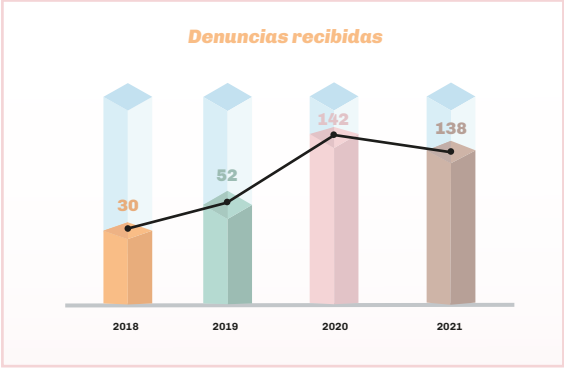
Payet Rey Cauvi Pérez

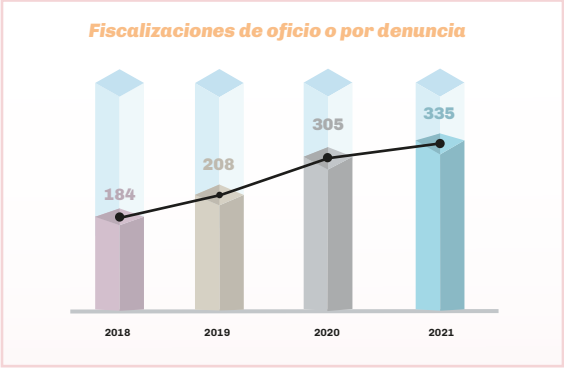
PRIVACIDAD & PROTECCIÓN DE DATOS

La Autoridad Nacional de Protección de Datos Personales ("ANPDP") viene fortaleciendo sus facultades como órgano encargado de velar por la protección de los datos personales, incrementando así su labor fiscalizadora y sancionadora, tal como se aprecia de las siguientes estadísticas:

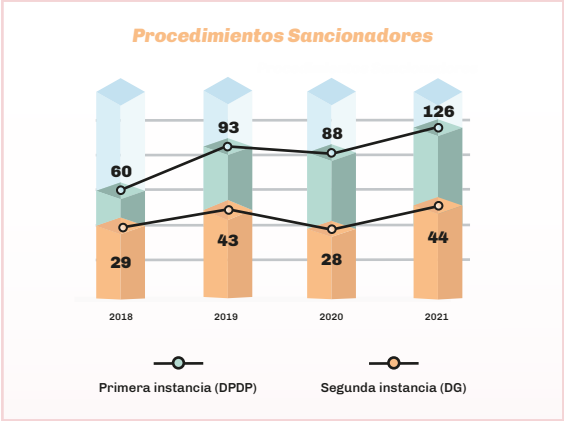
1. Entre los años 2020 y 2021, las denuncias por uso inadecuado de datos personales se han incrementado en un 240% a comparación de los dos años previos.



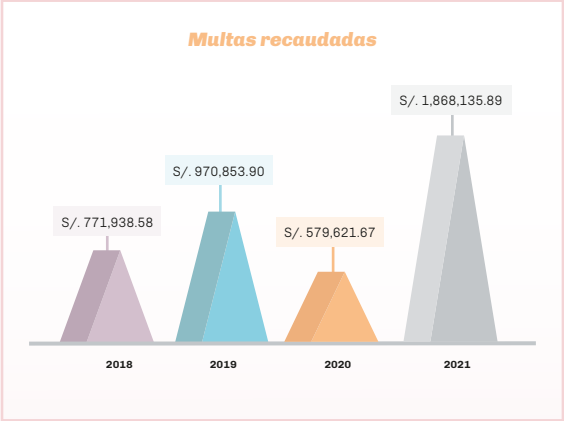
2. Las fiscalizaciones por parte de la ANPDP para verificar el cumplimiento de la normativa de datos personales, entre los años 2020 y 2021, se han incrementado en 60% a comparación de los dos años previos.



3. También se ha visto un incremento en los procedimientos administrativos sancionadores (PAS). En el año 2021, tanto la primera como la segunda instancia de la ANPDP han incrementado en un 40% y 50%, respectivamente, el número de PAS resueltos a comparación del año 2020.



4. Producto del incremento de la labor sancionadora de la ANPDP, en el año 2021 recaudó en multas **S/. 1'868,135.89**, equivalente a 220% más a comparación del año 2020.



En este boletín se resumen las principales opiniones y pronunciamientos emitidos durante el primer semestre del presente año en materia de datos personales. Asimismo, se reseñan las principales novedades legislativas y proyectos de ley. Finalmente, se detallan las novedades nacionales de la ANPDP e internacionales relacionadas con la materia ante señalada.

1. Principales opiniones emitidas por la Autoridad de Datos Personales

- **La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales ("DGTAIPD") precisó los alcances del primer contacto para fines publicitarios**

  Mediante Opinión Consultiva N° 1-2022-DGTAIPD, la DGTAIPD señaló que, si bien se puede establecer un primer contacto con el titular del dato para solicitar su consentimiento para el tratamiento de sus datos con fines publicitarios, dicho contacto solo puede ser realizado una única vez, independientemente del producto y/o servicio que requiera publicitar una misma persona jurídica.

  Asimismo, señaló que, en caso existan terceros contratados o subcontratados para el tratamiento de los datos personales, el anunciante seguirá siendo responsable por dicho tratamiento. Ello aun cuando el banco de datos sea de titularidad del tercero. Atendiendo a lo anterior, la DGTAIPD estableció que el anunciante y los encargados del tratamiento deben emplear medios de comunicación rápidos y eficientes para poner en conocimiento los casos de denegatoria de consentimiento de los titulares de los datos personales, con la finalidad de adoptar acciones para no volver a contactarlo nuevamente. **(Clic para ver Infografía)**.

- **La DGTAIPD precisó los alcances del artículo 18 de la Ley de Protección de Datos Personales ("LPDP")**

  Mediante Opinión Consultiva N° 2-2022-DGTAIPD, la DGTAIPD señaló -entre otros- que el último párrafo del artículo 18 prevé aquellos escenarios en los cuales se debe entregar información al titular del dato personal de forma posterior a la recopilación de sus datos y la obtención del consentimiento. En ese sentido, precisó que la expresión "*supuestos similares*" hace referencia a los supuestos en los cuales el destinatario de los datos (nuevo titular del banco de datos) asumirá la responsabilidad del tratamiento de los mismos debido a un cambio en la posición contractual como consecuencia de cualquier supuesto de reorganización societaria contemplado en la Ley N° 26887, Ley General de Sociedades (incluido escisiones de empresas); así como en operaciones que contemplen solo la transferencia de posición contractual (por ejemplo, casos de cesión de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial).

  Cabe señalar que previamente, mediante Opinión Consultiva N° 48-2018-JUS/DGTAIPD, la DGTAIPD señaló que el último párrafo del artículo 18 de la LDPD también incorpora una excepción al consentimiento en caso de transferencia de datos en el marco del proceso de una reorganización societaria. Por tanto, para interpretar los alcances del último párrafo del artículo 18 de la LPDP deberá leerse de manera conjunta las opiniones consultivas antes indicadas.

- **La DGTAIPD se pronuncia sobre el tratamiento de datos personales de trabajadores en el marco de contrataciones de servicio de planilla**

  Mediante Opinión Consultiva N° 3-2022-JUS/DGTAIPD, la DGTAIPD analizó el esquema en el cual (i) el Decreto Supremo N° 15-2010-TR, ha dispuesto que todos los empleadores están obligados a registrar a sus trabajadores en el T-REGISTRO, dentro del día en que estos ingresan a prestar sus servicios; y (ii) que para ello los empleadores pueden contratar a una persona natural o jurídica con la finalidad de que ésta realice las gestiones de registro y manejo en su nombre (la "prestadora del servicio de planilla").

  Al respecto, la DGTAIPD ha considerado que la empresa empleadora, al ser la que define los fines y medios del tratamiento, es la titular del banco de datos personales de sus trabajadores, con relación al registro de planillas. Dicha consideración se sostiene incluso en el supuesto en que los trabajadores accedan directamente al portal web de la prestadora del servicio de planilla para ingresar sus datos personales a fin de hacer efectiva la gestión de planillas. De esta manera, si la empresa empleadora decide contratar a una prestadora del servicio de planilla, ésta última asume la calidad de encargada del tratamiento de los datos personales, y con ello las obligaciones y responsabilidades que este cargo conlleva **(Clic para ver Client Memo)**.

- **La DGTAIPD estableció pautas sobre el tratamiento de datos personales para la prevención de delitos y cumplimientos regulatorios**

  Mediante Opinión Consultiva N° 6-2022-JUS/DGTAIPD, la DGTAIPD estableció las pautas que deben observar las personas jurídicas al tratar datos personales en el marco del sistema de prevención de los delitos de lavado de activos y financiamiento del terrorismo (SPLAFT) a efectos de cumplir con sus obligaciones de informar a la Unidad de Inteligencia Financiera (UIF-Perú), según lo previsto en la Ley N° 27693 y/o cuando tengan un modelo de prevención para determinar la responsabilidad penal de algún miembro, según lo previsto en la Ley N° 30424 **(Clic para ver Infografía)**.

- **La DGTAIPD explica los alcances del uso de sistemas de videovigilancia en caso de denuncias o sospechas razonables de hostigamiento sexual en instituciones educativas**

  Mediante Opinión Consultiva N° 7-2022-JUS/DGTAIPD, la DGTAIPD determinó que no sería necesario recabar el consentimiento para el uso de cámaras de videovigilancia en entornos escolares que tenga por finalidad la seguridad del alumno, sobre todo ante denuncias o sospechas razonables de acoso u hostigamiento sexual. Sin perjuicio de lo anterior, las instituciones educativas deben cumplir con todas las obligaciones previstas en la LPDP y su Reglamento, incluido el deber de informar sobre el tratamiento de imágenes y/o voces, además de observar los principios de proporcionalidad, finalidad, seguridad y calidad **(Clic para ver Infografía)**.

  Adicionalmente, para mayor información sobre los alcances de la LPDP en entornos escolares puede hacer clic **aquí**.

- **La DGTAIPD precisó los alcances del ejercicio de acceso de los titulares de datos personales respecto al tratamiento que se realice a través de sistemas de videovigilancia**

  Mediante Opinión Consultiva N° 8-2022-JUS/DGTAIPD, la DGTAIPD precisó los alcances del ejercicio del derecho de acceso por parte de los titulares de los datos personales en el marco del uso de sistemas de videovigilancia. De esta forma, se señaló que no sería necesario requerir una fotografía del titular del dato para atender una solicitud de acceso siempre y cuando este pueda ser identificado con la copia de su DNI; salvo los casos en los que la copia del DNI no permita su identificación (por ejemplo, foto desactualizada), en cuyo escenario se podrá exigir adicionalmente una imagen actual.

  Adicionalmente, la DGTAIPD señaló que las grabaciones serán entregadas al solicitante en un CD en blanco o por otros medios análogos seguros como ejemplo el almacenamiento temporal en la nube con un enlace de descarga. **(Clic para ver Infografía)**.

2. Principales resoluciones emitidas por la Autoridad de Datos Personales

- **La Dirección de Protección de Datos Personales ("DPDP") reiteró que se debe solicitar de forma independiente el consentimiento del titular para el tratamiento de datos personales con fines publicitarios**

  Mediante Resolución Directoral N° 3641-2021-JUS/DGTAIPD-DPDP, la DPDP mantiene el criterio de que está prohibido solicitar el "*consentimiento en bloque*"; es decir, solicitar un único consentimiento para finalidades principales y adicionales (por ejemplo, envío de publicidad, estudio de mercadotecnia, entre otros). Por ello, la DPDP precisa que se deben implementar casillas independientes para que el titular del dato personal brinde su consentimiento por cada finalidad adicional que se requiera.

  La DPDP reitera que la prohibición del "*consentimiento en bloque*" es inducir a error a los titulares de datos personales a fórmulas ambiguas o amplias que permitan captar datos para finalidades de prospección comercial propia o de terceros, inclusive, sin autorización expresa e inequívoca para ello.

- **La DGTAIPD precisó que el tope máximo para el cálculo de la multa se establece por el total de multas y no por cada sanción impuesta**

  Mediante Resolución Directoral N° 11-2022-JUS/DGTAIPD, la DGTAIPD aclaró que el tope del diez por ciento (10%) de los ingresos brutos anuales establecido como tope máximo para imponer sanciones a los administrados se aplica a la sumatoria de la totalidad de multas dictadas contra un administrado y no respecto de cada una de las multas impuestas por cada infracción cometida.

- **La DPDP desarrolló el concepto de responsabilidad proactiva y el concepto de dato biométrico como dato sensible**

  Mediante Resolución Directoral N° 655-2022-JUS/DGTAIPD-DPDP, la DPDP indicó que la responsabilidad proactiva de parte de quienes realicen tratamiento de datos personales implica establecer medidas de prevención que garanticen el cumplimiento de las obligaciones normativas (*privacy by design*) y medidas de limitación de la accesibilidad a los datos personales, evitando el acceso de personas o de quienes no requieren conocer los datos personales para cumplir con sus funciones; además de aplicar tal limitación según el criterio de minimización del tratamiento (*privacy by default*).

  Respecto al concepto de dato biométrico, la DPDP trajo a colación la definición del Reglamento General de Protección de Datos de Europa para determinar las razones por las cuales se considera a este tipo de dato como sensible. Así, se indicó que los datos biométricos son aquellos obtenidos a partir de un tratamiento técnico, relativo a características físicas, fisiológicas o conductuales, que permiten o confirman la identidad de una única persona. Asimismo, la DPDP señaló que las razones para considerar a los datos biométricos como datos sensibles, son que (i) permiten identificar de manera unívoca a la persona y (ii) su tratamiento es por medio de un procedimiento técnico específico.

- **La DPDP se pronunció sobre la recopilación de antecedentes penales, policiales, judiciales y denuncias ante el Ministerio Público**

  Mediante Resolución Directoral N° 1022-2022-JUS/DGTAIPD-DPDP, la DPDP señaló que el tratamiento de antecedentes penales, policiales, judiciales o denuncias ante el Ministerio Público proporcionados por entidades privadas sin competencia para ello sería ilícito y desleal, calificando dicha conducta como una infracción muy grave.

  Al respecto, la DPDP precisó que el acceso a los antecedentes penales, policiales, judiciales o denuncias ante el Ministerio Público solo es legítimo cuando se acude directamente al Poder Judicial o al Ministerio Público, ya sea de forma personal o cuando otra entidad competente lo requiera. Dicha licitud, no alcanza a terceras empresas privadas que no ostenten competencias legales para ello. Por tanto, la obtención de dicha información a través de una plataforma virtual provista por un tercero sin competencia es ilegítima **(Clic para ver Client Memo)** **(Click para ver Infografía)**.

3. Novedades Legislativas

- El 20 de abril de 2022 se publicó en el Diario Oficial El Peruano la Resolución Ministerial N°125-2022-PCM, mediante la cual se creó la "Mesa Técnica para proponer acciones y medidas para fortalecer la confianza digital", la cual tiene por objeto prevenir y reducir los ciberataques, el robo de teléfonos móviles, el uso indebido de medios digitales, el contacto no consentido mediante llamadas a fin de fortalecer la confianza digital.

  Inicialmente dicho grupo de trabajo tenía una vigencia de treinta (30) días hábiles contados desde el día siguiente a su instalación, la Resolución Ministerial N° 180-2022-PCM del 8 de junio de 2022 prorrogó dicho plazo a sesenta (60) días hábiles.

4. Proyectos de Ley

Proyectos de Ley 1161/2021-CR y 1162/2021-CR

Estos proyectos normativos tienen por finalidad realizar una reforma constitucional para permitir el levantamiento del secreto bancario y la reserva tributaria a solicitud del Juez, del Fiscal de la Nación, de comisiones investigadoras del Congreso, del Contralor General de la República respecto de funcionarios y servidores públicos, y del Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

Proyecto de Ley 776/2021-CR

El proyecto normativo en referencia tiene por finalidad establecer medidas de carácter excepcional que garanticen la seguridad en el ciberespacio frente a las amenazas o los ataques que afecten la seguridad nacional, y para la ejecución de operaciones de ciberseguridad y seguridad Digital, a través de la creación del Centro Nacional de Ciberseguridad del Perú – CENACI.

5. Novedades de la Autoridad de Datos Personales

- La ANPDP, por medio de la Dirección de Fiscalización e Instrucción (la "DFI"), ha iniciado acciones de fiscalización frente a una presunta filtración de datos mediante la plataforma de un organismo autónomo ocurrida el pasado 13 de mayo de 2022.

- A partir de hallazgos y sanciones previas, la ANPDP viene fiscalizando, por medio de la DFI, a personas jurídicas que emplean a terceros para recopilar información de sus postulantes vinculada a antecedentes penales, policiales, judiciales y denuncias ante el Ministerio Público, en tanto dicha información vendría de fuentes ilícitas. Asimismo, estaría fiscalizando la implementación de políticas de atención al ejercicio de derechos ARCO.

- Pese a no existir una guía de cookies, la ANPDP realizó una serie de fiscalizaciones vinculadas a esta materia que habrían determinado el inicio de varios procedimientos sancionadores. Estos procedimientos serían resueltos en los próximos meses y se espera que desarrollen mayores lineamientos sobre el tratamiento de datos a través de cookies, brindando mayor predictibilidad a los administrados.

6. Novedades Internacionales en Protección de Datos Personales

- El 24 de abril de 2022, la Unidad Regulatoria y de Control de Datos Personales de Uruguay declaró que había emitido, el 21 de diciembre de 2021, la Resolución N° 58/021 sobre los criterios para el tratamiento de datos personales durante la utilización de sistemas de videovigilancia. En particular, la resolución destaca el uso de los sistemas de videovigilancia en diferentes entornos.

- En mayo de 2022, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México publicó las "*Recomendaciones para el tratamiento de datos personales derivados del uso de la inteligencia artificial*" con la finalidad de que se efectúe un uso adecuado de la información personal y se garantice su privacidad mediante las tecnologías que emplean inteligencia artificial (IA).

  Entre sus recomendaciones se encuentran establecer plazos de conservación de los datos personales en el sistema de IA; monitorear y revisar de manera periódica las medidas de seguridad para la protección de los datos personales que son tratados por el producto o servicio de IA; implementar

medidas para la protección de los derechos, libertades e intereses legítimos de la persona titular de los datos personales cuando la IA desarrolla o utiliza, realiza decisiones automatizadas; entre otras.

- En Colombia, mediante Decreto 255 de 2022, el Ministerio de Comercio, Industria y Turismo reguló la implementación de Normas Corporativas Vinculantes ("NCV") para la certificación de buenas prácticas en protección de datos personales y su transferencia internacional entre empresas de un mismo grupo empresarial. Las NCV son un mecanismo de autorregulación voluntaria que constituye una alternativa adicional a la normativa colombiana y que tiene como finalidad facilitar la transferencia de datos personales entre responsables de un mismo grupo empresarial ubicados en diferentes países.

- El 9 de junio de 2022, la Agencia Española de Protección de Datos ("AEPD") publicó la Resolución del procedimiento N° PS/00591/2021, por medio de la cual se multa a un administrado, persona natural, por tener una cámara tipo cúpula mal orientada, que supuestamente afectaba los derechos del denunciante. Al respecto, la AEPD destacó que, las cámaras deben estar orientadas hacia el espacio concreto, evitando intimidar a los vecinos colindantes con este tipo de dispositivos, así como vigilar zonas de tránsito sin causa justificada.

Carlos Patrón
Socio
cap@prcp.com.pe

Giancarlo Baella
Asociado Principal
gbp@prcp.com.pe

Jimena Pérez
Asociada
jpd@prcp.com.pe

Ana Lucía Figueroa
Asociada
afd@prcp.com.pe

Luciana Márquez
Asociada
lma@prcp.com.pe