Preguntas y respuestas varias sobre la protección de datos personales en el Perú

Eduardo Javier Luna Cervantes

Abogado por la Universidad de Lima.
Máster en Derecho Constitucional por la Pontificia Universidad Católica del Perú.
Diplomado en Derecho Constitucional por el Centro de Estudios Políticos y Constitucionales de Madrid.
Profesor de Derecho Constitucional de la Universidad de Lima.
Director General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos del Perú.
Ex Jefe del Programa de Ética Pública y Prevención de la Corrupción en la Defensoría del Pueblo del Perú.

El presente artículo fue recibido por el Comité Editorial con fecha 20 de enero de 2020.

SUMARIO:

RESUMEN:

Este pretende ser un artículo informativo. Si se quiere, una aproximación a la cuestión de la protección de datos personales en el Perú, a finales de esta década que concluye. Lo ofrezco a partir de una libre asociación de ideas que concateno a modo de preguntas y respuestas, las cuales fluyen, si no de la experiencia de la función pública que desempeño en la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, sí, de seguro, de la reflexión académica que mi quehacer profesional suscita. Un telón que abre un escenario desde el cual siempre es más cómodo escribir y autoidentificarse.

Palabras clave: protección de datos, Autoridad Nacional de Protección de Datos Personales, Ley de Protección de Datos Personales, procedimiento trilateral de tutela, procedimientos sancionadores.

ABSTRACT:

This is intended to be an informative article. If desired, an approach to the issue of personal data protection in Peru, at the end of this decade that is concluding. I offer this from a free association of ideas that I connected as questions and answers, which came, if not, from my professional experience in the public function that I perform in the National Authority of Personal Data Protection of the Ministry of Justice and Human Rights; for sure, from the academic reflection that comes from my professional expertise. A curtain that opens a stage from which it is always more comfortable to write and self-identify.

Keywords: data protection, National Authority of Personal Data Protection, Law of Personal Data Protection, trilateral guardianship proceeding, sanctioning procedures.

I. ¿DÓNDE ESTAMOS?

La protección de los datos personales en el Perú no es reciente, si nos referimos a la normativa y a la institucionalidad que ella ha generado. La Ley de Protección de Datos Personales, Ley 29733 —en adelante, "LPDP"—, data del año 2011, aunque entrara en vigencia plena recién el 2013.[1] Fue modificada significativamente en el 2017 con el Decreto Legislativo 1353. La Autoridad Nacional de Protección de Datos Personales —en adelante, "ANPD"— entró en operaciones ese mismo año.

Sin embargo, lo que creo que sí es reciente en el país es la conciencia social y de las corporaciones públicas y privadas de lo que implica la protección de datos personales. Y esto se ha generado por una suma de factores: la marcada universalización de la legislación de protección de datos personales en las democracias modernas, donde la aprobación y vigencia del Reglamento Europeo de Protección de Datos Personales, es el hito más notorio y significativo en los últimos años[2]; la consecuente incorporación en las organizaciones de buenas prácticas o *benchmarking* en esta materia, exigencia de casas matrices que operan a nivel mundial y hacen del seguimiento de ellas estándares de excelencia; la conciencia por el valor económico de los datos personales, que hoy en día sustentan exitosos modelos de negocio[3]; los riesgos

1. Conforme a la Duodécima Disposición Complementaria Final de la LPDP, su vigencia plena se dio a los 30 días hábiles de publicado el reglamento, el mismo que se publicó el 22 de marzo de 2013, a través del Decreto Supremo Nº 003-2013-JUS que lo aprobó.

2. Vigente desde el 25 de mayo de 2018, establece normas de protección de datos para Europa. Se aplica a todas las empresas que tratan datos personales sobre personas en la Unión Europea, independientemente de dónde tienen su sede.

3. Sobre ello, es ilustrativa la nota *"El valor de los datos personales: entre 4 y 18 euros al mes, o más"* de Economía Digital.

   «El valor de los datos personales: entre 4 y 18 euros al mes, o más», Economía Digital, acceso el 16 de enero de 2020, https://www.economiadigital.es/tecnologia-y-tendencias/el-valor-de-los-datos-personales-entre-4-y-18-euros-al-mes-o-mas_633605_102.html.

generados a la seguridad e integridad de las personas —especialmente de niños y adolescentes—, como consecuencia de la interacción descuidada en las redes sociales; el daño a la imagen corporativa producida por brechas de seguridad que exponen y filtran datos de ciudadanos y clientes[4]; y, por qué no escribirlo, la creciente fiscalización que vienen realizando agencias de protección de datos en el mundo entero, incluida la peruana.[5]

II. ¿QUÉ SE PROTEGE?

Se protege derechos. Y es importante destacarlo desde el inicio. Desde la norma y la institución que ella genera —la ANPD— se pretende proteger, defender, garantizar y promover los denominados derechos de protección de datos personales o, como se les conoce también en doctrina, el derecho a la autodeterminación informativa. Así, toda fiscalización realizada, procedimiento incoado, sanción administrativa aplicada, charla informativa brindada, campaña de sensibilización ejecutada, medida de seguridad o inscripción de bancos de datos personales exigida, desde la ANPD, tiene como propósito la defensa del derecho fundamental reconocido en el artículo 2, inciso 6, de la Constitución Política[6], cuyo contenido se configura también por el artículo 61 del Código Procesal Constitucional, Ley 28237[7] y, por supuesto, por los derechos reconocidos en la propia norma sustantiva, la citada LPDP[8].

Esta perspectiva es fundamental, si se aborda la cuestión desde lo público. Aquí, no se trata de superar una barrera burocrática más, de cumplir con el ritualismo administrativo necesario para echar a andar un negocio, de sortear de la mejor forma posible la acción del Estado cuando este ejerce su *ius puniendi*, o de implementar en la organización propia una serie de medidas "de moda" para obtener un *International Organization for Standarization*-ISO de eficiencia y ganar prestigio corporativo. No; o al menos no es sólo eso, ni mucho menos. Se trata de garan-

4. Hay una vinculación directa entre vulnerabilidad en la seguridad de la información y el valor en el mercado de la corporación que la padece.

   «Alerta por ciberataque a gigante de aluminio», El Sol de México, acceso el 16 de enero de 2020, https://www.elsoldemexico.com.mx/mundo/alerta-por-ciberataque-a-gigante-de-aluminio-3207817.html.

5. Sólo en el año 2019, la ANPD realizó 304 visitas de fiscalización a 209 entidades. Se iniciaron en el mismo periodo 126 procedimientos administrativos sancionadores por infracciones a la LPDP. A decir de la información de la Autoridad —Informe Nº 01-2020-JUS/DGTAIPD—, se aprecia un incremento del 10%, en promedio, de las acciones realizadas respecto del año 2018. La tendencia es creciente año a año.

6. *"Artículo 2.- Toda persona tiene derecho:*
   (…)
   6) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar."

7. *"Artículo 61.- Derechos protegidos*
   El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para:
   (…)
   2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales."

8. Los derechos del titular de datos personales están reconocidos en el Título III de la LPDP. Específicamente, en los artículos 18 —derecho de información—, 19 —derecho de acceso—, 20 —derecho de actualización, inclusión, rectificación y supresión—, 21 —derecho a impedir el suministro—, 22 —derecho de oposición—, 22 —derecho al tratamiento objetivo—, 23 —derecho a la tutela— y 24 —derecho a ser indemnizado—.

tizar y proteger derechos. Y toda acción u omisión pública y privada en esta materia se juzga bajo esta lógica.

¿Y qué es lo que en específico se procura garantizar y proteger? Que cuando un actor público o privado se ocupe de nuestros datos personales —realice un tratamiento de ellos, si usamos el argot normativo— lo haga respetando una serie de principios y reglas. Simplificando el lenguaje, señalaríamos: (a) si va a exponerlos, lo haga con fidelidad, sin distorsionar las situaciones que los vinculan a ciertos hechos, y hasta donde sea lícito y razonable hacerlo; (b) si va a usarlos, que lo haga con mi consentimiento, de manera proporcional y para la finalidad declarada y conocida por mí; (c) si va a transferirlos, que me haga conocer a dónde y a quiénes; (d) si va a almacenarlos y procesarlos, que lo haga con seguridad y siempre informándome de ello y a la autoridad competente; y, (e) si va a hacer cualquiera de las acciones anteriores —y muchas más que el lenguaje simplificado no permite listar—, inobservando las prescripciones legales previstas y, por ende, mis derechos, pueda yo acudir a una autoridad competente para que se encargue del asunto y enmiende la situación.

Luego de estas nociones preliminares, ya cobra más sentido invocar el concepto de dato personal y de dato sensible. De acuerdo con el artículo 2, numeral 4, de la LPDP, se entiende por datos personales a toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados. Por su parte, los datos sensibles —artículo 2, numeral 5—, son aquellos datos personales 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.

Es la posibilidad de tener dominio sobre mis datos personales, incluidos los datos sensibles, lo que me confiere, como persona, la autodeterminación informativa.[9] Una autodeterminación que, en esta era digital y de la información, con una comunidad global que interactúa continuamente, casi resulta una quimera; considerando también los límites materiales y excepciones a este derecho, muchas veces representados por otras libertades o bienes jurídicos igualmente fundamentales para nosotros.

9. A este respecto es pertinente la distinción que hace el Tribunal Constitucional del derecho a la autodeterminación informativa con otros derechos relacionados; así, entiende que: *"El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen. Tampoco el derecho a la autodeterminación informativa debe confundirse con el derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución, que protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad. Finalmente, también se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad. En ese sentido, por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, prima facie y de modo general, un derecho de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales."*

(Continúa en siguiente página)

Una representación de ellos, los tenemos en la propia LPDP, específicamente en sus artículos 3 y 14. En efecto, de acuerdo con la LPDP, sus disposiciones no son de aplicación para los datos personales: (a) contenidos o destinados a ser contenidos en bancos de datos personales[10] creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar. Tampoco, a (b) los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito. Ello excluye, de entrada, del ámbito de aplicación de la LPDP a bases o bancos de datos generados para fines domésticos y privados, como lo puede ser una agenda con datos —imágenes, teléfonos, direcciones, etc.— de familiares, amigos o contactos, por ejemplo; al igual que excluye a los bancos de datos de personas que tienen agencias públicas como el Ministerio del Interior o la Policía Nacional, que registran antecedentes policiales de personas, por ejemplo; o bases de datos del Ministerio Público y de fiscalías especializadas, donde los bancos de datos personales de colaboradores eficaces o de personas comprendidas en determinadas investigaciones, pueden ser ejemplos paradigmáticos.

Asimismo, en este listado de excepciones y libertades contrapuestas, tenemos también los tratamientos de datos personales que pudieran hacerse (a) desde el ejercicio válido del derecho fundamental a la libertad de información, pensemos en el archivo periodístico de personas de interés público de un medio de comunicación; (b) el que se hace para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal; nuevamente, invocamos el ejemplo de registros de fiscalías especializadas; (c) el tratamiento efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros; (d) cuando se trate datos personales relativos a la solvencia patrimonial y de crédito; pensemos en la actividad de centrales de riesgo crediticio, regulada en la Ley 27489; o (e) en la recopilación o transferencia para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias; entre otras previs-

—el subrayado es nuestro—. *Cfr.*: Sentencia del Expediente Nº 1797-2002-HD/TC, fundamento jurídico 3. Asimismo, ha señalado: *"la protección del derecho a la autodeterminación informativa a través del hábeas data comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información, así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados."* —el subrayado es nuestro—. Ver misma Sentencia, fundamento jurídico 4. En similares términos lo hizo antes, la Sentencia del Expediente Nº 0666-1996-HD/TC, fundamento jurídico 2, y después, la Sentencia del Expediente Nº 1515-2009-PHD/TC, fundamento jurídico 5.

10. Un banco de datos personales es, a decir del artículo 2, numeral 1, de la LPDP, un conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

tas en el artículo 14 de la LPDP[11]. En todos estos casos, no se requiere contar con el consentimiento del titular de los datos personales que se tratan; por lo que deben entenderse como tratamientos legitimados con prescindencia de la voluntad de las personas con cuyos datos se opera.

III. ¿CÓMO SE PROTEGE?

Desde lo público se protegen estos derechos a través de la acción de la ANPD. Y específicamente a través de los procedimientos administrativos que tiene a su cargo, en razón de la LPDP.

Así, ante un tratamiento de datos personales que garantice que quien los exponga, lo haga con fidelidad, sin distorsionar las situaciones que los vinculan a ciertos hechos, y hasta donde sea lícito y razonable hacerlo, tenemos el llamado procedimiento trilateral de tutela, regulado en el artículo 24 de la LPDP y, por referencia directa, en la Ley 27444, Ley del Procedimiento Administrativo General, artículo 229 y siguientes.

A través de él, los administrados reclaman el respeto a los derechos de acceso, rectificación, cancelación y oposición —ARCO— a un tratamiento indebido de sus datos. Lo que se traduce en reclamaciones contra generadores de contenido, *webmasters*, buscadores, entre otros, luego de no conseguir que cese el tratamiento reclamado por la vía directa y previa al inicio del procedimiento administrativo.

Como todo procedimiento trilateral, este se sigue entre dos o más administrados ante la ANPD. La reclamación más usual suele ser aquella cuyo petitorio contiene la pretensión de que se elimine determinada noticia en la red que perjudica la imagen, buena reputación, vida privada, u otro, del reclamante. Lo que casi siempre termina reconduciéndose a un caso donde lo que se consigue, es que cese el tratamiento que "hipervisibiliza" su nombre al estar asociado a aquel enlace web —noticia— que lo perjudica, o que se rectifique la información que aquel propaga por estar desactualizada o porque el curso de los acontecimientos que sucedieron demostró que la misma no se ajustaba a la verdad.

Los casos que prosperan, sin ser exhaustivos en el relato, son aquellos donde quien reclama no es un personaje público o de interés para el público; objetivamente, la noticia tiene una carga o connotación negativa para los intereses del reclamante, puesto que suelen retratar algún pasaje penoso de su vida, marcado por algún padecimiento físico o mental que quedó registrado en la *web* por diversas circunstancias

11. Aquí también debemos incluir tratamientos: (a) de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público; (b) necesarios para la promoción de la competencia en los mercados regulados en la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos; (c) necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte; (d) cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento; (e) cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, o cuando medien razones de interés público previstas por ley, o cuando deban tratarse por razones de salud pública, o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados; (f) cuando se hubiera aplicado un procedimiento de anonimización o disociación, que impide la identificación del titular de datos; (g) cuando sean necesarios para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales —el primero es quien determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad, y el segundo, el que se encarga de un tratamiento en virtud de una relación jurídica que le vincula con el primero y delimita el ámbito de su actuación, respectivamente—; (h) cuando grupos económicos conformados por empresas que son consideradas sujetos obligados a informar a la Unidad de Inteligencia Financiera, comparten información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio; (i) distintos que deriven del ejercicio de competencias expresamente establecidas por ley.

—su vinculación filial o amical con algún personaje que tuvo interés público, pero que ya no, por ejemplo[12]—; su involucramiento involuntario y/o fortuito con un personaje que adquirió mala reputación o se vio envuelto en un caso judicial o policial de notoriedad pública —donde luego se demostraría su no vinculación con los hechos delictivos o con el personaje mal reputado[13]—; o, por tratarse de una situación embarazosa que marcó hace muchos años su biografía y que en la actualidad, sin ser un personaje de interés público, le impide una resocialización plena en su entorno; o, simplemente, porque se trata de una información que lo asocia a una persona con la cual ya no se tiene ningún vínculo y no se desea que la web perpetúe ese enlace del pasado que ya cumplió su finalidad, le desagrada y perturba su actual vida —un edicto matrimonial[14], por ejemplo—. Los casos son muchos y variados.

El riesgo latente en este tipo de procedimientos trilaterales es cruzar el umbral de lo que puede considerarse una afectación ilegítima a la libertad de información o expresión. Por eso es que la ANPD tiene el máximo cuidado en este tipo de procedimientos y ensaya con habitualidad resoluciones razonablemente deferentes hacia los reclamados cuando de contenidos noticiosos se trata.[15]

El otro tipo de procedimientos administrativos a cargo de la ANPD son los procedimientos sancionadores. A través de ellos, de la sanción impuesta por infracciones a la LPDP, se busca proteger los derechos sobre los datos personales desincentivando tratamientos proscritos por ley. Los derechos que antes enunciamos en términos sencillos: (a) si el agente —público o privado— va a usarlos, que lo haga con mi consentimiento, de manera proporcional y para la finalidad declarada y conocida por mí; (b) si va transferirlos, que me haga conocer a dónde y a quiénes; (c) si va a almacenarlos y procesarlos, que lo haga con seguridad y siempre informándome de ello y a la autoridad competente.

¿Cómo se traduce esto? Respeto a los principios de finalidad, proporcionalidad y consentimiento de la LPDP.[16] Si voy a requerir servicio de hos-

12. *Cfr.*: Resolución Directoral N° 84-2019-JUS/DGTAIPD.

13. *Cfr.*: Resolución Directoral N° 453-2018-JUS/DGTAIPD-DPDP. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2019/03/EXP-46-2017-RD-453-2018-DPDP.pdf.

14. *Cfr.*: Resolución Directoral N° 24-2019-JUS/DGTAIPD. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2019/09/EXP-48-2017-RD-24-2019-DGTAIPD.pdf.

15. *Cfr.*: Resolución Directoral N° 453-2018-JUS/DGTAIPD-DPDP. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2019/03/EXP-46-2017-RD-453-2018-DPDP.pdf.

16. *"Artículo 5. Principio de consentimiento*
Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

Artículo 6. Principio de finalidad
Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Artículo 7. Principio de proporcionalidad
Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados."

Y hay, por supuesto, otros principios de relevancia no ejemplificados aquí. Es el caso del principio de legalidad —artículo 4—, del principio de calidad —artículo 8—, principio de seguridad —artículo 9— —que más adelante

(Continúa en siguiente página)

pedaje en un hotel, este sólo debe requerirme aquellos datos personales que sean necesarios para brindarme dicho servicio[17]; si voy a matricularme en un centro de estudios, este sólo debe requerirme los datos necesarios a efectos de prestarme el servicio educativo ofrecido.[18] Si voy a postular a un trabajo, esta entidad sólo debe requerirme aquellos datos personales que sean necesarios por estar relacionados con el perfil requerido para dicho puesto.[19] Si voy a recabar y suministrar datos personales para determinar el riesgo crediticio de una persona, sólo debo recabar aquellos datos que resulten adecuados y proporcionales para dicha finalidad.[20] ¿Y si en todos estos casos decido igualmente recabar los datos personales no necesarios o justificados? Puedo hacerlo, por supuesto, siempre que recabe el consentimiento previo, informado, expreso e inequívoco del titular de los datos personales. Y si se trata de datos sensibles, ese consentimiento debe recabarse bajo una forma determinada y adicional, por escrito.[21]

También se traduce en seguir las prescripciones contenidas en el artículo 18 de la LPDP. Esto significa que el titular de los datos personales, de manera previa a la recopilación de sus datos, sea informado sobre la finalidad del tratamiento que recibirán. Quiénes son o pueden ser sus destinatarios; si existe o no un banco de datos personales en el que serán almacenados[22], así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de datos personales[23].

---

abordaré—, principio de disposición de recurso —artículo 10— y principio de nivel de protección adecuado —artículo 11—. Además, a decir del artículo 12 de la LPDP, la relación de principios es meramente enunciativa, por lo que se entiende que el catálogo de los mismos está abierto a otros que pudieran confluir necesariamente a este bloque normativo dedicado a la protección de los datos personales.

17. Por lo que datos como la procedencia, profesión o el estado civil, por ejemplo, no resultarían pertinentes e indispensables para contratar un servicio de hospedaje, como se determinó en el caso resuelto en la Resolución Directoral N° 62-2019-JUS/DGTAIPD de fecha 16 de setiembre de 2019.

18. No lo fueron, claramente, los antecedentes policiales en el caso de la Resolución Directoral N° 32-2018-JUS/DGTAIPD. Disponible en: https://pronabi.minjus.gob.pe/wp-content/uploads/2019/06/RD-32-2018.pdf.

19. No lo era, claramente, el dato acerca de los resultados de exámenes médicos practicados al postulante a un puesto de Ejecutivo de Producto, para determinar si padecía o no enfermedades de inmunodeficiencia, como ocurrió en el caso de la Resolución Directoral N° 04-2018-JUS-DGTAIPD. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2018/07/ITM-118-RD-04-2018-JUS-DGTAIPD-15-02-18-DOMIRUTH-TRAVEL-SERVICE-SAC-APELACION.pdf.

20. Lo que no ocurría con la imagen fotografiada ni la fecha de nacimiento de la persona, en el caso de la Resolución Directoral N° 26-2019-JUS/DGTAIPD. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2019/06/RD-26-2019-1.pdf.

21. Confróntese el artículo 13 de la LPDP.

22. Que, además, debiera inscribirse en el Registro Nacional de Bancos de Datos Personales; conforme a lo dispuesto en el artículo 34 de la LPDP, junto con las comunicaciones de flujos transfronterizos de datos —transferencias internacionales de datos personales—, las sanciones, medidas cautelares o correctivas impuestas por la ANPD. Este Registro público y gratuito le permite a cualquier persona, además, conocer la existencia de bancos de datos personales —no su contenido—, sus finalidades, así como la identidad y domicilio de sus titulares y, de ser el caso, de sus encargados. Disponible en: https://www.minjus.gob.pe/registro-proteccion-datos-personales/.

23. *"Artículo 2. Definiciones*
Para todos los efectos de la presente Ley, se entiende por:
(…).
8. Encargo de tratamiento. Entrega por parte del titular del banco de datos personales a un encargado de tratamiento de datos personales en virtud de una relación jurídica que los vincula. Dicha relación jurídica delimita el ámbito de actuación del encargado de tratamiento de los datos personales."

Este derecho-deber de informar que contiene el citado artículo 18[24], también exige que el titular de los datos personales conozca el carácter obligatorio o facultativo —de cara a la prestación del servicio o adquisición del bien deseado— que se le da a la absolución de preguntas formuladas con el propósito de recabar sus datos; es decir, las consecuencias. ¿Es obligatorio o no proporcionar el dato de mi estado civil o el número de hijos que tengo y sus edades, en la ficha de inscripción de un gimnasio para poder contratar con él el uso de sus instalaciones y máquinas para ejercicio físico?[25] ¿Es necesario que el postulante a un puesto de trabajo en una entidad prestadora de salud proporcione el dato de su religión —y si se bautizó—?[26]

Y, por último, el artículo 18 determina que se le informe al titular de datos personales si habrá o no transferencia de sus datos a terceros —nacionales o extranjeros—; cuánto tiempo se conservarán, y las vías —dirección, correo electrónico, teléfono, etc.— que tiene a su disposición para ejercer directamente ante quien los trata, sus derechos.

Finalmente, tenemos el rubro seguridad de la información —de los datos personales recabados, almacenados y procesados—. Los procedimientos sancionadores también pueden incoarse por infracciones a la LPDP y su reglamento, determinadas para esta materia. Y es que los titulares de los bancos de datos personales y los encargados de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales.[27] Estas medidas deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar[28] y con la categoría de datos personales de que se trate —si son sensibles, por ejemplo—.

Específicamente, nos estamos refiriendo a documentos de control de acceso a la información de datos personales, incluyendo la gestión de accesos desde el registro de un usuario; de gestión de los privilegios de dicho usuario; la identificación del mismo ante el sistema[29]; procedimientos documentados que definan la verificación periódica de los privilegios asignados. También, es fundamental generar y mantener registros que provean evidencia sobre las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema,

24. Para un conocimiento más exhaustivo y esclarecedor de las obligaciones derivadas de este artículo 18 de la LPDP, puede consultarse la Guía práctica para la observancia del "Deber de Informar", elaborada por la ANPD. Disponible en: https://www.gob.pe/institucion/minjus/informes-publicaciones/353793-guia-practica-para-la-observancia-del-deber-de-informar. También, la Resolución Directoral N° 43-2018-JUS/DGTAIPD que aprueba el modelo de cláusula informativa sobre las circunstancias y condiciones del tratamiento de datos personales requeridas por el artículo 18 de la LPDP. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2018/07/ANEXO-I_Condiciones-de-Tratamiento-de-Datos-Personales.pdf.

25. Cuestión que se trató en la Resolución Directoral N° 10-2018-JUS/DGTAIPD. Disponible en: https://pronabi.minjus.gob.pe/wp-content/uploads/2019/06/RD-10-2018.pdf.

26. *Cfr.*: Resolución Directoral N° 65-2016-JUS/DGPDP. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2017/02/RD-65.pdf.

27. Artículos 9 y 16 de la LPDP.

28. La ANPD tiene aprobada una Directiva de Seguridad de la Información con orientaciones según el tipo de tratamiento de datos personales que se efectúa, siguiendo una categorización de "Básico", "Simple", "Intermedio", "Complejo" o "Crítico" de los bancos de datos personales. Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2013/11/Directiva-de-Seguridad-DGPDP.pdf.

29. Entre los que se encuentran usuario-contraseña, uso de certificados digitales, *tokens*, entre otros.

horas de inicio y cierre de sesión y acciones relevantes.[30]

Igualmente, se deben establecer las medidas de seguridad relacionadas con los accesos autorizados a los datos mediante procedimientos de identificación y autenticación que garanticen la seguridad del tratamiento de los datos personales.

Es indispensable que los ambientes en los que se procese, almacene o transmita la información sean implementados con controles de seguridad apropiados.[31] Se deben contemplar los mecanismos de respaldo de seguridad de la información de la base de datos personales[32]; y, así, otras varias medidas de seguridad en caso de transferencia lógica o electrónica de datos personales, almacenamiento de documentación no automatizada, copia o reproducción de documentos, acceso a los mismos, entre otros.[33]

La potestad sancionadora de la ANPD se hace tangible con la imposición de multas como resultado final de los procedimientos incoados. Las infracciones están graduadas como "Leves", "Graves" y "Muy Graves", y las multas pueden ascender entre 0.5 a 5, más de 5 a 50, más de 50 a 100 Unidades Impositivas Tributarias, respectivamente[34]; que por el año 2020 se ha fijado en S/ 4,300.00 cada una. La cifra de las multas impuestas y recaudadas siempre será estimable[35], pero más cuantiosa aún es la cifra de las "multas no impuestas", dado que buena parte de las entidades públicas y privadas fiscalizadas por incumplimientos a la LPDP y su reglamento, subsanan las observaciones hechas por los fiscalizadores antes de la imputación de cargos o implementan las medidas correctivas establecidas por la ANPD, evitando con ello nuevas infracciones.

Esto último nos lleva a la última modalidad de protección de los datos personales por parte de la acción conocida de la ANPD; se trata de la prevención —y promoción— para evitar la afectación de los derechos. Pero esto tiene más sentido tratarlo en el próximo y último acápite.

IV. ¿HACIA DÓNDE VAMOS?

La irrupción de la tecnología digital y la interoperabilidad que ella permite entre actores públicos y privados, bancos o bases de datos —entre ellas la que contienen datos personales—, es imparable, y sería un error asumir una posición temerosa o desconfiada frente a esta realidad.

30. Como apunta la norma reglamentaria, estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, entre los que se encuentran el destino de los registros, una vez que éstos ya no sean útiles, su destrucción, transferencia, almacenamiento, entre otros.

31. Tomando como referencia las recomendaciones de seguridad física y ambiental recomendados en la Norma Técnica Peruana NTP-ISO/IEC 17799 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información —según refiere el artículo 40 del Reglamento de la LPDP—; la misma que ha sido sustituida por la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición, desde la vigencia de la Resolución Ministerial Nº 004-2016-PCM.

32. Con un procedimiento que contemple la verificación de la integridad de los datos almacenados en el respaldo, incluyendo, cuando sea pertinente, la recuperación completa ante una interrupción o daño, garantizando el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.

33. Estas y otros medidas de seguridad se encuentran recogidas entre los artículos 39 a 46 del Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS.

34. Artículo 39 de la LPDP.

35. Tan solo en el año 2019, la ANPD recaudó por concepto de multa pagada, la suma de S/ 970,853.90.

Todos nos hemos visto beneficiados por los avances de esta era: semáforos, teléfonos, electrodomésticos inteligentes, pulseras que monitorean el ritmo cardiaco, geolocalización, drones, códigos *QR*, internet de las cosas, *blockchain*, redes sociales, todo ello y mucho más ha contribuido definitivamente a estar mejor informados y a facilitar la vida a millones de personas en todo el mundo.

Pero como recordaba recientemente un colega colombiano dedicado a estas materias desde lo público, no todo lo tecnológicamente posible es éticamente deseable o aceptable. Y esta frase creo que retrata perfectamente mi idea de "lo que se viene", una fortalecida y compartida conciencia de proteger lo privado, de autodeterminarlo hasta donde sea posible hacerlo, y de exigir información transparente y fiable sobre el tratamiento que reciben nuestros datos por determinada organización, amén de exigirle a ella misma que los proteja de cualquier intromisión ilegítima.

Y estas expectativas sólo pueden satisfacerse con instituciones que funcionen y con entidades públicas y privadas que se tomen en serio los derechos y hagan de la ética pública su bandera, al margen del cumplimiento de cualquier ley vinculada a estas materias.

Por eso creo que es indispensable que se trabaje en prevención y en fomentar una cultura de protección de datos en el país; sobre todo entre los niños y adolescentes, siempre más expuestos que los adultos a sufrir las consecuencias de un descuidado manejo de sus redes sociales.[36]

Esa necesidad de prevenir y generar conciencia debe provenir de todos, actores públicos y privados. La ANPD tiene trabajos que exhibir[37], pero no sólo ella.[38]

Creo, por tanto, que el péndulo viene de vuelta y se situará en un punto menos extremo del que hemos presenciado hasta hace pocos años. Desde el Estado y las empresas se nota la preocupación, por un lado, de tener mayor presencia y hacer respetar una normativa que, en la actualidad, no sólo se circunscribe a la defen-

36. Por ejemplo, *grooming*, *sexting*, anglicismo y acrónimo para referirnos al engaño pederasta y a la práctica de enviar videos y/o fotos con contenido sexual o erótico, respectivamente.

37. Destaca, por ejemplo, el Primer Concurso de Dibujo e Historietas *#YoCuidoMisDatosPersonales* que se realizó en el segundo semestre de 2019. Significó el despliegue de su personal a 21 colegios públicos y privados de Lima y Callao, para brindar charlas informativas a 6590 estudiantes. Participaron 815 trabajos provenientes de 95 colegios. Disponible en: https://www.gob.pe/institucion/minjus/noticias/50749-minjusdh-convoca-a-concurso-escolar-de-dibujo-e-historietas-para-fortalecer-cultura-de-proteccion-de-datos-personales y https://www.gob.pe/institucion/minjus/noticias/69127-el-minjusdh-premia-a-ganadores-del-primer-concurso-escolar-de-dibujo-e-historieta-yocuidomisdatospersonales. También, las incursiones en espacios públicos —playas y plazas— para sensibilizar a la ciudadanía sobre la necesidad de proteger sus datos personales. Entre ellas, y la participación en ferias institucionales de servicios del Sector Justicia, se estima —la propia ANPD, Informe Nº 01-2020-JUS/DGTAIPD— que en el año 2019 se llegó con este formato a 12,747 personas. A este número, hay que agregarle 2700 personas naturales, muchas de ellas representantes de personas jurídicas o entidades públicas, a quienes durante el año pasado se capacitó sobre los alcances de la LPDP y las obligaciones que ella prescribe en materia de seguridad de la información y políticas de privacidad.

38. Por ejemplo, desde la Agencia Española de Protección de Datos, en coordinación con otras instancias gubernamentales de ese país como el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado del Ministerio de Educación y Formación Profesional, han lanzado las iniciativa "AseguraTIC - Seguridad del Menor en Medios Digitales", disponible en: https://intef.es/aseguratic/; una iniciativa que pretende convertirse en iberoamericana y que reúne abundantes recursos aportados por diferentes entidades públicas y privadas para que sirvan de base a la elaboración de materiales curriculares, en relación con el uso responsable de internet y la prevención de sus riesgos por los niños y adolescentes. También, desde la sociedad civil y la empresa, destaca la iniciativa del curso virtual *#AltoAlCiberacoso*, auspiciado por la empresa Movistar, Capital Humano y Social Alternativo - CHS Alternativo, entre otras. Disponible en: https://altoalciberacoso.com/.

sa del consumidor y la protección de los datos personales, sino que también abarca a la seguridad digital en su conjunto[39]; y, de otro lado, el sector privado, de transmitir la sensación de seguridad a los clientes respecto a cómo se manejan sus datos personales a partir de las políticas y medidas de seguridad que se adoptan.[40]

La sinergia entre lo público y privado es el camino para alcanzar un equilibrio razonable entre necesidades de mercado, de negocio, de seguridad, entre otras, con el derecho a la protección de los datos personales. Un buen ejemplo de esta sinergia ha sido la recientemente aprobada Directiva de la ANPD sobre tratamiento de datos personales mediante sistemas de videovigilancia[41]; la misma que refleja la experiencia institucional de esta entidad en las labores de fiscalización, y la perspectiva del sector privado sobre la cuestión, que colaboró activamente con sus aportes y observaciones desde que el proyecto de documento prescriptivo fuera pre-publicado el año pasado.

La protección de datos personales en estos tiempos no parece ya una quimera, lo que sí, un proceso en construcción al que estamos llamados a contribuir todos.

39. Muestras recientes de ello son el Decreto Legislativo 1412 que aprueba la Ley de Gobierno Digital, la cual establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública; o, el Decreto de Urgencia 007-2020 que aprueba el marco de confianza digital y dispone medidas para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional. Lo más saltante de este Decreto de Urgencia es que se crea un Centro Nacional de Seguridad Digital, que operará como una plataforma digital a través de la cual se gestione, dirija, articule y supervise la operación, educación, promoción, colaboración y cooperación de la seguridad digital a nivel nacional, como componente integrante de la seguridad nacional; además, se crea el Registro Nacional de Incidentes de Seguridad Digital, con el objetivo de recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional, que puedan servir de evidencia o insumo para su análisis, investigación y solución.

40. Un buen ejemplo internacional, es sin duda Facebook, a propósito de los eventos conocidos del año pasado. Disponible en: https://www.nytimes.com/es/2019/05/05/espanol/facebook-nuevo-diseno-privacidad.html. En sede nacional, y a propósito de los ciberataques de agosto de 2018, podemos recordar algún comunicado de la Asociación de Bancos del Perú en este sentido, disponible en: https://www.asbanc.com.pe/Paginas/Noticias/DetalleNoticia.aspx?ItemID=682.

41. Directiva Nº 01-2020-JUS/DGTAIPD, aprobada por Resolución Directoral Nº 02-2020-JUS/DGTAIPD, publicada en el diario oficial El Peruano, el 16 de enero de 2020. El tratamiento objeto de esta directiva comprende la grabación, captación, transmisión, conservación o almacenamiento de imágenes o voces, incluida su reproducción o emisión en tiempo real o cualquier otro tratamiento que permita el acceso a los datos personales relacionados con aquellos, para fines de seguridad, control laboral y otros.