La protección de datos en el Perú en el contexto de InterPARES TRUST

Aída Luz Mendoza Navarro

Introducción

Las Tecnologías de la Información y Comunicaciones (TIC) favorecen las relaciones humanas, permitiendo contar con una comunicación en tiempo real; sin embargo, la información respecto de su titular puede ponerse en riesgo cuando terceros no autorizados acceden a la reservada o sensible, invadiendo su derecho a la privacidad.

En ese contexto, surgen las leyes de protección de datos que los países han emitido, al tiempo que investigaciones internacionales asumen el tema ofreciendo valiosos aportes para minimizar los riesgos que aún ofrecen. La atención con diversidad de profesionales es lo indicado, cuyos valiosos aportes contribuyen a mejorar su aplicación y a disminuir los riesgos para crear confianza en los ciudadanos.

Aspectos de la protección de datos en la legislación peruana

La Ley N° 29733 de Protección de Datos Personales del Perú (LPDP) tiene su antecedente en el artículo 2, inciso 6 de la *Constitución Política*, que establece el derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten a la persona o su familia (PCM, 2013).

El proyecto InterPARES en América Latina y el Caribe
Apuntes sobre archivos digitales, transparencia, acceso a la información y protección de datos personales
ISBN: 978-607-96598-X-X en trámite • PP. 134-139

La LPDP tiene por objeto garantizar (art. 1°) el derecho fundamental a la protección de los datos personales de acuerdo con la *Constitución Política del Perú*, (PCM, 2011).

El Reglamento de la LPDP, aprobado por el DS N° 003-2013-JUS, en su artículo 2°, inc. 4, se refiere a la definición de datos personales, indicando que se trata de información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier otro tipo sobre personas naturales que se identifica por medios que puedan ser razonablemente utilizados (MINJUSDH, 2013). Se precisa que el tratamiento de los datos personales es lícito cuando el titular de los datos lo autorizó con su consentimiento, expresado en forma directa y clara, a lo que le siguen una serie de medidas de seguridad, responsabilidades, restricciones específicas tanto para el titular del banco de datos personales como para el encargado de su tratamiento.

Según el Decreto Legislativo 1412, artículo 18.4, Ley de Gobierno Digital, la prestación de servicios digitales debe garantizar el acceso a la información requerida por otra entidad de la Administración Pública, sobre los datos de las personas que se encuentren en su poder en medios electrónicos, pero solo para sus funciones y competencias, no pudiendo realizar intercambio de información que pueda afectar la seguridad nacional o aquella relacionada con la legislación sobre Transparencia y Acceso a la Información Pública, o la excluida por Ley y por Decreto Legislativo N° 1353, en el que se crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública y Datos Personales, que es una Dirección General dependiente del Viceministerio de Justica que carece de autonomía. Se trata de una unidad orgánica de cuarto nivel organizacional, subordinada al Viceministerio –a diferencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), de México–. La Dirección General en alusión cuenta con una Dirección de Protección de Datos Personales y un Tribunal de Transparencia y Acceso a la Información que, de acuerdo con el artículo 6° y el inc. c del artículo 7, dirime mediante opinión técnica vinculante sobre los casos de conflicto surgidos por aplicación de la LPDP y según el art. 3° de las modificaciones del DL en comentario, se establece que se aplica a los datos contenidos o destinados a ser contenidos en banco de datos personales de la administración pública y privada, objeto de protección de datos sensibles -definidos en la ley como datos biométricos que pueden identificar al titular, su origen racial y étnico, los ingresos económicos, opiniones o convicciones de orden político, religioso, filosóficos, sindical, la salud o la vida sexual–.

Por Resolución de la Secretaría de Gobierno Digital N° 001-2018-PCM/SEGDI, de 12 de enero de 2018, se aprobaron los *Lineamientos de Almacenamiento de la Información en la Nube* (PCM, 2018). El documento contiene principios generales para el uso de los servicios en la

Ir al Contenido

nube; requisitos en materia de seguridad de la información y protección de datos de carácter personal; normativa interna; contratación y operación.

Según los lineamientos, las entidades de la Administración Pública (AP) asumen responsabilidades en relación con los servicios junto con el proveedor. Ambas partes evalúan las prácticas necesarias para garantizar sus entornos. Destacamos que los lineamientos indican que la AP, cuando se trate de datos personales de alta confidencialidad con características críticas para la seguridad del país, pueden evaluar que la localización de los datos se restrinja al ámbito territorial, optando por contratar servicios en nube que almacenen y procesen estos datos de entorno de nube dedicado, para mayor seguridad.

La LPDP no menciona la contratación de servicios en la nube, pero en el artículo 9° sobre el principio de seguridad considera que el titular del banco de datos personales y el encargado de su tratamiento establecen las medidas técnicas, organizativas y legales que garanticen la seguridad de los datos personales con el fin de proteger su alteración o acceso no autorizado. Estimo que en este tema la ley debió ser mucho más precisa en el momento de la contratación, sobre todo cuando se trata de datos del servicio público, no basta la delegación de las medidas en el encargado de los datos.

La protección de datos es un tema esencialmente jurídico que se inicia con el principio de consentimiento del titular de los datos para su tratamiento según la LPDP peruana. Es el titular el que legitima el tratamiento; por lo demás, todo el texto de la norma gira en la actuación del titular de la entidad y el encargado de los datos personales, concluyendo en la especificación de sanciones cuando no se observan las medidas de protección de la privacidad de los datos personales.

Los lineamientos señalan que la AP debe mantener el control total y la propiedad sobre sus datos y puedan elegir –según la evaluación de riesgos e impactos– la ubicación geográfica en la que se almacenen los mismos. Los prestadores de servicios en la nube deben proporcionar controles de identidad y acceso a la infraestructura y los datos del cliente, cumpliendo estándares y observando las políticas de seguridad –como visibilidad, control y auditabilidad–.

Adicionalmente, se expidieron dos decretos de urgencia, que traen algunas disposiciones, a nuestro modo de ver, importantes referidas a la PDP:

> *Decreto de Urgencia N° 06-2020*, (El peruano, 2020: 3). Crea el Sistema Nacional de Transformación Digital y tiene como principios, entre otros, reconocer los datos como activo estratégico para diseñar políticas, entrega de servicios digitales y hacer

Ir al Contenido

una gestión transparente y ética de los datos en procesos y estructura de gobernanza. Sobre protección de datos personales, incide en la preservación de seguridad, asegurando la estructura de gobernanza, regulación y liderazgo para el equilibrio de la apertura de datos, niveles de privacidad y seguridad digital. Se asigna a la Secretaría de Gestión Pública como el ente rector, y además se crean los Comités de Gobierno Digital en cada entidad pública.

Decreto de Urgencia N° 07-2020. Crea el Marco de Confianza Digital y dispone medidas para su fortalecimiento. Surge como recomendación de la Organización para la Cooperación y el Desarrollo Económico (OCDE). El dispositivo es necesario para articular acciones con los actores relevantes en la gestión de seguridad digital y fortalecimiento de la confianza. Los ámbitos de protección, entre otros, son los datos, la transparencia y la seguridad digital. Se destaca la confianza digital como componente de la Transformación Digital. La norma alcanza a los organismos públicos y privados.

La Secretaría de Gobierno Digital está facultada para emitir la normativa técnica en materia de Confianza Digital. Se crea el Registro Nacional de Incidentes de Seguridad Digital Confidencial para recibir, consolidar y mantener datos e información sobre los incidentes reportados por los proveedores de servicios digitales a nivel nacional que serán evidencia o insumo para su análisis, investigación y solución. La norma permite a las entidades públicas y privadas administrar los datos personales, biométricos y espaciales, activos estratégicos, para garantizar que se comparta su proceso, el acceso, su publicidad, almacenamiento, conservación y que se pongan a disposición, considerando necesidades de información, uso ético y transparencia, riesgos en cumplimiento de la normativa de protección de datos personales, gobierno digital y seguridad digital.

InterPares Trust en la protección de datos

InterPARES Trust (ITrust; 2012-2019) de carácter multidisciplinario e interdisciplinario abordó, entre otros temas, la confianza y confiabilidad de documentos y datos en línea. Al respecto, Luciana Duranti –directora del proyecto– y Adam Jansen se refieren a cómo alcanzar las metas y objetivos de la investigación, entre otros, descubriendo cómo las políticas y prácticas sobre manejo de los documentos digitales de instituciones y profesionales pueden afectar la confianza del público sobre ellos, bajo la dependencia de los servicios de Internet. Se trata de anticiparse a los problemas para mantener la confianza en los documentos digitales de entidades que sufren niveles de desconfianza –como las

Ir al Contenido

policiales, financieras, médicas, de radiodifusión, *hacktivists*, organizaciones y profesionales gubernamentales. También se propuso establecer la importancia de los contextos nacionales/culturales en relación al nivel de confianza que disfrutan los documentos digitales en Internet. Otro de los objetivos fue articular políticas, procedimientos y prácticas Modelo para crear, gestionar, accediendo y/o almacenando registros en Internet, como medios de comunicación y computación en la nube o ambientes tecnológicos móviles, y además probarlos en una variedad de contextos para aprobar normas a nivel internacional y desarrollar buenas prácticas; además de formular propuestas y Modelos para la reforma legal y requisitos funcionales, dirigidos a los sistemas en el que los proveedores de Internet almacenan y gestionan documentos digitales.

Las investigaciones realizadas por ITrust nos llevan a reflexionar sobre las medidas o garantías para la transmisión o puesta en servicio de la información en Internet. En ese contexto, vendría muy bien a las organizaciones peruanas encargadas del Gobierno Digital, la Transparencia de la Función Pública y la Protección de Datos, líneas arriba referidas, revisar los resultados de las investigaciones de ITrust para implementar los servicios digitales bajo medidas que busquen crear confianza en la población respecto de los medios tecnológicos, además de garantizar, tal como se expresa en el artículo 18.8 del DL 1412, la conservación de las comunicaciones y documentos generados a través de canales digitales en las mismas o mejores condiciones que aquellas utilizadas por los medios tradicionales.

Conclusiones

La LPDP indica las medidas de uso una vez autorizado el tratamiento de los datos, según el principio de consentimiento. La facilidad de transmisión de la información por medios digitales demanda tomar todas las previsiones necesarias para proteger los datos para usos distintos a la autorización de su tratamiento.

InterPares Trust se fija una serie de objetivos de investigación cuyos resultados son un valioso aporte en diversas áreas de tratamiento de datos por medios electrónicos.

Referencias

PCM (1993). *Constitución Política del Perú*. Disponible en: http://www.pcm.gob.pe/wp-content/uploads/2013/09/Constitucion-Pol%C3%ADtica-del-Peru-1993.pdf

PCM, (S/f). "Ley de protección de datos personales, N° 29733". Disponible en: http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf.

El peruano (2018, enero 4). "Aprueban Lineamientos para uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano". En El peruano. Diario Oficial del Bicentenario. Disponible en: https://busquedas.elperuano.pe/normaslegales/aprueban-lineamientos-para-uso-de-servicios-en-la-nube-para-resolucion-no-001-2018-pcm-segdi-1605580-1/.

PCM (2018). *Lineamientos para el uso de servicios en la Nube para entidades de la Administración Pública del Estado Peruano*. Disponible en: https://www.peru.gob.pe/normas/docs/Lineamientos_Nube.PDF.

El peruano (2020, enero 4). "DU N° 06-2020. Sistema Nacional de Transformación Digital", p. 3. Disponible en: https://busquedas.elperuano.pe/download/url/decreto-de-urgencia-que-crea-el-sistema-nacional-de-transfor-decreto-de-urgencia-n-006-2020-1844001-1.

El peruano (2020, enero). "DU N° 07-2020, Marco de Confianza y medidas de fortalecimiento". Disponible en: https://busquedas.elperuano.pe/normaslegales/decreto-de-urgencia-que-aprueba-el-marco-de-confianza-digita-decreto-de-urgencia-n-007-2020-1844001-2/.

Duranti, L.; Jensen, A. (S/f). *The InterPARES Trust Project – Trust and Digital Records in an Increasingly Networked Society*. Disponible en: https://interparestrust.org/trust.

PCM (2018, septiembre 13). "Decreto Legislativo 1412 de Gobierno Digital". Disponible en: https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf.