Revista *SAPERE*
Facultad de Derecho – USMP
Vol. 1 Núm. 28 (2025)

Gobierno digital y protección de datos personales en la administración pública peruana

Raquel Estefany Torres Montano
rtorresm@usmp.pe
Estudiante del 11° ciclo Derecho USMP
https://orcid.org/0009-0007-5386-5509

Sumario:

Resumen

El Estado peruano se encuentra inmerso en un proceso de transformación digital de la Administración Pública, lo que plantea desafíos en la protección de los datos personales; la Constitución Política del Perú garantiza el derecho fundamental a la intimidad y a la autodeterminación informativa (art. 2.6), marco en el cual la Ley N.° 29733 (2011) estableció normas para el tratamiento de datos personales. En ese contexto, el reciente Reglamento aprobado por el Decreto Supremo N.° 016-2024-JUS (30 nov. 2024) actualiza y fortalece el esquema normativo de protección de datos, introduciendo nuevas obligaciones y derechos (notificación de incidentes, oficiales de datos personales, entre otros). Adicionalmente, el marco de gobierno digital se ha fortalecido con el Decreto Legislativo N.° 1412 (Ley de Gobierno Digital), que consagra principios como la "privacidad desde el diseño" de los servicios digitales y el "nivel de protección adecuado" para los datos personales, vinculándolos expresamente con la Ley N.° 29733.

En este artículo se analiza críticamente el entramado normativo vigente en la materia, considerando principios constitucionales (privacidad, transparencia y debido proceso) y jurisprudencia relevante. La doctrina constitucional peruana ha reafirmado que la

autodeterminación informativa –reconocida en el artículo 2.6 de la Constitución implica el control ciudadano sobre su información personal. Un ejemplo paradigmático es la STC N.° 238/2022 (habeas data), donde el Tribunal ordenó al Estado encriptar y eliminar datos de un ciudadano luego de una filtración indebida, vinculando además el "derecho al olvido" con la dignidad personal. Asimismo, la jurisprudencia ha ponderado el derecho de acceso a la información pública frente a la protección de datos sensibles: en la STC N.° 04724-2019/TC, el Tribunal autorizó la entrega de contratos de trabajo tras anonimizar datos sensibles (ingresos, salud, vida sexual), equilibrando el principio de transparencia con la intimidad.

Sin embargo, la implementación efectiva de estos estándares enfrenta retos importantes. Se reflexiona sobre los riesgos que supone la expansión digital del Estado (potenciales brechas de seguridad, uso de datos biométricos y geolocalización, falta de capacitación del personal, brechas presupuestales, etc.) y la tensión con otros fines legítimos, como la transparencia y la eficiencia administrativa. Finalmente, se proponen recomendaciones para fortalecer las instituciones encargadas (Autoridad Nacional de Protección de Datos, Secretaría de Gobierno Digital, etc.), implementar medidas de "privacidad por diseño" en proyectos públicos, designar oficiales de datos en cada entidad y promover una cultura de protección de datos en la administración pública; el análisis busca contribuir al pensamiento crítico desde la perspectiva del derecho y la realidad social.

Palabras clave: Gobierno digital; protección de datos personales; privacidad; transparencia; autodeterminación informativa.

I. Introducción

El gobierno digital implica la adopción de tecnologías de la información y la comunicación (TIC) para mejorar la gestión y los servicios del Estado; en el Perú, este proceso ha sido potenciado por iniciativas como el Decreto de Urgencia N.° 007-2020 (Marco de Confianza Digital) y el Decreto Legislativo N.° 1412 (Ley de Gobierno Digital). Sin embargo, la digitalización masiva de procesos públicos eleva la relevancia de la protección de datos personales, dado que la Administración acumula, procesa y comparte volúmenes crecientes de información ciudadana. En nuestro ordenamiento, el derecho a la intimidad y a la autodeterminación informativa está consagrado en el artículo 2.6 de la Constitución Política del Perú, el cual señala que toda persona tiene derecho a que "los servicios informáticos… no suministren informaciones que afecten la intimidad personal y familiar". Inspirada en ese mandato constitucional, la Ley N.° 29733 (2011) se propuso garantizar el derecho fundamental a la protección de los datos personales mediante un tratamiento adecuado. A su vez, la aprobación del Reglamento (DS N.° 016-2024-JUS, 30 nov. 2024) busca modernizar dicho régimen ante los retos de las tecnologías emergentes.

Este artículo jurídico analiza críticamente el marco normativo vigente sobre protección de datos personales en la administración pública peruana, con especial énfasis en la interacción entre el gobierno digital y los derechos fundamentales. Se examinan los principios constitucionales involucrados (privacidad, transparencia y debido proceso) y la jurisprudencia relevante del Tribunal Constitucional, así como ejemplos prácticos de su aplicación; además, se discuten los desafíos institucionales y tecnológicos que enfrenta el sector público para implementar eficazmente las políticas de protección de datos, reflexionando sobre los riesgos de vulneración de derechos ante la expansión digital del Estado. Finalmente, se esbozan recomendaciones para el fortalecimiento institucional y la incorporación del enfoque de privacidad desde el diseño, todo ello desde un enfoque académico, reflexivo y críticamente orientado.

II. Marco normativo.

La Constitución peruana establece el derecho fundamental a la intimidad y al buen nombre (art. 2, incisos 7 y 5), así como el inc. 6: el derecho "a que los servicios informáticos… no suministren informaciones que afecten la intimidad personal y familiar". Partiendo de este mandato, la Ley N.° 29733, Ley de Protección de Datos Personales, fue promulgada en 2011; el artículo 1 de la Ley dispone que su objeto es "garantizar el derecho fundamental a la protección de los datos personales, previsto en el numeral 6 del artículo 2 de la Constitución". Así, todo tratamiento de datos personales tanto en entidades públicas como privadas debe realizarse con respeto a la dignidad humana y a otros derechos constitucionales.

La Ley 29733 reconoce los derechos de los titulares (Derechos ARCO: Acceso, Rectificación, Cancelación y Oposición) sobre sus datos, y establece obligaciones para los responsables y encargados de los bancos de datos (informar condiciones, adoptar medidas de seguridad, registrarse en el Registro Nacional, etc.). Define además categorías especiales como los "datos sensibles" información sobre salud, origen étnico, opiniones políticas, vida sexual, datos biométricos, entre otros cuya protección demanda mayores garantías. La Autoridad Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia, es el órgano competente para supervisar y sancionar el adecuado cumplimiento de la ley. Esta ley original se complementó con un reglamento aprobado en 2013 (DS N.° 003-2013-JUS), el cual fue derogado por la reciente norma de noviembre de 2024, en línea con la actualización de estándares internacionales.

1. Reglamento de Datos Personales (DS N.° 016-2024-JUS)

El 30 de noviembre de 2024 se publicó el Decreto Supremo N.° 016-2024-JUS que aprueba el Reglamento de la Ley 29733. Esta norma (ratificada por Resolución Ministerial) responde a "los desafíos contemporáneos" de las nuevas tecnologías digitales. El reglamento, de más de 135 artículos, introduce conceptos y obligaciones actualizados. Entre sus innovaciones destacan la ampliación de las definiciones de dato personal (incluyendo localización e identificadores en línea), la inclusión de los datos neuronales

como sensibles, y la precisión del ámbito de aplicación en el territorio nacional. Se incorporan los principios de transparencia y responsabilidad proactiva en el tratamiento (para empoderar al titular y exigir medidas a los responsables); también se reconoce expresamente el derecho a la portabilidad de los datos (art. 76 reglamento) y se establecen mecanismos obligatorios de notificación de incidentes de seguridad tanto a la Autoridad como al titular dentro de plazos estrictos (48 horas).

De particular relevancia para el sector público es la figura del Oficial de Protección de Datos Personales; el nuevo reglamento exige designar un oficial de datos en todas las entidades públicas (y en ciertos supuestos privados) que manejen grandes volúmenes de datos o sensibles, esta figura, prevista inicialmente en el reglamento de la Ley de Gobierno Digital de 2021, ahora se extiende formalmente y deberá implementarse en plazos que dependen del tamaño de la entidad. Además, se refuerzan las obligaciones de seguridad: las entidades deben contar con una política de seguridad de la información documentada y controles de acceso efectivos. El reglamento es de obligatorio cumplimiento desde el 29 de marzo de 2025, con algunos plazos diferidos para la implementación de ciertas disposiciones (portabilidad, oficiales de datos, etc.). En conjunto, este marco normativo actualizado busca alinear al Perú con estándares internacionales (por ejemplo, la existencia de un oficial de protección es común en modelos como la Unión Europea) y fortalecer la capacidad estatal de protección de datos personales.

2. Ley N.° 1412 – Ley de Gobierno Digital

Como parte de la agenda de modernización estatal, el Decreto Legislativo N.° 1412 (“Ley de Gobierno Digital”) estableció en 2009 (y sucesivos reglamentos) un marco de gobernanza para las TIC en la Administración Pública, esta ley define el gobierno digital como el uso estratégico de tecnologías y datos para generar valor público, e introduce principios rectores específicos para la digitalización. En particular, su artículo 5 incluye el principio de “Privacidad desde el diseño” (5.3), que exige que en la concepción y configuración de servicios digitales se adopten medidas preventivas tecnológicas, organizacionales y procedimentales para resguardar la privacidad. Asimismo, el principio de “Nivel de protección adecuado para los datos personales” (5.10) dispone que todo

tratamiento de datos en el entorno de gobierno digital debe hacerse conforme a la Ley de Protección de Datos Personales y su reglamento, de este modo, el enfoque del gobierno digital peruano incorpora expresamente la protección de datos como elemento central de su diseño.

Otros principios del DL 1412 complementan este enfoque: la "Equivalencia Funcional" reconoce garantías digitales equiparables a las tradicionales (seguridad jurídica en servicios en línea), y el principio de "Datos Abiertos por Defecto" prioriza la apertura de información pública "sin comprometer el derecho a la protección de datos personales"; estos lineamientos obligan a las entidades públicas a repensar sus procesos con visión holística de seguridad, interoperabilidad y privacidad. Además, el DL 1412 otorga a la Secretaría de Gobierno Digital de la PCM la rectoría en materia de gobierno, seguridad y datos digitales, de modo que existe un ente rector coordinador con la Autoridad de Datos (Ministerio de Justicia) para armonizar la política digital nacional. Finalmente, cabe mencionar normas complementarias: la Ley N.° 27806 (Transparencia y acceso a la información pública) regula el derecho de toda persona a solicitar datos al Estado, y la Ley del Procedimiento Administrativo (TUO de la Ley N.° 27444) establece garantías de debido proceso en la función pública. Estos cuerpos normativos deben interpretarse en conjunto con la Ley de Protección de Datos, cuidando el equilibrio entre apertura informativa y reserva de datos sensibles.

III. Principios constitucionales y jurisprudencia relevante

1. Derecho a la privacidad y autodeterminación informativa

El derecho a la intimidad y la autodeterminación informativa constituyen pilares del debate sobre datos personales; según el Tribunal Constitucional, la autodeterminación informativa (art. 2.6 CP) es "el derecho que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos". Esto incluye la facultad de verificar la legalidad de la obtención de los datos y exigir que cumplan criterios de veracidad, integridad, utilidad y caducidad. La jurisprudencia confirma que dichos derechos son exigibles tanto contra el sector privado

como contra el Estado: en la STC N.° 238/2022 (Caso Vocati Consulting), el Tribunal declaró fundado un habeas data tras una filtración indebida de datos policiales a un consultor privado. La sentencia ordenó al Estado encriptar permanentemente las bases de datos del Sistema de Registro de Denuncias (SIDPOL) y eliminar los datos del demandante, pues la continuación del archivo de una denuncia (finalmente archivada) ya no era justificable y vulneraba su honor y trabajo.

Este caso destaca dos conceptos clave: por un lado, que el Estado también debe adoptar medidas (tecnológicas y organizativas) para proteger los datos desde su origen; por otro, que el "derecho al olvido" se considera expresión de la autodeterminación informativa; el Tribunal recuerda que el derecho al olvido garantiza la supresión de información personal que, por cambios fácticos o jurídicos, ya no se ajusta a la realidad y perjudica derechos como el honor o la intimidad. En la sentencia se enfatiza que, aunque la filtración fue cometida por una empresa privada, corresponde evaluar la fuente originaria (el SIDPOL) y la responsabilidad estatal en prevenir accesos indebidos.

En síntesis, el TC ha reafirmado que el tratamiento de datos personales (incluso por parte del Estado) debe adecuarse estrictamente a lo establecido en la Constitución y la Ley N.° 29733, bajo pena de vulnerar derechos fundamentales. El reconocimiento judicial de la autodeterminación informativa y del olvido fortalece el énfasis constitucional en la privacidad y exige medidas proactivas (encriptado, eliminación, etc.) por parte de las entidades públicas. Estos desarrollos subrayan la necesidad de que la administración pública incorpore, en su gobierno digital, mecanismos efectivos de protección desde el diseño coincidiendo con lo que dispone el DL 1412 – y promueva el correcto ejercicio de los derechos ARCO de los ciudadanos.

2. Derecho a la información pública y balance con datos sensibles

En paralelo, el derecho constitucional de acceso a la información pública (art. 2.5 CP) impone a las entidades del Estado la obligación de proveer datos a cualquier ciudadano que lo solicite, salvo excepciones legalmente previstas; la ley de transparencia (Ley 27806) y su reglamento confirman este principio de máxima publicidad. Sin embargo, surge un

punto de fricción cuando la información requerida incluye datos personales sensibles. En estos casos, ¿qué prevalece: el interés público en la transparencia o la intimidad del afectado?

El Tribunal Constitucional ha resuelto esta colisión con criterios de ponderación. En la STC N.° 04724-2019-PHD/TC, un sindicato solicitó al Ministerio de Trabajo copias de contratos laborales de una empresa minera. El Ministerio respondió negando la información, aduciendo que los contratos contendrían datos sensibles (ingresos económicos, afiliación sindical) cuya revelación lesionaría la privacidad. El TC confirmó que, en principio, los datos sensibles no son públicos, pero también reconoció la importancia constitucional de la publicidad administrativa. El fallo resolvió que la información debía entregarse "previa anonimización o tachado de los datos sensibles". En otras palabras, el derecho de acceso se satisface mediante la supresión o enmascaramiento de la información confidencial, permitiendo al solicitante obtener datos útiles sin vulnerar la intimidad de terceros.

Esta jurisprudencia ejemplifica la necesidad de equilibrar derechos en la práctica del gobierno digital: no puede haber transparencia absoluta que ponga en riesgo la privacidad de los ciudadanos; a su vez, impone a las entidades públicas la carga de depurar sus bases de datos antes de su divulgación, lo que exige capacidad técnica y normativa claras. Las normas de protección de datos facilitan este enfoque: la Ley 29733 permite el tratamiento (incluida la comunicación) de datos personales cuando se garantice su anonimización. Asimismo, el DS 016-2024-JUS consagra obligaciones de anonimizar datos sensibles en ciertos flujos de información y detalla procedimientos de comunicación entre entidades. En suma, la doctrina constitucional refuerza que la protección de datos y el acceso a la información son valores complementarios que deben armonizarse mediante criterios técnicos y legalmente institucionalizados.

3. Principio del debido proceso y otros estándares constitucionales

El debido proceso es un principio constitucional (art. 139.3 CP) que exige que la actuación estatal se realice conforme a la ley, con garantías de defensa, contradictorio y motivación

en las resoluciones. Su vinculación específica con la protección de datos surge en escenarios en que el uso de información personal impacta procedimientos administrativos o judiciales. Por ejemplo, si un ciudadano es sometido a una sanción administrativa basada en datos recolectados por medios digitales, dicho procedimiento debe respetar el estándar de legalidad y permitirle verificar la fiabilidad de la información que se le imputa. Más aún, las entidades públicas deben contar con marcos normativos claros para el tratamiento de datos en el procedimiento administrativo; de lo contrario, se corre el riesgo de violar el debido proceso. Si bien no existe abundante jurisprudencia en el Perú sobre este cruce, se infiere que cualquier normativa interna de procesos digitales (como puede ser trámites electrónicos) debe garantizar los derechos de defensa y audiencia, así como la protección de la base de datos de prueba.

De igual modo, otros principios constitucionales cobran relevancia: la transparencia en la gestión pública y la eficacia administrativa invitan a que el Estado utilice bien los datos para mejorar servicios. El desafío radica en hacerlo sin sacrificar la legalidad y la privacidad. En definitiva, la protección de datos en el gobierno digital es un reflejo del principio de legalidad: todo tratamiento debe tener respaldo normativo y respeto a los fines perseguidos, evitando el uso inadecuado o arbitrario de la información ciudadana.

IV. Desafíos y riesgos en la práctica

La proliferación de servicios digitales y el incremento en la recolección de datos plantean múltiples riesgos de vulneración de derechos fundamentales en el ámbito público. En primer lugar, existen brechas tecnológicas y de seguridad; la rápida adopción de plataformas electrónicas no siempre va acompañada de inversiones suficientes en seguridad cibernética, casos como el mencionado Sidpol (cuyos datos se filtraron) ilustran cómo sistemas críticos (bases policiales, registros electorales, administrativos) pueden quedar expuestos si no se implementan controles robustos (encriptación, autenticación multifactor, monitoreo de accesos). Adicionalmente, la gestión de incidentes de seguridad es un reto: el nuevo reglamento exige notificación rápida de incidentes, pero las entidades históricamente no han desarrollado protocolos ni cultura de reporte. Es necesario, por tanto,

entrenar al personal en detección y respuesta a vulneraciones, y dotar de recursos a la Autoridad Nacional para recibir y supervisar dichas notificaciones.

En segundo lugar, está el desafío organizacional; muchas instituciones públicas aún operan con sistemas inconexos o papel, la interoperabilidad, meta del gobierno digital, implica compartir datos entre entidades (entre RENIEC, SUNARP, entidades de salud y educación). Sin embargo, este intercambio debe hacerse con cautela: requiere establecer acuerdos técnicos y legales (consentimientos, confidencialidad) y asegurar que sólo personal autorizado acceda a datos sensibles. El Decreto Legislativo 1412 promueve la interoperabilidad digital, pero en la práctica las entidades deben adaptar sus reglamentos internos al reglamento de datos personales y garantizar "privacidad por diseño" desde la fase de desarrollo de cualquier sistema compartidad. Por ahora, existen riesgos de procedimiento de datos cruzados sin control (por ejemplo, dotación de información interinstitucional sin anonimización adecuada), lo que podría vulnerar derechos.

Un tercer riesgo es de carácter normativo y de cumplimiento: la dispersión legislativa puede confundir: además de la Ley de Protección de Datos y su reglamento, las entidades deben observar leyes sectoriales (Salud, Educación, Relaciones Exteriores, etc.), la Ley de Transparencia y la Ley de Procedimiento Administrativo. Cuando éstas entran en colisión, por ejemplo, una norma sectorial que exige publicar datos estadísticos versus la restricción de Ley 29733 se requiere jerarquía y coordinación jurídica, algo que no siempre ocurre de manera fluida. Por otro lado, la implementación de los nuevos requisitos (p.ej. designación de oficiales de datos) representa una carga administrativa adicional, que muchas veces cae en el personal de oficina de partes o en direcciones de sistemas de información sin claro soporte presupuestal; esto impone la necesidad de actualizar el Reglamento de Organización y Funciones de cada entidad (para incluir estas responsabilidades) y de asignar recursos humanos calificados.

Finalmente, se presenta una tensión sociopolítica: la ciudadanía espera eficiencia y apertura de datos en la era digital, pero al mismo tiempo teme el mal uso de su información (vigilancia masiva, robo de identidad). Por ejemplo, la implementación de la identidad digital nacional (DNI electrónico) o de sistemas biométricos en programas sociales ha

generado debate sobre la privacidad; sin conciencia y transparencia, estos proyectos pueden acentuar la desconfianza ciudadana, asimismo, la pandemia de COVID-19 evidenció problemas: se crearon sistemas de teletrabajo y atención virtual expeditos, pero sin evaluar plenamente los riesgos de seguridad e intrusión en datos de salud o laborales.

En resumen, la expansión digital del Estado es un fenómeno irreversible, pero para que sea legítima debe incorporar desde su génesis los salvaguardas legales y técnicos adecuados. Los riesgos de vulneración como hackeos, excesos en recolección de datos, decisiones automatizadas sin supervision son reales y deben abordarse con políticas integrales que incluyan no solo leyes, sino presupuesto, formación y mecanismos de vigilancia interna.

V. Recomendaciones para el fortalecimiento institucional

Frente a los retos identificados, es imprescindible adoptar medidas concretas que fortalezcan la protección de datos en la administración pública:

Fortalecer la Autoridad Nacional de Protección de Datos Personales: dotarla de recursos financieros y tecnológicos para fiscalizar efectivamente las entidades públicas; esto implica incrementar su capacidad de inspección y sanción, así como su vinculación con organismos internacionales (por ejemplo, participar en redes globales de privacidad), asimismo, se recomienda que el informe anual de actividades de la Autoridad (que debe remitir al Ministerio de Justicia) incluya indicadores de cumplimiento gubernamental.

Implementar Oficiales de Protección de Datos (ODP): asegurar que todas las entidades cumplan con la obligatoriedad de designar un ODP antes del plazo máximo previsto. Estos oficiales deben ser capacitados formalmente y contar con independencia en su función; también convendría elaborar lineamientos nacionales que especifiquen las funciones del ODP público, tomando en cuenta las directrices de la PCM sobre transformación digital. La coordinación entre los ODP de diferentes entidades (por ejemplo, a través de una red interinstitucional) podría favorecer buenas prácticas compartidas.

Cultura y capacitación: es esencial formar a los servidores públicos en materia de privacidad y seguridad de la información; esto incluye talleres sobre tratamiento legítimo

de datos, derechos ARCO, uso seguro de plataformas digitales y procedimientos para reporte de incidentes; asimismo, se deben promover campañas de difusión ciudadanas que informen a la población sobre sus derechos de protección de datos y los canales para reclamar ante la Autoridad. El desconocimiento de la ley suele ser un obstáculo tanto para la exigencia de derechos como para el cumplimiento de deberes.

Privacidad por diseño y evaluaciones de impacto: toda nueva aplicación o servicio digital del Estado debe incorporar desde su concepción medidas de seguridad y minimización de datos, sería recomendable institucionalizar la práctica de Evaluaciones de Impacto en Privacidad (DPIA) previo al lanzamiento de sistemas que procesen datos personales sensibles o masivos. Estas evaluaciones, que incluyen la participación de la Autoridad o de expertos independientes, ayudarán a identificar riesgos y mitigaciones antes de afectar a los ciudadanos.

Mejorar la seguridad de los sistemas y los procedimientos de gestión de incidentes: actualizar y unificar políticas de seguridad de la información en las entidades; promover certificaciones de seguridad (como ISO 27001) en sistemas crítico, implementar monitoreo continuo de redes. Además, se debe establecer un canal único de notificación de brechas a la Autoridad, con flujos claros de información y sanciones por reporte tardío o inadecuado.

Políticas de transparencia equilibradas: revisitar normas internas para garantizar que la entrega de información pública siempre considere la anonimización de datos sensibles; las disposiciones del TC (como la anonimización previa) deberían incorporarse como protocolos estándar en las unidades de transparencia de cada entidad. Así se evita la discrecionalidad administrativa y se protege a los afectados, fomentando al mismo tiempo el acceso al resto de la información.

Coordinación interinstitucional: fortalecer la sinergia entre la Secretaría de Gobierno Digital (PCM), el Ministerio de Justicia (Autoridad de Datos), la Autoridad Nacional de Transparencia y otras entidades rectoras. Por ejemplo, crear mesas de trabajo periódicas donde se analicen casos de protección de datos en proyectos de Gobierno Digital.

Igualmente, alinear los planes de trabajo de la Autoridad con los objetivos del Plan de Gobierno Digital nacional.

Adecuación normativa continua: si bien hay cierto intento de modernizar el marco, es necesario monitorear su impacto y prever ajustes legislativos futuros; en el contexto del gobierno digital, podrían necesitarse enmiendas que especifiquen, por ejemplo, el uso de algoritmos en la función pública, el manejo de inteligencia artificial que procesa datos personales, o regulaciones sectoriales específicas (salud, educación) coherentes con la ley general.

En síntesis, el cumplimiento efectivo de la protección de datos en el ámbito público requiere más que leyes; exige un compromiso institucional integral. Las recomendaciones apuntan a convertir los principios jurídicos en prácticas administrativas y tecnológicas tangibles. Solo así se podrá asegurar que la expansión digital del Estado se traduzca en mejoras reales para los ciudadanos, sin comprometer nuestros derechos fundamentales.

VI. Conclusiones

La expansión del gobierno digital en el Perú presenta una oportunidad histórica para mejorar la gestión pública, pero simultáneamente conlleva desafíos significativos en la protección de los datos personales; el análisis doctrinario desarrollado evidencia que el país dispone ya de un marco normativo sólido integrado por la Constitución, la Ley 29733 y su reciente reglamento, así como la Ley de Gobierno Digital que articula la protección de datos con los principios constitucionales de privacidad y transparencia. La jurisprudencia del Tribunal Constitucional ha avanzado en la interpretación de estos derechos, subrayando la responsabilidad estatal en garantizar la intimidad de la información y estableciendo criterios claros de equilibrio con la publicidad informativa.

No obstante, quedan brechas en la aplicación práctica de estas normas; la vulnerabilidad de los sistemas informáticos públicos, la fragmentación institucional y la falta de recursos humanos especializados son obstáculos reales que pueden traducirse en vulneraciones de derechos, como ejemplifica el caso del SIDPOL. Por ello, el reto es convertir la regulación en realidad cotidiana: incorporando evaluaciones de impacto en cada proyecto digital,

formando al personal en protección de datos y asignando un peso efectivo a la privacidad desde la fase de planificación de iniciativas tecnológicas.

En conclusion, la protección de datos personales en la era del gobierno digital no debe verse como un mero cumplimiento formal, sino como un elemento esencial de legitimidad estatal. Un gobierno confiable es aquel que no solo ofrece servicios en línea, sino que también garantiza que la expansión digital no erosione los derechos fundamentales de las personas; en ese sentido, las recomendaciones aquí expuestas aspiran a contribuir al fortalecimiento institucional necesario, promoviendo un Estado moderno y, al mismo tiempo, respetuoso del derecho a la intimidad y a la información de sus ciudadanos.

VII. Bibliografía

Castillo Córdova, H. (2021). Derechos fundamentales en la era digital. Palestra Editores.

https://www.researchgate.net/publication/371161336_Derechos_fundamentales_en_la_era_digital

Congreso de la República del Perú. (1993). Constitución Política del Perú. Diario Oficial El Peruano.

https://www.leyes.congreso.gob.pe/documentos/constituciones_ordenado/constit_1993/texto_actualizado_cons_1993.pdf

Congreso de la República del Perú. (2002). Ley N.º 27806: Ley de Transparencia y Acceso a la Información Pública. Diario Oficial El Peruano.

https://www.minjus.gob.pe/wp-content/uploads/2020/03/ley27806.pdf

Congreso de la República del Perú. (2011). Ley N.º 29733: Ley de Protección de Datos Personales. Diario Oficial El Peruano.

https://www.leyes.congreso.gob.pe/documentos/leyes/29733.pdf

Ministerio de Justicia y Derechos Humanos. (2024). Decreto Supremo N.º 016-2024-JUS que aprueba el Reglamento de la Ley N.º 29733. Diario Oficial El Peruano.

https://www.gob.pe/institucion/anpd/normas-legales/6554453-n-016-2024-jus

Naciones Unidas, Consejo de Derechos Humanos. (2022). Informe del Relator Especial sobre el Derecho a la Privacidad en la Era Digital (A/HRC/49/55).

https://undocs.org/es/A/HRC/49/55

Organización para la Cooperación y el Desarrollo Económicos. (2019). Recomendación del Consejo sobre Gobernanza de Datos del Sector Público.

https://www.oecd.org/gov/oecd-recommendation-on-public-sector-data-governance.ht

Presidencia del Consejo de Ministros. (2018). Decreto Legislativo N.º 1412: Ley de Gobierno Digital. Diario Oficial El Peruano.

https://sgd.gob.pe/normas

Presidencia del Consejo de Ministros. (2023). Texto Único Ordenado de la Ley N.º 27444: Ley del Procedimiento Administrativo General. Diario Oficial El Peruano.

https://www.servir.gob.pe/media/13102/ley-27444-tuo-2023.pdf

Tribunal Constitucional del Perú. (2019). Exp. N.º 04724-2019-PHD/TC. Sentencia sobre acceso a contratos laborales y anonimización de datos.

https://magazinjurisprudencial.com/el-sindicato-puede-solicitar-al-ministerio-de-trabajo-los-contratos-de-trabajo-presentados-por-el-empleador-exp-n-04724-2019-phd-tc/