Revista de Derecho YACHAQ N.° 13
Centro de Investigación de los Estudiantes de Derecho (CIED)
Universidad Nacional de San Antonio Abad del Cusco
ISSN: 2707-1197 (en linea)
ISSN: 1817-597X (impresa)
Fecha de recepción: 23/10/2021
Fecha de aceptación: 23/01/2022
[pp. 25-37]

La responsabilidad proactiva en la normativa peruana de protección de datos personales

Accountability in Peruvian personal data protection ruling

Raúl Vásquez Rodríguez

Resumen: Con la entrada en vigor del Reglamento 2016/679, comenzó a regir el principio de Responsabilidad Proactiva para el tratamiento de datos personales, redirigiendo el enfoque de las obligaciones hacia objetivos relacionados con la permanente prevención y la capacidad de rendición de cuentas sobre las obligaciones; a fin de garantizar de manera más eficiente la protección de los derechos de las personas sobre la privacidad. Dicha circunstancia actual lleva a preguntarse si en el ordenamiento jurídico peruano existen previsiones referidas a la protección de datos personales que conlleven la exigencia de adoptar medidas, políticas y hábitos preventivos respecto de la privacidad; y si podría hablarse de un principio de responsabilidad proactiva en un momento dado.

Palabras clave: protección de datos personales, responsabilidad proactiva.

Abstract: Since the European General Data Protection, accountability principle is in force for any data protecting handling operation, focusing on a new kind of tasks, aimed to prevention and accouting goals, in order to ensure privacy in the most efficient way.

This current fact aims to inquire about the Peruvian law and its specific rules which require establish preventive standards, policies and usages on privacy and personal data protection and likewise, if sometime, how accountability principle would be incorporate in Peruvian law.

Keywords: personal data protection, accountability.

I. INTRODUCCIÓN

En la actualidad, uno de los principales referentes normativos en cuanto al derecho fundamental a la protección de datos personales es el Reglamento 2016/679 del Parlamento Europeo y del Consejo de Europa, relativo a la protección de las personas físicas en el tratamiento de datos personales y a la libre circulación

[*] Abogado y Magíster en Derecho de la Propiedad Intelectual y de la Competencia por la Pontificia Universidad Católica del Perú, con especialización en Derecho Administrativo por la Universidad de Salamanca. Miembro del Colegio de Abogados de Lima.

de estos datos (en adelante, RGPD), el cual, desde su vigencia, ha introducido instituciones que buscan actualizar y reforzar el resguardo de la intimidad de las personas.

Utilizo el infinitivo «actualizar» porque en el entorno digital en el que actualmente las actividades humanas se desenvuelven, el refuerzo de la garantía mencionada implica no solo fuerza o coerción, sino mayor conocimiento de dicho entorno y, sobre todo, mayor disposición a renovar y reformular la ciencia adquirida, a fin de evitar su anquilosamiento e inoperancia antes nuevas situaciones. La nueva fuerza, como se observa en el derecho relacionado con las nuevas tecnologías, es la actualización constante, estar lo más adelante posible.

En nuestros tiempos de constante revolución tecnológica, el único factor «permanente» es la importancia de la información de toda índole, como insumo y como valor, lo que conlleva a que buena parte de dicha revolución y de la producción de conocimiento, se avoque a multiplicar maneras de explotarla, al punto de poder hablar de un mercado autónomo de datos con sus correspondientes usos tecnológicos y comerciales. Es tal la importancia de la información, que redunda en la trascendencia de las tecnologías para su explotación, haciendo que los intereses normativos se transformen (Muñoz de Alba, 1998, pp. 585-586), amplíen su espectro, se actualicen también, y exijan al Derecho una intervención permanentemente, adaptable, «a fin de evitar un desborde del «poder informático» que fácticamente ya ejercen aquellos que pueden acceder, manejar y sacar provecho de tales tecnologías (Sagüés, 1998, p. 862).

El RGPD ha adoptado instituciones que, si no satisfacen totalmente tal necesidad de avance por sí mismas, dejan condiciones para ello, asignan roles a los partícipes en el tratamiento de los datos personales, ya no solo exigencias a cumplir para evitar ser sancionados, sino funciones derivadas de la socialización de la protección de los datos personales que dicho reglamento comunitario promueve, al buscar que estas sean desempeñadas por quien efectúa las actividades reguladas, sin que ello implique un repliegue del derecho o de la administración, ni la posibilidad de un sistema de regulación «a la carta» a favor de dichos partícipes (Rodotá, 2005, pp. 9-10) o cualquier otra forma de abdicación.

Para desarrollar este artículo, en su primera parte, escojo una de las innovaciones normativas que socializa la protección de la privacidad, y que pretende cambiar la forma de promover el cumplimiento de la normativa y la prevalencia de los derechos y libertades de las personas: el principio de responsabilidad proactiva o *accountability*. Dicho principio es sencillo de explicar, pero más complicado de esquematizar; se desarrolla de forma fragmentada en la RGPD, y establece la prevención y permanente capacidad de respuesta en el tratamiento de datos personales como principal meta, más que una obligación.

En la segunda parte, atendiendo a la enseñanza que suele tomar nuestro sistema jurídico del sistema comunitario europeo, y a la comunión de figuras jurídicas, se escogerán figuras en la normativa peruana de protección de datos personales que reflejen la acogida que ya tiene dicho principio en nuestro ordenamiento, que, con su anterioridad en el tiempo, ya recojan en su esencia los propósitos de permanente prevención y capacidad de respuesta. Para ello, se analizará tanto la Ley N.° 29733, Ley de Protección de Datos Personales (en adelante, LPDP) conjuntamente con su reglamento, aprobado por el Decreto Supremo N.° 003-2013-JUS (en adelante, Reglamento de la LPDP), a fin de encontrar y desarrollar disposiciones específicas que reflejen los propósitos mencionados.

II. LA PROTECCIÓN DE DATOS PERSONALES EN EL ENTORNO DEL RGPD

1. Orígenes de la regulación comunitaria europea

Las eventuales amenazas que las tecnologías de la información habrían podido provocar para los derechos de las personas fueron ob-

jeto de preocupación en el Consejo de Europa desde fines de la década de los 60 del siglo XX. Todo ello se manifestó con la emisión de la Resolución N.° 509 de la Asamblea del Consejo de Europa, sobre los Derechos Humanos y los nuevos logros científicos y técnicos (Palma, 2018a, pp. 12-13), adoptada en 1968, con el fin de ir desarrollando métodos de protección específicos del derecho a la vida privada y familiar del artículo 8 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales (en vigor desde 1950), que comprendía el derecho la protección de los datos personales.

A fin de preservar tal derecho, y con calidad vinculante para los países miembros del Consejo de Europa, el 28 de enero de 1981 se emite el Convenio 108, que hace énfasis en el tratamiento automatizado de los datos personales, concatenando la protección con el interés comunitario de regular el tránsito de información y con las directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de la Organización para la Cooperación y el Desarrollo Económico en 1980. Este convenio, que fue objeto de actualización en el 2001 y en 2018, estableció, por primera vez, los deberes de los responsables del tratamiento y los derechos de los titulares de los datos personales, mediante el establecimiento de los contenidos mínimos que cada norma nacional debía desarrollar.

Con el dictado de normativas nacionales que diferían, entre sí, en cuanto a los niveles de protección, surgía un obstáculo para la libre circulación de datos, necesaria para el mercado interior de la Unión Europea (Fernández y León, 2016, p. 37). Por lo que se hizo permanentemente necesaria una armonización de normas a nivel comunitario. Con dicho objetivo se dicta la Directiva 95/46/CE de 1995, relativa a la protección de las personas físicas respecto del tratamiento de sus datos y a la libre circulación de estos.

Mediante un simple cotejo de fechas, se puede apreciar que el RGPD, que reemplazó a dicha directiva más de veinte años después, es una norma plenamente consciente de la innovación tecnológica, de la incidencia de la internet en las modalidades de tratamiento de los datos personales y su ámbito globalizado, así como del carácter de derecho fundamental independiente de la protección de datos personales, reconocido en el artículo 8 de la Carta Europea de Derechos Humanos del 2000. Por ello, tiene como objeto la regulación del revalorado derecho fundamental a la protección de datos personales. Y, a través de él, a la protección de otros derechos fundamentales, sin ensombrecer la libre circulación y, mucho menos, la necesidad de un régimen regional armónico; sin fragmentaciones que propicien inseguridad jurídica (Piñar, 2016b, pp. 56-60), ni rigidez normativa ante los cambios tecnológicos en el tratamiento de datos personales. Para ello, se recurrió ya no a una norma que establezca estándares de armonización, sino a la uniformización de derechos y obligaciones en todos los estados partícipes, contando con recursos concretos como «la creación de confianza y la garantía de control», señalados en el Considerando 7 del RGPD, como bien apunta Di Pizzo (2018, p. 245).

2. El principio de responsabilidad proactiva o *accountability* en el RGPD

El artículo 5 del RGPD establece los principios de conducta que rigen el tratamiento de datos personales, vale decir, las pautas que debe seguir la actividad de tratamiento: cómo se deben recoger, tratar y ceder; y qué valores son los que garantiza, como la intimidad y otros que incumben a las personas que, en este caso particular, deben ser utilizados para la integración e interpretación de toda la norma, ante cualquier laguna que pueda surgir gracias a los avances tecnológicos en tales actividades (Puyol, 2016, pp. 135-136). Atendiendo también a lo que desarrolla Zamudio (2012, p. 15), estos principios, como en la generalidad de las normativas, son raíces y fuentes interpretativas de las disposiciones subyacentes en la norma, al condensar sus finalidades generales.

Así, el apartado 1 de dicho artículo establece características que debe desarrollar el tratamiento para ser legítimo y garantizar los derechos y libertades de la persona: lícito y leal; mínimo indispensable en cantidad, modo y tiempo; con finalidad determinada; sobre datos exactos y actuales, y protector de la integridad y confidencialidad de la información personal. Entonces se establecen, desde estos principios, obligaciones a aplicar en cada operación o cadena de operaciones.

Ahora bien, el apartado 2 del mismo artículo señala lo siguiente: «El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("responsabilidad proactiva")» (Reglamento 2016/679 del Parlamento Europeo y del Consejo de Europa, 2016).

Al margen de la relación de causalidad establecida respecto de los principios, este apartado incorpora una obligación de nivel superior, de carácter permanente e independiente de cada operación particular de tratamiento de datos personales: La capacidad de demostrar que cumple con los principios, que concreta el principio de responsabilidad proactiva.

El aislamiento de esta disposición, respecto de la redacción de los otros principios, se debe a la necesidad de generalidad o perpetuidad de esta capacidad, lo cual implica mayores actos fuera del control efectivo de la licitud de cada actividad de tratamiento; como el diseño de sistemas y procedimientos, prácticas empresariales, mejora continua de las herramientas técnicas y organizativas, entre otras actividades de permanente desarrollo, avocadas a la protección de la privacidad y que esté presente en todo momento, como un valor predeterminado (Lorenzo, Palma y Trujillo, 2018, pp. 143-144), no solo como respuesta ante una denuncia o fiscalización.

Esta concepción se basa en la obra de Ann Cavoukian, excomisionada de Información y Privacidad de Ontario (Canadá), al hallar que «el cumplimiento de normas prestablecidas era insuficiente para proteger la privacidad, puesto que el avance de la tecnología supera a lo establecido para un período o situación específica. Por ello, consideró necesario que la privacidad no se active solo ante un riesgo específico, estando más bien, permanentemente activa de la estructura y del funcionamiento de los sistemas» (Cavoukian, 2009).

Conociendo el aceleramiento de la tecnología y la tangible desventaja que esta circunstancia conllevaba en lo concerniente a la protección de la privacidad y otros derechos de las personas, durante la redacción del RGPD se tomó en cuenta lo desarrollado por Cavoukian a fin de traducirlo en un principio expreso y claro, que haga obligatoria la socialización entre los responsables del tratamiento, de la protección de los derechos y libertades de las personas, y promueva las conductas preventivas en lugar de reactivas (Piñar, 2016a, p. 16), tendiendo a intervenir sobre las causas más que sobre consecuencias.

En ese sentido, el considerando 74 del RGPD, que delinea el contenido del principio de responsabilidad proactiva, desarrolla lo siguiente:

> Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas. (Reglamento 2016/679 del Parlamento Europeo y del Consejo de Europa, 2016)

Siendo lo transcrito la esencia de lo normado en el apartado 2 del artículo 5 del RGPD, queda en evidencia que la obligación continua, respecto de la aplicación de medidas dirigidas al cumplimiento de dicha norma, consiste en

la capacidad de demostrar o rendir cuentas de la permanente conformidad con la misma (de ahí, su vinculación con el anglicismo *accountability*), así como la eficacia de dichas medidas, las cuales deben guardar proporcionalidad con la modalidad y finalidades del tratamiento de datos personales, el contexto en el que se desarrolla y los riesgos que su desenvolvimiento puede generar.

Entonces, conociendo el núcleo de tal principio, corresponde mencionar algunas disposiciones subyacentes de dicho reglamento:

- Privacidad desde el diseño y por defecto (artículo 25): Obliga al responsable a privilegiar la privacidad al momento de escoger los medios del tratamiento, adecuados para salvaguardar la privacidad; o, de ser el caso, de crear tales medios, para lo cual, se debe adoptar la minimización en el tratamiento y en la cantidad de datos personales como regla por defecto, como función originaria, extensible durante toda la vida de la operación (Duaso, 2016, pp. 306-310).
- Seguridad en el tratamiento (artículo 32, apartado 1): A fin de preservar la integridad y confidencialidad de los datos personales, quien realice el tratamiento de los datos personales deberá adoptar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.
- Evaluación del riesgo (artículo 32, apartado 2): Para dotar de mayor diligencia, se requiere identificar los riesgos a los que pueden estar expuestos los datos personales, así como la trascendencia de su afectación (López, 2016, pp. 291-292).

Por supuesto, debido a su calidad de principio, debe entenderse que la responsabilidad proactiva no solo debe aplicarse al momento de escoger las medidas de seguridad o estudiar los riesgos que puede implicar una particular actividad de tratamiento; más bien, implica el deber del responsable y de quien participe en el tratamiento de datos personales, de rendir cuentas sobre la concordancia de tal actividad con el RGPD, en casos en los que deba comprobarse la legitimidad de un tratamiento por la obtención del consentimiento válido de los titulares de los datos personales, la atención de solicitudes de ejercicio de los derechos de estos (los clásicos, denominados «ARCO», así como los nuevos propuestos en dicho reglamento, como el de la portabilidad de datos) o el tratamiento de datos personales exactos y estrictamente necesarios para una finalidad determinada.

En consecuencia, el principio de responsabilidad proactiva del RGPD exige a quien realiza el tratamiento de datos personales, priorizar la prevención, así como el ejercicio permanente del control de la licitud en la generalidad de las operaciones de tratamiento, procurando en este la mejora y atención continua a los cambios tecnológicos y a los desafíos que estos propongan a la protección de los datos personales.

III. LA PROTECCIÓN DE DATOS PERSONALES EN EL ORDENAMIENTO JURÍDICO PERUANO

1. Desarrollo del derecho fundamental a la protección de datos personales

Más allá de los compromisos adoptados por el Perú, en materia de derechos fundamentales a nivel internacional, es necesario para este trabajo analizar la composición constitucional del mencionado derecho en el ordenamiento jurídico, teniendo como punto de partida la Constitución Política del Perú (en adelante, la Constitución), en su artículo 2, en el cual se incorporan también derechos conexos, como el derecho a la intimidad.

Al respecto, debido a la inevitable relación entre ambos derechos, derivada básicamente del hecho por el cual la vulneración de uno implica generalmente una intromisión a la

intimidad, es necesario demarcar una distinción de este con el derecho a la protección de datos personales, a fin de determinar las garantías que ofrece cada una.

El numeral 7 del artículo 2 de la Constitución «ofrece como garantía para la intimidad personal y familiar, la prohibición del escudriñamiento y/o divulgación no deseada de los actos de las personas, en su esfera totalmente individual, cuidando la soberanía de todo hombre sobre su propio espacio sin importar su condición» (Saldaña, 2012, p. 204), así como la familiar, amical, laboral; resguardando la inviolabilidad de tales actos y, de forma mediata, el equilibrio necesario para su desarrollo individual y en sociedad (Fernández, 2004, p. 59). De ello, surge concretamente la prohibición de intromisiones a la información referente a dichas esferas, así como la extracción de la misma.

Según lo desarrollado en mi artículo, «La protección de datos personales en Perú en el contexto Covid-19», el numeral 6 de dicho artículo constitucional establece protección contra el suministro de información que pueda afectar la intimidad personal y familiar y, en general, ante acciones de terceros sobre la información del individuo que perjudiquen su intimidad, haciendo que el ejercicio del derecho se ejerza a través del control de las acciones de terceros sobre su información, de acuerdo con la voluntad o criterio de la persona (Vásquez, 2020b, pp. 58-59).

Entonces, a través de tal derecho fundamental:

> se otorga a la persona la facultad de determinar qué se hace con ella y el destino que esta podrá tener, proporcionando no solo el poder de repeler intromisiones, sino también de prevenir, evitar y/o revertir los efectos de actividades de terceros que expongan su información personal, se tenga o no su consentimiento u otro supuesto que legitime tal tratamiento de información. Tales facultades satisfacen la necesidad de equilibrio a favor del individuo en la sociedad de la información y de acelerada evolución de las tecnologías mediante las cuales se procesa masivamente información, cuyo uso predominante corresponde a entidades públicas y privadas que ejercen poderes fácticos. (Pérez, 1996, pp. 23-24)

Los caracteres del derecho fundamental a la protección de datos personales son desarrollados también a través de sentencias del Tribunal Constitucional revisadas en mi artículo «El consentimiento para tratamiento de datos personales de salud en tiempos del COVID-19», como la recaída en el Expediente N.° 1797-2002-HD[1], que reconoce su autonomía respecto del derecho a la intimidad contemplado en el numeral 7, gracias a los poderes que otorga sobre terceros, lo cual es reforzado en la sentencia del Expediente N.° 4739-2007-PHD/TC[2], en la que se desarrolla la facultad de ejercer tal derecho fundamental ante el ac-

[1] **Tribunal Constitucional, 29 de enero de 2003, sentencia del Expediente N.° 1797-2002/HD**
«3. [...] 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».

[2] **Tribunal Constitucional, 15 de octubre de 2007, sentencia del Expediente N.° 4739-2007/HD**
«2. [...] el derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal».

cionar de personas naturales o jurídicas, públicas o privadas, confirmando el imperio del titular sobre su información personal y la prevalencia de su voluntad respecto del manejo de dicha información (Vásquez, 2020a, p. 151).

«Debe anotarse que la verdadera fuerza de este derecho fundamental, reside en los deberes u obligaciones que emanan hacia los terceros que realizan el tratamiento de los datos personales, así como en la existencia de un sistema de protección cuya implementación es una obligación del Estado» (Landa, 2017, pp. 76-77), de acuerdo con lo desarrollado en la normativa legal y reglamentaria destinada a su garantía, constituida por la LPDP y su reglamento.

2. Desarrollo legal y reglamentario del derecho fundamental a la protección de datos personales

La LPDP y su reglamento son las normas infraconstitucionales mediante las cuales se desarrollan los derechos de las personas derivados del derecho fundamental a la protección de datos personales. Asimismo, se establecen las condiciones de licitud del tratamiento de datos personales, a través de sus principios rectores, de las cuales emanan las obligaciones a cumplir por las personas o entidades que efectúen dicho tratamiento, las cuales se encaminan también a tutelar los derechos de las personas titulares de los datos personales.

Entre tales principios se encuentran dos a través de los cuales se desarrollan muy claramente disposiciones que requieren de comportamientos dirigidos a la prevención y a la comprobación permanente del cumplimiento, por parte de quienes realizan el tratamiento de datos personales: El principio de consentimiento y el principio de seguridad.

2.1. El principio de consentimiento de la LPDP

Siguiendo al principio establecido en el artículo 5 de la LPDP[3], el consentimiento constituye uno de los escenarios ordinarios de legitimación de tratamiento de datos personales, al igual que los mencionados en el artículo 14 de dicha ley[4] (situaciones en las que no es obligatorio obtener el consentimiento); así como

---

[3] **Congreso de la República, 3 de julio de 2011, Ley N.° 29733, Ley de Protección de Datos Personales. Diario oficial *El Peruano*.**
«**Artículo 5. Principio de consentimiento**
Para el tratamiento de los datos personales debe mediar el consentimiento de su titular».

[4] **Congreso de la República, 3 de julio de 2011, Ley N.° 29733, Ley de Protección de Datos Personales. Diario oficial El Peruano.**
«**Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales**
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
[...]
5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
[...]»

uno de los primeros factores que se debe configurar para asegurar la licitud en el proceso de tratamiento de datos personales.

De acuerdo con lo desarrollado en el artículo de mi autoría «El consentimiento para tratamiento de datos personales de salud en tiempos del COVID-19», en dicho artículo se establece la acción a la cual está obligado el responsable del mencionado tratamiento en situaciones ordinarias: Obtener la manifestación de voluntad del titular de los datos personales, mediante la cual decide si permite el tratamiento, siguiendo unas condiciones mínimas de conocimiento y libertad, desarrolladas como requisitos mínimos de validez del consentimiento en otros artículos de la misma ley y su reglamento, como el inciso 13.5 del artículo 13[5] de la LPDP y el artículo 12 de su reglamento, que son las siguientes:

- **Libre:** La manifestación de voluntad de otorgar el consentimiento (como todo acto jurídico contemplado en el Código Civil) no debe someterse a coacción, engaño, dolo o cualquier otra distorsión o impedimento de sus facultades.
- **Previo:** El consentimiento debe otorgarse antes del inicio de la acción de tratamiento para la cual se solicita.
- **Expreso e inequívoco:** El consentimiento debe manifestarse de forma tangible, ya sea de forma escrita (virtual o física), verbal o a través de una conducta indiscutiblemente favorable a autorizar el tratamiento.
- **Informado:** Para obtener el consentimiento, el responsable debe otorgar, de forma previa, la información detallada sobre los factores básicos del tratamiento a realizar y las condiciones en las que se efectuará (siguiendo lo establecido en el numeral 4 del artículo 12 y el artículo 18 de la LPDP); permitiendo al titular de los datos personales su pleno entendimiento y, con ello, la formación de su voluntad consciente (Vásquez, 2020a, pp. 154-155).

En este punto, es necesario analizar la disposición del artículo 15 del Reglamento de la LPDP, referido al sustento o carga de la prueba, que establece que:

> Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley y en el presente reglamento, la carga de la prueba recaerá en todos los casos en el titular del banco de datos personales o quien resulte el responsable del tratamiento.

Esta disposición se incorpora debido a que el tratamiento efectuado sobre los datos personales de una determinada persona, implica una intromisión a su espacio, una alteración de su estado ordinario, cuya legitimidad debe ser comprobada por quien la propició. Por tal motivo, se requiere comprobar que se establecieron condiciones adecuadas para que el titular decida su voluntad con todos los elementos de juicio necesarios y, sin alteración o coacción alguna del razonamiento (libertad e información), la pueda manifestar de manera inequívoca, que no deje lugar a interpretaciones ni en el momento de su emisión ni después (expresión tangible de consentimiento), con lo que se pueda autorizar a iniciar el tratamiento (carácter previo), que no es lo mismo que «convalidar» un tratamiento ya iniciado, lo cual no es admisible en nuestro ordenamiento jurídico.

---

[5] **Congreso de la República, 3 de julio de 2011, Ley N.° 29733, Ley de Protección de Datos Personales. Diario oficial *El Peruano*.**
«**Artículo 13. Alcances sobre el tratamiento de datos personales**
[...]
13.5 Los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. El consentimiento debe ser previo, informado, expreso e inequívoco».

Tal circunstancia obliga, a quien realiza el tratamiento de datos personales, a efectuar acciones que superen la mera solicitud válida de consentimiento, llegando a conservar los soportes de la manifestación de tal voluntad (formatos impresos o soporte digital), a implementar los medios para atender las posibles revocaciones o solicitudes de derechos ARCO posteriores, a restringir o cesar inmediatamente el tratamiento de los datos de aquellas personas que no lo consientan, entre otros factores respecto de los cuales, el sujeto que efectúa el tratamiento debe ser capaz en todo momento de presentar sustento, a fin de poder demostrar también la licitud de su actividad.

2.2. El principio de seguridad de la LPDP

En la LPDP, el principio de seguridad se regula desde los artículos transcritos a continuación:

> **Artículo 9. Principio de seguridad**
>
> El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.
>
> **Artículo 16. Seguridad del tratamiento de datos personales**
>
> 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.
>
> Los requisitos y condiciones que deben reunir los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.
>
> 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.

De dichos artículos, se desprenden los medios que debe adoptar quien realiza el tratamiento de datos personales (medidas técnicas, organizativas y legales) para evitar las consecuencias sobre la seguridad de la información que se busca prevenir, a través de la evasión o control oportuno de un incidente de seguridad, las cuales se encuentran reseñadas en el artículo «El principio de seguridad de la Ley de protección de datos personales»:

- **Alteración:** Cambio en el contenido de los datos personales, que se puede dar a través del sistema utilizado para su tratamiento o en el caso del tratamiento no automatizado, con la manipulación del soporte impreso o escrito donde se plasmaron tales datos.
- **Pérdida:** Desaparición parcial o total del contenido de los datos personales debido a su eliminación en el respectivo soporte, la destrucción o sustracción de este.
- **Tratamiento o acceso no autorizado:** Acceso y actividad de tratamiento de datos personales efectuada por una entidad o por una persona no autorizada, vinculada o no al responsable, que carezca de autorizaciones o de una cualidad personal (cargo) que lo legitime para acceder o efectuar la mencionada actividad. (Vásquez, 2019)

Entonces, la seguridad aplicada a la protección de los datos personales, debe entenderse como la disposición de medidas por parte de quien realiza el tratamiento de datos personales. Está dirigida a resistir y prevenir las consecuencias previamente listadas, configurables a través de un incidente de seguridad. Con lo cual, como señala adecuadamente Dávara (2000, pp. 24-25), se evitan atentados

contra los derechos de los titulares de tal información personal. A su vez, se busca preservar la exactitud de los datos personales, así como la restricción de su empleo en actividades lícitas y legítimas, centrándola exclusivamente en su uso por parte del personal cuyas funciones dependan de ello, en el seno de una organización.

En este punto, es pertinente señalar que la normativa peruana ofrece una relativa libertad de medios para alcanzar tales objetivos. Solamente en el capítulo V del título III del Reglamento de la LPDP (artículos 39 al 45) presenta unas medidas de seguridad específicas, cuyas aplicaciones deben entenderse como un mínimo inicial a partir de las cuales se desplegarán las actuaciones que sean necesarias, de acuerdo con el contexto, tipo y finalidad del tratamiento que se esté realizando, así como la naturaleza de los datos personales y los riesgos que dicha actividad pueda generar.

Asimismo, conviene indicar que, salvo por la aplicación de los mencionados artículos del Reglamento de la LPDP, la obligación que se desprende de este principio es una de medios, de diligencia, de mantener la posibilidad de poder abarcar lo más posible, sin desconocer un grado residual de vulnerabilidad que puede existir en el tratamiento de datos personales, pese a la implementación correcta de tales medidas.

Entendiendo como premisa que siempre habrá una desventaja respecto de la tecnología, lo que debe comprobar el responsable del tratamiento en su diligencia, asimismo el haber adoptado las medidas de seguridad necesarias, tecnológicamente disponibles y de una intensidad acorde con la sensibilidad de la información personal almacenada, para prevenir y evitar, en lo más posible, las consecuencias perjudiciales reseñadas; quien, además, debe acoger de forma permanente tales conductas, como parte de las políticas y usos empresariales, con lo cual puede generar un entorno más seguro y más listo para anticipar cualquier nuevo riesgo o amenaza que la tecnología pueda traer.

IV. CONCLUSIONES

De lo estudiado, se desprende que en los casos revisados, existe la necesidad de que el cumplimiento de las disposiciones dirigidas a preservar la privacidad de la información de las personas tienda a exigir comportamientos permanentemente preventivos, «siempre listos» y no solamente reactivos, que respondan solo a las alertas de denuncias o actividades de fiscalización; con lo cual, el tratamiento de los datos personales que se realiza, en todo momento, garantice los derechos y libertades de las personas.

Respondiendo a la necesidad planteada desde la introducción, de que la normativa, más que establecer o dictar acciones específicas, deje paso a nuevas formas de alcanzar el objetivo a través de la prevención, en ambos casos encontramos normas que establecen obligaciones de medios que guardan cierta neutralidad en los mismos (Remolina, 2013, pp. 220-221) que conlleve a una flexibilización de los mismos; que tienen como obligación final que el responsable del tratamiento haga permanente y prioritaria, en todas las acciones que compongan las cadenas y actividades de tratamiento, la protección de la privacidad y la prevención ante cualquier amenaza existente o potencial.

Debe anotarse que una materia tan involucrada con el avance tecnológico y la explotación de la información, como la protección de datos personales, siempre deberá tener algo de flexibilidad, establecer objetivos claros y espacio a hábitos, más que «acciones permanentes», así como a la renovación de conocimientos y medidas, con la finalidad de no perder el paso a los cambios y formas nuevas que introduzca la tecnología en el entorno digital, sobre todo.

Por ello, no debería sorprender demasiado que la LPDP, que cumplió diez años de publicada, y su reglamento, publicado en mayo de 2013, tenga disposiciones que deje espacio a actuaciones preventivas, a hábitos organizacionales siempre activos y a la revisión de los

mismos, básicamente por el carácter permanentemente cambiante de todo aquello relacionado con las tecnologías de información y comunicaciones en el mundo digital.

En tal sentido, resulta importante la positivización de esa convocatoria a los responsables del tratamiento de datos personales, de tomar acción en beneficio de los derechos y libertades, a través del principio de responsabilidad proactiva y de las disposiciones subyacentes del RGPD revisadas en la parte 1 de este artículo que, en apariencia, no harían más que acoger una necesidad obvia, que tímidamente se atendía en la Directiva 95/46/CE, pero que actualmente tiene un rango ordenador de principio.

En el caso peruano, no se puede descartar la acogida de la responsabilidad proactiva como un principio que guíe las operaciones del tratamiento de datos personales, considerando el carácter meramente enunciativo del listado de principios de la LPDP, determinado así en su artículo 12[6], que puede permitir dar mayor alcance e importancia a una exigencia cada vez más necesaria para equilibrar los poderes fácticos que surgen en los vínculos informáticos, concretamente más favorables para quienes dominan las herramientas y extracción de información.

Para alcanzar tal equilibrio, siguiendo a Cavoukian, las normas impositivas y sancionadoras ya están —siempre estuvieron—; lo que se necesita, adicionalmente, es promover los hábitos, los comportamientos preventivos y la diligencia permanente, sin descartar otras opciones que se puedan adaptar a esta materia, como el seguimiento o la regulación responsiva, la autorregulación siempre vigilada por el Estado, que nunca debe abdicar en su deber de garantizar los derechos fundamentales.

V. BIBLIOGRAFÍA

Adsuara, B. (2016). El consentimiento. En Piñar, J. L. (director). *Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad* (pp. 151-169). Editorial Reus S. A.

Castro, K. (2008). El Derecho Fundamental a la Protección de Datos Personales: Aportes para su Desarrollo en el Perú. *Ius et Veritas*, *18*(37), pp. 260-277.

Cavoukian, A. (2009). *Privacy be Design. The 7 foundational principles*. https://www.ipc.on. ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Dávara Fernández De Marcos, I. (2011). *Hacia la Estandarización de la Protección de Datos Personales*. Editorial La Ley.

Dávara Rodríguez, M. A. (2000). *La Protección de Datos Personales en el Sector de las Telecomunicaciones*. Universidad Pontificia Comillas.

Dávara Rodríguez, M. A. (2015). *Manual de Derecho Informático (11)*. Editorial Aranzadi S. A.

Di Pizzo Chiacchio, A. (2018). *La Expansión del Derecho al Olvido Digital. Efectos de «Google Spain» y el Big Data e implicaciones del Nuevo Reglamento Europeo de Protección de Datos*. Editorial Atelier.

Duaso Calés, R. (2016). Los principios de protección de datos desde el diseño y protección.

[6] **Congreso de la República, 3 de julio de 2011, Ley N.° 29733, Ley de Protección de Datos Personales. Diario oficial *El Peruano*.**

«**Artículo 12. Valor de los principios**

La actuación de los titulares y encargados de tratamiento de datos personales y, en general, de todos los que intervengan con relación a datos personales, debe ajustarse a los principios rectores a que se refiere este Título. Esta relación de principios rectores es enunciativa.

Los principios rectores señalados sirven también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de esta Ley y de su reglamento, así como de parámetro para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia».

de datos por defecto. En Piñar Mañas, J. L. (director). *Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad* (pp. 295-320). Editorial Reus S. A.

Fernández Sessarego, C. (2004). *Derecho de las Personas. Exposición de Motivos y Comentarios al Libro Primero del Código Civil Peruano (Novena edición)*. Editorial y Librería Jurídica Grijley E. I. R. L.

Fernández Conte, J. y León Burgos, D. (2016). Antecedentes y proceso de reforma sobre protección de datos en la Unión Europea. En Piñar Mañas, J. L. (director). *Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad (pp. 35-50).* Editorial Reus S. A.

Landa Arroyo, César. (2017). *Los derechos fundamentales.* Pontificia Universidad Católica del Perú, Fondo Editorial.

Lete Del Río, J. M. (1996). *Derecho de la Persona.* Madrid: Editorial Tecnos S. A.

Lorenzo, S., Palma, A. y Trujillo, C. (2018). Responsabilidad proactiva. En Murga Fernández, J. J.; Fernández Scagliusi, M. A. y Espejo Lerdo De Tejada, M. (directores). *Protección de Datos, Responsabilidad Activa y Técnicas de Garantía* (pp. 143-172). Editorial Reus S. A.

Muñoz de Alba Medrano, M. (1998). Los nuevos derechos humanos en la era tecnológica: ¿El Hábeas Data…la solución? En *V Congreso Iberoamericano de Derecho Constitucional.* Instituto de Investigaciones Jurídicas - Universidad Nacional Autónoma de México. Serie: G, Estudios Doctrinales, N.° 193, pp. 583-599.

Palma Ortigosa, A. (2018). Contexto normativo de la protección de datos personales. En J.J. Murga Fernández, M.A. Fernández Scagliusi y M. Espejo Lerdo De Tejada (directores). *Protección de Datos, Responsabilidad Activa y Técnicas de Garantía* (pp. 12-24). Editorial Reus S. A.

Palma Ortigosa, A. (2018). Principios Relativos al Tratamiento de Datos Personales. En Murga Fernández, J. J.; Fernández Scagliusi M. A. y Espejo Lerdo De Tejada, M. (directores). *Protección de Datos, Responsabilidad Activa y Técnicas de Garantía* (pp. 39-50). Editorial Reus S. A.

Pérez Luño, A. (1996). *Manual de Informática y Derecho.* Editorial Ariel.

Piñar Mañas, J. L. (2016). Introducción. Hacia un nuevo modelo europeo de protección de datos. En Piñar Mañas, J. L. (director). *Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad* (pp. 15-22). Editorial Reus S. A.

Piñar Mañas, J. L. (2016). Objeto del Reglamento. En Piñar Mañas, J. L. (director). *Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad* (pp. 51-62). Editorial Reus S. A.

Puyol Montero, J. (2016). Los Principios del Derecho a la Protección de Datos. En Piñar Mañas, J. L. (director). *Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Privacidad* (pp. 135-150). Editorial Reus S. A.

Remolina Angarita, N. (2013). *Tratamiento de Datos Personales: Una Aproximación Internacional y Comentarios a la Ley 1581 de 2012*. Editorial Legis S. A.

Rodotá, S. (2005). ¿Cuál derecho para el nuevo mundo? *Revista de Derecho Privado* (9), 5- 20.

Rubio Correa, M. (2017). *Para conocer la Constitución de 1993* (6.ª ed.). Pontificia Universidad Católica del Perú, Fondo Editorial.

Sagüés, N. P. (1998). Habeas Data: Su desarrollo constitucional. En Instituto de Investigaciones Jurídicas - Universidad Nacional Autónoma de México (editor). *V Congreso Iberoamericano de Derecho Constitucional* (pp. 859-872).

Saldaña Díaz, M. N. (2012). *'Right to privacy':* La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis. *UNED Revista de Derecho Político* (85), 195-240.

Trujillo Cabrera, C. (2018). Las Bases de Legitimación del Tratamiento de Datos Personales. En Especial, el Consentimiento. En Murga Fernández, J. J.; Fernández Scagliusi, M. A. y Espejo Lerdo De Tejada, M. (directores). *Protección de Datos, Responsabilidad Activa y Técnicas de Garantía* (pp. 51-75). Editorial Reus S. A.

Vásquez Rodríguez, Raúl. (2019, 7 de diciembre). El principio de seguridad de la Ley de protección de datos personales. *LP Derecho.* https://lpderecho.pe/principio-seguridad-ley-de-proteccion-datos-personales-raul-vasquez-rodriguez/

Vásquez Rodríguez, Raúl (2020). El consentimiento para el tratamiento de datos personales de salud en tiempos del Covid-19. *Yachaq Cied Derecho*, (11), 145-164.

Vásquez Rodríguez, Raúl. (2020). La protección de datos personales de salud en Perú en el contexto Covid-19. *Integración Regional & Derechos Humanos*/*Revista Regional,* Año VII, (2), 49-71.

Zamudio Salinas, M. (2012). El marco normativo latinoamericano y la ley de protección de datos personales del Perú*. Revista Internacional de Protección de Datos Personales* (1), 2-21.