbito, la protección de datos personales y transparencia, la cual, es dirigida, supervisada y evaluada por la Autoridad Nacional de Protección de Datos Personales del Minjurdh.

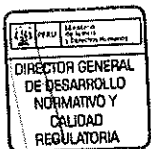
El Decreto de Urgencia N.º 007-2020 establece que el Centro Nacional de Seguridad Digital brinda información sobre los registros de los incidentes de seguridad digital a los responsables de los ámbitos del Marco de Seguridad Digital, de conformidad con el artículo 32 del Decreto Legislativo N.º 1412, y del Marco de Confianza Digital, debiendo observar para tal efecto la normatividad en materia de protección de datos personales.

Asimismo, el literal e) del inciso 9.1 del artículo 9 del Decreto de Urgencia N.º 007-2020 establece que las entidades de la administración pública y los proveedores de los servicios digitales deben reportar y colaborar con la autoridad de la protección de datos personales cuando se verifique un incidente de seguridad digital que involucre datos personales. En cuanto al uso ético de las tecnologías digitales, el inciso 12.3 del artículo 12, indica que el tratamiento de los datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

De este modo, en el ámbito de la confianza digital se establece diversas disposiciones que reconocen el ejercicio del derecho a la protección de los datos personales,



E. LUNA C.



G. VALDIVIESO P.



E. REDAZA I.

evidenciándose que dicha normativa resulta compatible con el objetivo y finalidad de la regulación plasmada en el presente Reglamento.

Finalmente, conviene tomar en cuenta que mediante Decreto Supremo N.º 164-2021-PCM, que aprueba la Política General de Gobierno para el período 2021-2026, se estableció en el Eje 8 denominado Gobierno y transformación digital con equidad, se incluye como línea de intervención 8.1.5 "*Consolidar las acciones de seguridad y confianza digital para la protección de la ciudadanía frente a los riesgos y amenazas en el entorno digital*", política a la que también se encuentra alineado el presente Reglamento que establece mecanismos para resguardar el principio de seguridad en el tratamiento de datos personales.

De este modo, el presente Reglamento se encuentra conforme con el inciso 6) del artículo 2 de la Constitución Política del Perú; la Ley N.º 29733, Ley de Protección de Datos Personales; la Ley N.º 29158, Ley Orgánica del Poder Ejecutivo; el Decreto de Urgencia N.º 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento; la Ley N.º 29809, Ley de Organización y Funciones del Ministerio de Justicia y Derechos Humanos; y, el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo N.º 013-2017-JUS.

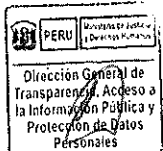
Asimismo, se encuentra alineado a la Política General de Gobierno, aprobada mediante Decreto Supremo N.º 164-2021-PCM, para el período 2021-2026 establece como Eje 8 al "Gobierno y transformación digital con equidad" y permita que el país cuente con un marco normativo más sólido y con un mayor nivel de protección de datos personales debido al aumento exponencial de la recopilación y transferencia de datos personales, así como del avance de las nuevas tecnologías.

Ámbito internacional

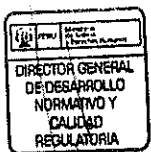
Si bien a la fecha no existen obligaciones provenientes de tratados internacionales ratificados por el Estado peruano, en materia de protección de datos personales, el Perú recurre a diversos documentos internacionales que sirven como fuente valiosa para el óptimo desarrollo de las funciones realizadas por la Autoridad Nacional de Protección de Datos Personales, la cual tiene competencia para dictar las normas, lineamientos, instrumentos y establece los procedimientos en materia de protección de datos personales, a través del cual se promueve un tratamiento adecuado de los datos de las personas y, en particular, en el Sistema Nacional de Transformación Digital y el uso de las tecnologías digitales en el entorno digital.

Así, por ejemplo, se toma como referente internacional, el Convenio N.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su reciente actualización Convenio N.º 108+, que reconoce el derecho a la protección de datos personales⁴⁸ como un derecho autónomo desarrollando su contenido y conceptos básicos para su aplicación.

Este instrumento consagra que todo tratamiento de los datos personales debe realizarse sobre la base del consentimiento libre, específico e informado. Asimismo, establece que los datos personales deben ser tratados de manera transparente y justa, que sean recopilados a un propósito específico y que no sean excesivos, y que puedan conservarse por un tiempo que no sea superior al propósito que se persigue.



E. LUNA C.



G. VALDIVIESO P.



E. REBAZA I.

⁴⁸ Aprobado el 28 de enero de 1981. Disponible en: <https://bit.ly/3rE93Ik>

En el 2021, se aprobó los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales de la Organización de Estados Americano (con anotaciones), como instrumento de *soft law* interamericano que tiene por objetivo servir como punto de referencia para el fortalecimiento de sus respectivos marcos jurídicos en la materia, y orientar el desarrollo colectivo de la región hacia una protección armónica y efectiva de los datos personales.⁴⁹

Por su parte, la Organización para la Cooperación y el Desarrollo Económico (OCDE) adoptó las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. Este instrumento da cuenta de los principios y contenidos básicos que deben recoger las normativas internas de los países para asegurar el respeto a la privacidad y la protección de los datos personales.⁵⁰

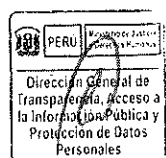
Así también, es pertinente considerar los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017⁵¹, que tiene por objeto establecer un marco común de principios y derechos de protección de datos personales que sirve como base para las diferentes legislaciones nacionales de los estados iberoamericanos de forma que se garantice una protección homogénea en la región y se facilite el flujo transfronterizo de los datos personales entre los países.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)⁵² en cuanto establece el tratamiento de personas fallecidas, elaboración de perfiles, evaluación de impacto, flujo transfronterizo, entre otros temas relevantes incluidos en el nuevo Reglamento.

En suma, a través del nuevo Reglamento se busca actualizar y optimizar la normativa reglamentaria en materia de protección de datos personales adoptando algunas de las figuras y mecanismos regulados en instrumentos internacionales que constituyen un referente relevante para fortalecer el régimen jurídico nacional.

Finalmente, en lo relacionado a la realización del Análisis de Impacto Regulatorio Ex Ante, cabe precisar que la Comisión Multisectorial de Calidad Regulatoria (CMCR) ha determinado que el nuevo Reglamento se encuentra comprendido en la excepción contemplada en el numeral 18 del artículo 28.1 del Decreto Supremo N.º 063-2021-PCM, Decreto Supremo que aprueba el Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis del Impacto Regulatorio Ex Ante.

Efectivamente, luego de realizar la evaluación del Anexo 7 "Formato de aplicación de excepción al AIR Ex Ante", la Comisión Multisectorial de Calidad Regulatoria determinó: *"la improcedencia del AIR Ex Ante del proyecto normativo, en virtud de la excepción establecida en el numeral 18 del inciso 28.1 del artículo 28 del Reglamento del AIR Ex Ante; por lo tanto, no requiere realizar el AIR Ex Ante por parte de la entidad"*.



E. LUNA C.



G. VALDIVIESO P.



H. REBAZA I.

⁴⁹ https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

⁵⁰ Directrices de la OCDE sobre la protección de la privacidad y flujos transfronterizos de datos personales, ver: <https://www.oecd.org/sti/ieconomy/15590267.pdf>

⁵¹ https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

⁵² <https://www.boe.es/doi/2016/119/L00001-00088.pdf>