

## **PRINCIPALES DESAFÍOS DEL DERECHO A LA PRIVACIDAD Y OTROS DERECHOS HUMANOS EN LA ERA DIGITAL**

### **1. Las Tecnologías de la Información y Comunicación (TIC) en el Estado peruano**

Los avances tecnológicos en materia de información y comunicación, propios de la actualidad, exigen que el Estado adecue sus procedimientos y políticas en orden de favorecer la participación de la ciudadanía en la administración de la cosa pública y la gestión estatal.

En tal sentido, el Perú inició una serie de acciones de reforma con el objeto de instituir el gobierno electrónico, partiendo de la Declaración de Florianópolis hasta la instauración de la Secretaría de Gobierno Digital (SeGDi), en el año 2017.

La Secretaría de Gobierno Digital, creada mediante Decreto Supremo N° 022-2017-PCM, tiene competencia para formular y proponer políticas nacionales o sectoriales, planes, normas, licenciamientos y estrategias en materia informática y gobierno electrónico. Asimismo, cumple con la función de ser el órgano rector del Sistema Nacional de Informática.

En ese sentido, la implementación de un organismo rector en materia informática no solo contribuye a mejorar el uso de las tecnologías en el ámbito estructural, sino que plantea un nuevo escenario donde los derechos fundamentales requieren de una especial atención para que puedan ser ejercidos a través de espacios digitales.

Así, el derecho a la libertad de expresión y la protección de datos personales revisten en general de una vital importancia para garantizar la efectividad de los servicios públicos, la transparencia y la vigencia de los demás derechos en estos tiempos.

### **2. Libertad de expresión en la era digital**

La libertad de expresión supone el derecho de cada individuo de poder difundir libremente sus ideas, opiniones y hechos de toda índole a través de cualquier medio, sino también implica que la sociedad pueda conocer opiniones ajenas y acceder a todo tipo de información<sup>1</sup>.

Así lo ha resaltado la Corte Interamericana de Derechos Humanos al afirmar que «[para] el ciudadano común tiene tanta importancia el conocimiento de la opinión ajena o de la información de que disponen otros como el derecho a difundir la propia»<sup>2</sup>.

---

<sup>1</sup> Cfr. CORTE INTERAMERICANA DE DERECHOS HUMANOS (1985). Opinión consultiva OC-5/85. La Colegiación Obligatoria de Periodistas (Arts. 13 y 29 Convención Americana sobre Derechos Humanos), párr. 30.

<sup>2</sup> Ídem. Párrafo 32.

Por tal motivo, el Estado debe garantizar el ejercicio irrestricto de tales libertades, sea omitiendo acciones que supongan su restricción arbitraria o adoptando medidas que coadyuven con el referido fin.

En esa línea, se debe poner de relieve la importancia que ha tenido el internet en la vida de los seres humanos y, en particular, en el ejercicio de las libertades comunicativas, dado que ha servido como instrumento de comunicación instantáneo y de bajo costo, y como medio de difusión de información e ideas<sup>3</sup>.

Los rasgos esenciales del internet lo han convertido en un instrumento que permite que el ejercicio de la libertad de expresión e información se lleve a cabo de manera plural, democrática, abierta y expansiva<sup>4</sup>; siendo necesario preservar su estructura original para el goce de las mencionadas libertades comunicativas<sup>5</sup>.

Es por ello que la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos consideró que las políticas públicas o regulaciones sobre la materia que impulse el Estado deben encontrarse debidamente orientadas a partir de principios tales como:

- Acceso
- Pluralismo
- No discriminación
- Privacidad
- Neutralidad de red

En el caso peruano, se proyectó al 2021, a propósito de la celebración del Bicentenario de nuestra independencia, el cumplimiento de metas y programas estratégicos a ser cumplidos a largo plazo, los mismos que fueron recogidos en el denominado Plan Estratégico de Desarrollo Nacional Plan Bicentenario: El Perú hacia el 2021<sup>6</sup>, el cual fue presentado por el Centro Nacional de Planeamiento Estratégico – CEPLAN.

En el marco de lo dispuesto en dicho plan, y en atención al impacto que supone el uso del internet en el ejercicio de los derechos a la libertad de expresión e información, el Estado estableció como objetivo nacional, entre otros, que las personas tengan acceso equitativo a servicios básicos de calidad. Por tal motivo, se fijaron políticas orientadas a la capacitación de los estudiantes en el uso de las Tecnologías de la Información y Comunicación (TIC)<sup>7</sup>, así como también a la promoción de la inversión pública y privada para mejorar el acceso de la ciudadanía - en particular de quienes se encuentren en situación de pobreza y pobreza extrema - a los servicios de telecomunicaciones<sup>8</sup>.

---

<sup>3</sup> Cfr. ASAMBLEA GENERAL DE NACIONES UNIDAS. Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión. A/66/290. 10 de agosto de 2011, párrafo. 10.

<sup>4</sup> Cfr. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2013). Libertad de expresión e internet. OEA/Ser L/V/II. CIDH/RELE/INF. 11/13. 31 diciembre 2013. Párrafo. 12.

<sup>5</sup> *Ídem.*, párrafos 13 y 14.

<sup>6</sup> Aprobado mediante Decreto Supremo N° 054-2011-PCM

<sup>7</sup> Centro Nacional de Planeamiento Estratégico - CEPLAN (2011). *Plan bicentenario: El Perú hacia el 2021*. Prime9ra Edición. Lima. p. 93

<sup>8</sup> *Ídem.*, p. 94.

Asimismo, como parte del eje estratégico Estado y Gobernabilidad, se advirtió la necesidad de contar con una función pública democrática, transparente y participativa, por lo que se propuso contar en la toma de decisiones públicas con una participación ciudadana eficiente y en igualdad de condiciones, considerando principalmente como medida el ejercicio de la libertad de expresión y de prensa<sup>9</sup>.

La necesidad que la sociedad peruana se beneficie en toda su plenitud del uso de las TIC se abordó también en el 2006. En ese año se publicó<sup>10</sup> el «Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 1.0», el cual fue actualizado en el 2011,<sup>11</sup> siendo denominado «Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0», a través de los cuales se plantea una serie de objetivos y estrategias, tales como:

- Asegurar el acceso inclusivo de la ciudadanía en áreas rurales y urbanas a la sociedad de la información, siendo necesario para ello contar con redes dorsales de fibra óptica, desarrollar conectividad en zonas no atendidas, entre otros.
- Fomentar a través de medidas concretas el desarrollo de competencias para que la ciudadanía participe en la sociedad de la información y el conocimiento.
- Garantizar oportunidades de uso de las TIC que permitan alcanzar un desarrollo más inclusivo de la sociedad.
- Fomentar la investigación y el desarrollo sobre las tecnologías de la información y comunicación para su uso teniendo en consideración prioridades de la nación.
- Intensificar la producción de bienes y servicios, así como la competitividad mediante el desarrollo y aplicación de las TIC
- Promover el crecimiento de la industria de las tecnologías de la información y comunicación en el país.
- Brindar, desde la administración pública, servicios de calidad a la ciudadanía.
- Asegurar que los planes nacionales, regionales y locales contemplen lo previsto en la Agenda Digital Peruana 2.0.

Debemos destacar que, con el fin de verificar el cumplimiento del mencionado plan, se creó la Comisión Multisectorial Permanente – CODESI<sup>12</sup>.

Como se advierte, uno de los objetivos a cumplir por el Estado de cara al 2021, es permitir a la población, en especial quienes se encuentran en situación de pobreza, tener acceso a servicios de telecomunicaciones, contribuyendo a concretizar los derechos a las libertades de expresión e información.

---

<sup>9</sup> *Óp. Cit.* Centro Nacional de Planeamiento Estratégico - CEPLAN (2011). pp. 121 – 125.

<sup>10</sup> Plan publicado el 21 de junio de 2006 mediante Decreto Supremo N°031-2006-PCM.

<sup>11</sup> A través del Decreto Supremo N°066-2011-PCM, publicado el 27 de julio de 2011.

<sup>12</sup> Dicha comisión fue creada mediante Decreto Supremo N°065-2015-PCM, norma publicada en setiembre de 2015.

Ahora bien, teniendo en consideración los planes hasta ahora mencionados, debemos precisar las normas que buscan regular aspectos vinculados al ejercicio de las libertades comunicativas en internet, como normas referidas a la accesibilidad en la red o sobre el control de contenidos e infraestructura.

<b>MARCO LEGISLATIVO PERUANO EN MATERIA DE LIBERTAD DE EXPRESIÓN E INFORMACIÓN</b>				
<b>Norma y año de publicación<sup>13</sup></b>	<b>Tipo</b>	<b>Descripción</b>	<b>Reglamento</b>	<b>Vigencia</b>
Ley N°28530 «Ley de promoción de acceso a internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de internet», publicada el 25 de mayo del 2005.	Accesibilidad	Tiene por objeto garantizar el acceso al uso de internet y a las tecnologías de la información a las personas con discapacidad.  Para tal propósito, prevé la adopción de políticas que busquen promover y capacitar a dichas personas en materias relacionadas con el uso del internet.  Promueve la adecuación de portales y páginas web de entidades públicas y de privados que presten servicios de información al consumidor para facilitar el acceso al internet de las personas con discapacidad, entre otras medidas.	Decreto Supremo N°13-2009-MINDES, aprobado en el 2009.	Vigente
Reglamento de Neutralidad de red aprobado mediante Resolución de Consejo Directivo N°165-2016-CD/OSIPTEL, publicado el 26 de diciembre del 2016.		A través del presente reglamento, el mismo que fue emitido en el marco de lo dispuesto en la Ley N°29904 «Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica», se han fijado principios a fin de garantizar el respeto por la neutralidad de la red. Asimismo, se han dispuesto medidas de diversa índole y se han determinado infracciones y sanciones referentes a la neutralidad de red.		
Ley N°28119, «Ley que prohíbe el acceso de menores de		Tiene por objeto prohibir que menores de edad accedan a páginas web o a cualquier otra forma de comunicación en red de contenido o		Vigente

<sup>13</sup> Las publicaciones son efectuadas en el diario Oficial El Peruano.

<p>edad a páginas web de contenido pornográfico y a cualquier otra forma de comunicación en red de igual contenido, en las cabinas públicas de internet», publicada el 13 de diciembre del 2003, y modificada posteriormente en el 2007 por la Ley N°29139.</p>	<p>Control de contenidos</p>	<p>información pornográfica.</p> <p>Para tal propósito, dispone la instalación de software especiales de filtro o bloqueo.</p> <p>Esta ley es aplicable para todo establecimiento que brinde servicio de cabinas públicas de internet u otra forma de comunicación a través de la red.</p>	<p>Decreto Supremo N°025-2010-ED, aprobado en el 2010.</p>	
<p>Decreto Supremo N°034-2010-MTC, publicado en el 2010.</p>		<p>Establece como Política Nacional la Implementación de una red dorsal de fibra óptica para facilitar a la población el acceso a Internet de banda ancha y promover la competencia en la prestación de este servicio.</p>	<p>-----</p>	<p>Vigente</p>
<p>Ley N°29904, «Ley de promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica», publicada el 20 de julio del 2012.</p>	<p>Infraestructura</p>	<p>Tiene por objeto impulsar el desarrollo de la banda ancha en todo el país, para lo cual se prevé el despliegue de infraestructura, servicios, contenidos y aplicaciones, lo cual coadyuvara con la inclusión social.</p> <p>Es necesario precisar, que a través de dicha ley se reconoce como política de Estado el contar con una Red Dorsal Nacional de Fibra óptica, ello con la finalidad de facilitar el acceso a la banda ancha, siendo responsable de su implementación el Ministerio de Transportes y Comunicaciones.</p>	<p>Decreto Supremo N°014-2013-MTC</p>	<p>Vigente</p>
<p>Resolución Ministerial</p>		<p>Norma que dispone la publicación de Proyecto de</p>		

N°1134-2017-MTC-01.03, publicado en noviembre de 2017.		Decreto Supremo que aprueba la Política Nacional de Banda Ancha y Tecnologías de la Información y la Comunicación (TIC), en el portal institucional del Ministerio	-----	
--	--	--	-------	--

Si bien recientemente se ha establecido un marco normativo referido a la neutralidad de red, es necesario que se generen espacios en los que el Estado promueva la discusión sobre la referida temática y así proscribir todo acto de discriminación que se pueda presentar sobre el particular.

Del mismo modo, se debe indicar que no se han advertido acciones concretas que conlleven a la promoción del acceso al internet de las personas con discapacidad.

De otro lado, es importante y necesario contar con plataformas plurales en los que se pueda discutir sobre las acciones que el Estado y la sociedad puedan adoptar frente a aspectos que no están protegidos por la libertad de expresión y que se manifiestan a través de la red, tales como propaganda de guerra, pornografía infantil, discursos de odio, injuria, entre otros.

Al respecto, debemos poner de relieve las recomendaciones brindadas por la Relatoría Especial para la Libertad de Expresión a los estados miembros de la Organización de Estados Americanos, a través del Informe Anual aprobado en el 2017 por la Comisión Interamericana de Derechos Humanos:

- El marco normativo que se aplique al internet debe atender a las particularidades de este y deben estar conformes a los estándares internacionales referidos a la libertad de expresión, por lo que se debe proscribir toda reglamentación que haya sido desarrollada para otros medios de comunicación.
- Se debe promover la autorregulación como instrumento necesario para afrontar las expresiones injuriosas que se emitan en la red.
- Es necesario que el Estado, respecto a la responsabilidad por los contenidos generados por terceros, brinde protección a quienes participen como intermediarios de internet y brinden servicios técnicos.
- Para garantizar el goce efectivo del derecho a la libertad de expresión a través de internet, es necesario impulsar el acceso universal a este.
- En atención al principio de neutralidad de red, se debe proscribir todo acto de discriminación respecto del tratamiento de datos y el tráfico de internet.

### 3. Transparencia y privacidad en el Gobierno Abierto

La Sociedad de Gobierno Abierto (*Open Government Partnership*) es una iniciativa multilateral que se funda en tres grandes pilares: transparencia, participación y colaboración, y tiene como objetivos mejorar los niveles de transparencia mediante la apertura de datos que permita a la administración pública rendir cuentas y a la ciudadanía ejercer un adecuado control social, así

como permitir su participación en el diseño e implementación de las políticas públicas, favoreciendo de esta manera espacios de colaboración entre las entidades públicas y la sociedad civil<sup>14</sup>.

Dichos esfuerzos se enmarcan en el propósito de fortalecer los sistemas democráticos, afianzar la confianza de la ciudadanía en la administración pública, potenciar la participación y mejorar la calidad, eficacia y eficiencia de los servicios públicos y los gobiernos.

El Perú pertenece a la «Alianza para el Gobierno Abierto», la cual representa una iniciativa internacional voluntaria y multisectorial encargada de promover la transparencia y las buenas prácticas gubernamentales en materia de acceso a la información pública que busca empoderar a los ciudadanos como actores concedores y fiscalizadores de la gestión pública.

Entre los principios de la Alianza resaltan el de transparencia y acceso a la información pública, rendición de cuentas, participación ciudadana y tecnología e innovación. Ello porque los gobiernos reconocen la necesidad e importancia de proveer un acceso abierto a la tecnología para garantizar una ciudadanía informada al momento de la toma de decisiones sobre asuntos de relevancia pública.

### **3.1. Acceso a la información pública en el Gobierno Abierto:**

El acceso a información pública a través de internet fomenta la participación de los ciudadanos en los procesos de decisión de un Estado democrático. Por sus características, el internet permite aumentar la cantidad de información públicamente disponible, difundirla masivamente y a bajo costo, y publicarla en forma dinámica, permitiendo que se trabaje con y sobre ella<sup>15</sup>. De esa manera, los ciudadanos pueden acceder a internet para extraer los datos e información relevante para ellos, en lugar de utilizar la información que se construye en torno a las necesidades de la burocracia<sup>16</sup>.

En el «Plan de Acción de la Alianza para el Gobierno Abierto», el Estado peruano ha asumido una serie de compromisos basados en las cuatro áreas propuestas por la Alianza:

---

<sup>14</sup> REPORTE DE CUMPLIMIENTO PLAN DE ACCIÓN DE GOBIERNO ABIERTO DEL PERÚ. Septiembre de 2013. Disponible «<http://sgp.pcm.gob.pe/wp-content/uploads/2017/10/Mesa-Nacional-de-Gobierno-Abierto-Proceso-de-co-creacion-Plan-AGA.pdf>». Consultado: 04 de abril de 2018.

<sup>15</sup> ORGANIZACIÓN DE LOS ESTADOS UNIDOS. Relator Especial de las Naciones Unidas sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (OEA). *Declaración Conjunta Declaración Conjunta sobre Acceso a la Información y sobre la Legislación que Regula el Secreto*. 6 de diciembre de 2004. Ver, además, Cumbre Mundial sobre la Sociedad de la Información. *Compromiso de Túnez*. Doc. WSIS-05/TUNIS/DOC/7-S. 28 de junio de 2006, párr. 11.

<sup>16</sup> LANZA, Edison. Relator Especial para la Libertad de Expresión Relatoría Especial de Libertad de Expresión. Informe Anual 2016. Página 454

- Mejorar los niveles de transparencia y acceso a la información pública, mediante la revisión de la normativa vigente y el seguimiento a su cumplimiento. En cuanto a la Transparencia activa, se debe garantizar la operatividad de los Portales de Transparencia Estándar y respecto a la Transparencia pasiva, se debe mejorar los mecanismos de acceso a la información, capacitando y sensibilizando a los funcionarios y ciudadanos en la importancia de garantizar este derecho.
- Fortalecer los espacios de participación, concertación y fiscalización y los mecanismos de rendición de cuentas en todos los niveles de gobierno, cobra importancia en la utilización de tecnologías de la información para recoger opiniones y sugerencias de la ciudadanía, así como para devolverle a esta información relevante.
- Garantizar un servicio civil moderno e íntegro, sistemas de adquisiciones y contrataciones blindadas contra la corrupción y un control efectivo y disuasivo, y
- Gobierno electrónico y mejoras en la calidad de los servicios públicos, en especial aquellos dirigidos a los sectores de la población que viven en condiciones de pobreza, y garantizar mecanismos de información y denuncias para monitorear su desempeño.

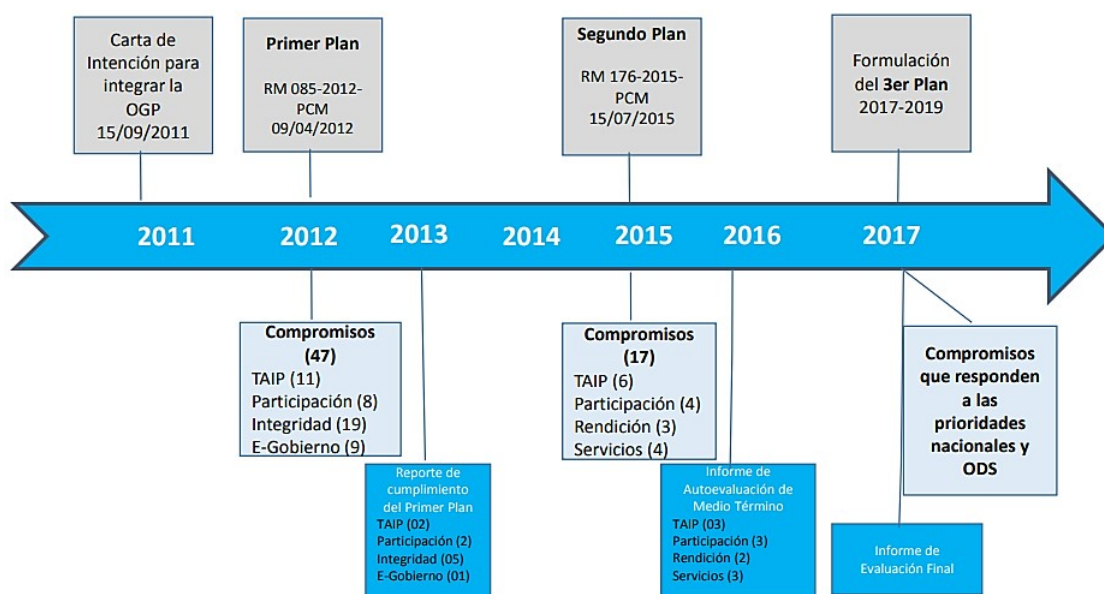
Cabe señalar que el «Plan de Alianza de Gobierno Abierto» se ha ido implementado desde el 2011, conforme a las fases que se exponen en la siguiente línea de tiempo<sup>17</sup>:

---

<sup>17</sup> Gráfico tomado del Plan de Acción de Gobierno Abierto 2017 – 2019. Disponible: «<http://sgp.pcm.gob.pe/wp-content/uploads/2017/09/Talleres-Plan-AGA-2017-2019.pdf>». Consultado: 04 de abril de 2018.



## Línea de Tiempo del Plan AGA



En cuanto a la formulación del «III Plan de Acción para Gobierno Abierto» para el periodo 2017 – 2019, se pueden destacar los siguientes compromisos asumidos en materia de transparencia y acceso a la información pública:

- **Revisar y mejorar el marco normativo en materia de transparencia y acceso a la información pública:** Para ello se requiere la sinergia de las entidades públicas y de la sociedad civil.
- **Fortalecer la institucionalidad sobre Transparencia y Acceso a la Información Pública:** Evaluar si las entidades han designado a los funcionarios responsables del acceso a la información pública en el Manual de Organización y Funciones (MOF) y han regulado los procedimientos de atención de solicitudes en el Texto Único de Procedimientos Administrativos (TUPA).

Monitorear los procesos de hábeas data contra las entidades de la administración y la ejecución de las sentencias.

- **Desarrollar instrumentos para incrementar la transparencia y acceso a la información:** Incorporar en sus instrumentos de gestión cualquier tipo de actividad que contribuya al cumplimiento de la normativa de transparencia y acceso a la información pública y deben estar conforme con las políticas en la materia.

Monitorear la operatividad de los Portales de Transparencia estándar y otros mecanismos que hacen uso de tecnologías de la información.

Asimismo, la agenda nacional del Gobierno Abierto ha planteado diferentes objetivos en distintos sectores que –a través de la tecnología de la información-

permita un acercamiento de los ciudadanos al Estado, mejora de los servicios y transparentar los actos del Estado, evitando la corrupción.

PRIORIDADES GUBERNAMENTALES	OBJETIVOS RELACIONADOS A TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA
Propuesta de compromisos en Educación	2. Desarrollo de un sistema con interfaces de voz para la traducción en idioma originario que facilite el acceso a la información
Propuesta de compromisos en Seguridad Ciudadana	2. Generación de información estructurada sobre delitos patrimoniales, delitos sexuales, homicidios para fines de análisis, difusión de estadísticas y toma de decisiones para reducir la victimización (Poder Ejecutivo y Judicial)
Propuesta de compromisos en Salud	2. Establecer estándares que faciliten el acceso a la información en materia de salud: Avanzar en la interoperabilidad, mediante un Registro Nacional de Información del Sector Salud (RNISS) y procedimientos e instructivos que faciliten el acceso a éste a través de la Estrategia digital de datos abiertos.

En el plano normativo, no puede evidenciarse un avance significativo o una regulación específica sobre la materia, pues solo se han expedido normas genéricas respecto al ejercicio del derecho de acceso a la información:

- **Ley de Transparencia y Acceso a la Información Pública - Ley N° 27806 (2002):** Tiene por finalidad promover la transparencia de los actos del Estado y regular el derecho fundamental del acceso a la información consagrado en el numeral 5 del Artículo 2 de la Constitución Política del Perú y sus preceptos son aplicables a todas las entidades de la Administración Pública y a las personas jurídicas sujetas al régimen privado descritas en el inciso 8) del Artículo I del Título Preliminar de la Ley N° 27444 que gestionen servicios públicos o ejerzan funciones administrativas del sector público bajo cualquier modalidad.
- **Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública - Decreto Supremo N° 043-2003-PCM (2003):** Todas las actividades y disposiciones de las entidades comprendidas en la Ley están sometidas al principio de publicidad. Esta normatividad regula la Transparencia activa (Portales de Transparencia Estándar) o Transparencia pasiva, atención de solicitudes de acceso a la información pública.
- **Reglamento de la Ley de Transparencia - Decreto Supremo N° 072-2003-PCM (2003) y modificatoria - Decreto Supremo N° 070-2013-PCM (2013):** Aplicable a las entidades de la administración pública señaladas en el artículo 2° de la Ley. Asimismo, en lo que respecta al procedimiento de acceso a la información y a las empresas del Estado. No regula aquellos procedimientos para la obtención de copias de documentos que la Ley haya previsto como parte de las funciones de las Entidades y que se encuentren contenidos en su Texto Único de Procedimientos Administrativos.

- **Decreto Legislativo N° 1353 (2017):** Crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y busca fortalecer el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses. Las normas contenidas en dicho Decreto Legislativo son aplicables a todas las entidades públicas y así como a las empresas del Estado, personas naturales y jurídicas de derecho privado, en lo que corresponda; y a las personas comprendidas en la Ley N° 29733, Ley de Protección de Datos Personales.
- **Decreto Supremo N° 019-2017-JUS (2017):** Este Reglamento desarrolla las disposiciones establecidas en el Reglamento del Decreto Legislativo N° 1353 y modifica la aplicación y ejecución de los procedimientos establecidos en la Ley N° 27806, Ley N° 29733 y el Decreto Supremo N° 070-2013-PCM. Además, se establece que el contenido de los correos electrónicos o aplicaciones de mensajería electrónica de los funcionarios públicos no son de acceso público.

Finalmente, es importante precisar que mediante el Decreto Legislativo N° 1088 se creó y reguló la organización y funcionamiento del Sistema Nacional de Planeamiento Estratégico y del Centro Nacional de Planeamiento Estratégico (CEPLAN), que tiene como finalidad la planificación estratégica como instrumento técnico de gobierno y gestión para el desarrollo armónico y sostenido del país.

El CEPLAN presentó el «Plan Estratégico de Desarrollo Nacional Bicentenario 2021», el cual contiene los lineamientos de política, las prioridades, los objetivos, las metas y la definición de las acciones de orden estratégicos para el desarrollo armónico y sostenido del país.

Tal como se ha indicado, este documento pretende generar un impacto positivo en la reducción de las brechas de acceso a la información, incluso de los sectores de bajos ingresos de los países en vías de desarrollo, que permitirá nuevas oportunidades de negocios y de desarrollo para más peruanos y peruanas.

Es por ello, que el Plan Bicentenario incluye entre los objetivos y lineamientos correspondientes al eje estratégico «Estado y Gobernabilidad»<sup>18</sup>, el afianzamiento de la transparencia y la rendición de cuentas. Para lograr estos objetivos es básico fortalecer la conectividad, a través del acceso a internet, y políticas de telecomunicaciones en condiciones de mayor calidad y menores tarifas a los sectores mayoritarios del país.

### **3.2. Protección de Datos Personales ante el avance de la tecnología:**

Tanto las empresas públicas como privadas cuentan con bancos de datos personales que los ciudadanos proporcionan. Por ello, con el fin de proteger la información que pueda considerarse personales o sensibles, se ha establecido un marco legal que regula el almacenamiento, tratamiento, seguridad y transferencia

---

<sup>18</sup> CEPLAN. Plan Estratégico de Desarrollo Nacional Actualizado. Perú hacia el 2021. Lima: Centro Nacional de Planeamiento Estratégico, 2016, pág. 117.

datos personales, cuya disponibilidad facilita el desarrollo de otros derechos, pero amenaza la vigencia y el pleno ejercicio del derecho a la vida privada en línea<sup>19</sup>.

Los datos personales requieren estándares más severos de protección; puesto que el desarrollo de internet potencia y simplifica las comunicaciones y el almacenamiento y sistematización de datos, pero también simplifica y potencia la habilidad de Estados y particulares de monitoreo, interceptación y vigilancia que constituyen serios riesgos a la vida privada de las personas<sup>20</sup>.

Atendiendo a esta problemática, el Estado peruano ha ido expidiendo diversas normas – de carácter nacional o sectorial –, conforme se detallan a continuación:

- **Ley de Protección de Datos Personales – Ley N° 29733 (2011)**: Tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2.6 de la Constitución Política. Incluye los principios que debe orientar el tratamiento de los datos personales contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Regula también los alcances, limitaciones y seguridad del flujo de datos de y los derechos de los titulares de los datos personales
- **Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información - Ley N° 27489 (2001)**: Regula el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, confidencialidad y uso apropiado de dicha información.
- **Norma que regula el uso de datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado - Decreto Legislativo N° 1182 (2015)**: Fortalece las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, a través del uso de tecnologías de la información y comunicaciones por parte de la Policía.
- Resolución Directoral de realización de flujo transfronterizo de datos personales (transferencia internacional) - Resolución Directoral N°003-2014-JUS/DGPDP (2014).
- Resolución Directoral de aprobación de directiva de seguridad de la información administrada por los Bancos de Datos Personales – Resolución Directoral N° 019-2013-JUS/DGPDP (2013).

---

<sup>19</sup> LANZA, Edison. Relator Especial para la Libertad de Expresión Relatoría Especial de Libertad de Expresión. Informe Anual 2016, pág. 456.

<sup>20</sup> Ídem.

- Resolución Directoral de aprobación del formulario de realización de flujo transfronterizo de datos personales - Resolución Directoral N° 002-2013-JUS/DGPDP (2013).
- Resolución Directoral de aprobación de la directiva de seguridad de la información administrada por los Bancos de Datos Personales - Resolución Directoral N° 003-2013-JUS/DGPDP (2013).
- Norma técnica sobre técnicas de seguridad y sistemas de gestión de seguridad de la información - Resolución Ministerial N° 004-2016-PCM (2016).
- Norma técnica sobre Código de Buenas Prácticas para la gestión de la seguridad de la información - Resolución Ministerial N° 246-2007-PCM (2007).
- Norma técnica para el almacenamiento y respaldo de la información procesada por entidades de la administración pública - Resolución Jefatural N° 386-2002-INEI (2002).

Por otro lado, si bien el uso de las tecnologías de la información permite a las entidades de la administración pública acercarse a la ciudadanía, a través de información disponible en las plataformas virtuales, almacenamiento y tratamiento de datos, ello supone también un mayor riesgo por la aparición de delitos informáticos que impactan en derechos como el acceso a la información pública y la protección de datos personales.

En ese sentido, mediante la dación de Ley N° 30096, se busca prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, así como otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciber delincuencia.

<b>Tipo Penal</b>	<b>Derecho sobre el cual impacta</b>
Artículo 4.- Atentado a la integridad de sistemas informáticos	Acceso a la información pública
Artículo 7.- Interceptación deliberada e ilegítima de datos informáticos, de transmisiones no públicas, Agravante: Cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.	Acceso a la información pública
Artículo 9.-Suplantación de identidad	Protección de Datos personales
Artículo 10.- Abuso de mecanismos y dispositivos informáticos fabrica, diseña, desarrolla, vende, facilita,	Protección de Datos personales

distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley	
---	--

#### 4. Jurisprudencia relevante sobre el tratamiento de la privacidad en la era digital

##### 4.1 Protección al contenido de los correos electrónicos asignados a los trabajadores dentro del marco de una relación laboral:

El empleo del correo electrónico u otros mecanismos de comunicación instantánea se han vuelto muy frecuente en los centros de trabajo. En efecto, estos instrumentos son asignados por el empleador a los trabajadores con la finalidad de garantizarles un mejor desarrollo en sus funciones y, a la vez, supervisar el debido cumplimiento de sus obligaciones.

Sin embargo, ante la ausencia de una regulación específica, el conflicto emanado por el control en el uso de los sistemas informáticos de comunicación a cargo del empleador y el derecho a la intimidad (informativa) de los trabajadores, ha generado un importante desarrollo jurisprudencial.

Así, en un primer momento, el Tribunal Constitucional sostuvo que el derecho al secreto y a la inviolabilidad de las comunicaciones y documentos privados está reconocido, inclusive, dentro del ámbito laboral. Por tanto, «[aunque], ciertamente, puede alegarse que la fuente o el soporte de determinadas comunicaciones y documentos le pertenecen a la empresa o entidad en la que un trabajador labora, ello no significa que la misma pueda arrogarse en forma exclusiva y excluyente la titularidad de tales comunicaciones y documentos, pues con ello evidentemente se estaría distorsionando el esquema de los atributos de la persona, como si estos pudiesen de alguna forma verse enervados por mantenerse una relación de trabajo.»<sup>21</sup>

Posteriormente, dicho tribunal viró su criterio, señalando como premisa general que los medios informáticos proporcionados por el empleador con fines laborales no conceden una «expectativa razonable de confidencialidad» a los trabajadores, razón por la cual el contenido no está protegido por el derecho al secreto de las comunicaciones.

Expresamente, señaló que «[cuando] se examina, entonces, el problema del uso de los recursos informáticos en el centro laboral (específicamente el e-mail laboral y el chat o mensajero interno), es preciso tener en cuenta, en primer lugar, que los medios utilizados por el trabajador para la comunicación son "bienes del empleador" y su otorgamiento a los trabajadores es con fines esencialmente laborales; por lo que el manejo de dichos bienes es, en principio, de interés del empleador, quedando facultado éste para ejercer el

<sup>21</sup> TRIBUNAL CONSTITUCIONAL. Expediente N° 1058-2004-AA/TC. Sentencia del 1058-2004-AA/TC, fundamento 18.

control sobre dichos medios. Dado que difícilmente puede generarse sobre medios que no son privados, sino laborales (en su origen y en su destino), una expectativa razonable de secreto o confidencialidad, el proceso comunicativo realizado a través del e-mail laboral y el chat o mensajero interno no puede considerarse, en principio, como una comunicación protegida por el derecho al secreto de las comunicaciones.»<sup>22</sup>

Finalmente, un pronunciamiento reciente de la Corte Suprema de Justicia de la República sobre la materia, retomó el criterio jurisprudencial inicial, considerando que representa un exceso del empleador señalar que, por ser propietario de las cuentas de correo electrónico de sus trabajadores, se encuentra facultado a revisar su contenido, pues ello implicaría una virtual colisión con el derecho a la intimidad e inviolabilidad de las comunicaciones de los trabajadores.

De esta manera, el «control empresarial encuentra sus límites en que su ejercicio sea funcional y racional. Es funcional porque debe estar relacionado al contexto empresarial y el empleador no puede controlar la esfera privada del dependiente; por otro lado, cuando se dice que el control debe ser racional se parte de la idea de que el control debe ser el resultado de un proceso intelectual que lo justifique y que dé razón al proceso de toma de decisión.»<sup>23</sup>

Por ello, se puede concluir que la justicia nacional reconoce la necesidad de proteger la privacidad informativa en los medios de comunicación tecnológicos en el ámbito de una relación laboral, estableciendo límites a la potestad de dirección y supervisión que le asiste a los empleadores.

#### **4.2 Acceso a la información pública contenida en los correos electrónicos institucionales de los funcionarios públicos:**

El acceso a la información contenida en los correos electrónicos de los servidores públicos ha merecido un tratamiento distinto al previsto en el ámbito laboral, pues por la propia naturaleza del derecho fundamental en juego resultan aplicables otras normas y principios que estructuran su ejercicio.

Un caso emblemático se presentó con el proceso de habeas data interpuesto por un ciudadano contra un ex Ministro de Energía y Minas, quien había solicitado la información contenida en sus correos electrónicos sobre el nuevo Reglamento Nacional de Hidrocarburos, y cuyo otorgamiento fue denegado por atentar con la intimidad personal e inviolabilidad de las comunicaciones.

En primera instancia, el juez del Quinto Juzgado Constitucional declaró fundada la demanda, resaltando que: i) De acuerdo con el artículo 61° del

---

<sup>22</sup> TRIBUNAL CONSTITUCIONAL. Expediente N° 3599-2010-PA/TC. Sentencia del 10 de enero de 2012. Voto concurrente del magistrado Eto Cruz, fundamento 14.

<sup>23</sup> CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Casación N° 14614-2016-LIMA. Sentencia del 10 de marzo de 2017, fundamento Décimo Quinto.

Código Procesal Constitucional, la información pública que consta en un correo electrónico estatal también es información pública; ii) No se ha solicitado información de un correo particular, sino del institucional, creado y entregado por el Ministerio de Energía y Minas al ex ministro para que ejerza su función pública; iii) La información requerida no tiene nada que ver con la intimidad del funcionario, en tanto se trata de información pública relevante vinculada a la promulgación del Reglamento Nacional de Hidrocarburos; y, iv) El principio de máxima publicidad permite entregar la información, ya que con ello se combate la cultura del secreto y se demuestra la transparencia de los actos públicos<sup>24</sup>.

Sin embargo, en segunda instancia, la Sala decidió revocar lo resuelto para declararlo improcedente. En sus argumentos, consideró que: i) El Ministerio tenía una directiva sobre el uso del correo electrónico, el cual indicaba que su contenido informativo ostentaba carácter privado; ii) Los correos electrónicos no son suministrados por el Ministerio para que los trabajadores realicen funciones laborales en forma exclusiva; iii) El Ministro, como trabajador del Estado, tiene derecho a la intimidad, el mismo que no se reduce al ámbito doméstico o privado, sino también involucra a las relaciones interpersonales en el trabajo; iv) No es factible diferenciar qué correo electrónico tendría la información pública o privada, por lo que acceder a todos los mensajes hasta individualizarlo, afectaría el derecho a las comunicaciones; y, v) La mencionada Directiva señala que los mensajes electrónicos con una antigüedad mayor a 45 días son eliminados, razón por la cual la información requerida ya no existiría.

Frente a esta situación, el caso ha sido elevado a la máxima instancia en materia constitucional, quien se encargará de evaluar finalmente si corresponde o no entregar la información pública comprendida en las cuentas electrónicas institucionales.

Sin perjuicio de ello, la Defensoría del Pueblo ha emitido un informe especializado respecto al tema en ciernes<sup>25</sup>, concluyendo que: i) Todo dato generado, obtenido o que se encuentra en posesión del Estado y que no sea confidencial, reservado o secreto, constituye información de carácter público; ii) La información generada, recibida o transmitida por un funcionario o servidor público desde su cuenta de correo electrónico institucional se presume pública, porque se trata de información que está bajo el control del Estado y ha sido generada a través de un medio habilitado y proporcionado al funcionario o servidor público para el cumplimiento de su función (pública); iii) La información de los correos electrónicos institucionales no recae en el ámbito del derecho al secreto e inviolabilidad de las comunicaciones y documentos, pues este derecho fundamental protege toda injerencia ilegítima sobre las comunicaciones o documentos de carácter privado en las que existe una expectativa razonable de confidencialidad; y, iv) La entidad obligada debe

---

<sup>24</sup> PODER JUDICIAL. Expediente N° 36677-2014-0-1801-JR-CI-05. Sentencia del 24 de junio de 2015, fundamento sexto, noveno, décimo segundo y décimo cuarto.

<sup>25</sup> DEFENSORÍA DEL PUEBLO. Informe N° 01-2015-DP/AAC: «Acceso a la información generada, recibida o transmitida a través de la cuenta de correo electrónico institucional de un funcionario o servidor público», del 27 de mayo de 2015.



justificar por qué la información solicitada tiene el carácter de confidencial y, por ende, debe estar excluida del conocimiento público.

Finalmente, en el plano normativo, se ha emitido un Proyecto de Ley, denominado «Ley que promueve la transparencia en la adopción de decisión públicas»<sup>26</sup> con la finalidad de que el Congreso de la República reconozca el acceso público a la información de los correos electrónicos institucionales, con las excepciones de ley, y el deber de conservar dicha información.

#### **4.3 Bloqueo desde la cuenta privada de Twitter de un funcionario público:**

La regulación del ejercicio de las libertades comunicativas a partir del manejo de las redes sociales, como el Twitter o Facebook, es aún bastante incipiente en nuestro ordenamiento. Por ejemplo, el Poder Judicial tuvo la oportunidad de conocer el caso de un ciudadano que interpuso un proceso de amparo contra el ex Primer Ministro de la República, Pedro Cateriano Bellido, por haberlo bloqueado de su cuenta personal de Twitter (@PCaterianoB),

El ciudadano alegó que al impedirle el seguimiento a su cuenta y, por ende, conocer la información de un alto funcionario, se había afectado su derecho a la libertad de expresión y de acceso a la información pública.

Si bien la demanda fue rechazada porque al momento de resolver el caso el demandado ya no ejercía el cargo, es importante resaltar que para el órgano jurisdiccional el ejercicio de la función pública se antepone a la naturaleza privada en el manejo de la red social.

Así, manifestó «lo limitado que es el uso de las redes sociales, pues en ellas existen filtros de bloqueo donde un usuario de Twitter puede restringir a quienes le permite el acceso a su perfil y bloquear a quienes no desea que accedan; sin embargo, en el caso de autos se trata de una persona quién desempeñaba el cargo de Presidente del Consejo de Ministros el cual es portavoz del Estado Peruano aunque el Twitter era personal [...]»<sup>27</sup>

#### **4.4 Acceso a la lista de personas bloqueadas desde la cuenta de Facebook de una institución pública:**

Otro caso vinculado con el derecho de acceso a la información pública sobre las redes sociales se presentó cuando un ciudadano solicitó la relación completa de usuarios bloqueados en la página oficial de Facebook de la Municipalidad Metropolitana de Lima.

En un inicio, la entidad estatal denegó lo solicitado porque entendió que esa información era confidencial, por lo que de ser proporcionada vulneraría la «integridad personal y comunicacional» de los implicados, según lo dispuesto en la Ley de Transparencia y Acceso a la Información Pública.

---

<sup>26</sup> Remitido al Congreso de la República mediante Oficio N° 019-2017/DP, del 08 de febrero de 2017.

<sup>27</sup> PODER JUDICIAL. Expediente N° 08427-2015-0-1801-JR-CI-01. Sentencia del 24 de agosto de 2016, fundamento séptimo.

Sin embargo, cuando el Poder Judicial analizó esta controversia, declaró fundada la solicitud de información, habida cuenta que «la lista de los usuarios bloqueados de Facebook solo versa sobre el nombre que han consignado en esta red social, desprendiéndose de ello que, no se pone en peligro la intimidad personal de dichos usuarios, es decir, no se aprecia una intromisión real e ilegítima en su vida íntima o familiar.»<sup>28</sup>

Cabe precisar que este caso aún se encuentra en trámite, luego de haber sido impugnado por el representante legal de la corporación edil. No obstante, permite advertir que la expansión funcional de las entidades del Estado en estas plataformas de interacción virtual con la ciudadanía requiere también el deber de garantizarles el ejercicio pleno de sus derechos fundamentales.

#### **4.5 Despido laboral por comentarios vertidos a través de una cuenta de Facebook personal:**

El ordenamiento laboral peruano establece como causal de despido al faltamiento de palabra verbal o escrita en agravio del empleador o sus representantes<sup>29</sup>. Medida que, incluso, comprende las expresiones que se deslizan por las cuentas personas en las redes sociales.

Así lo ha entendido el Poder Judicial en la oportunidad que tuvo para analizar el caso de un trabajador que había sido despedido por su empleador, debido a los comentarios que difundió vía Facebook contra un supervisor de la empresa.

En aquella situación, en ente judicial manifestó lo siguiente: «[...] se encuentra acreditado que la imputación de cargos efectuada en contra del actor, está relacionada con el faltamiento de palabra verbal o escrita realizado por el demandante desde su cuenta personal de red social “Facebook” en contra del Supervisor de Agentes de Seguridad de la demandada Tecnología Textil S.A., el mismo que se encuentra configurado como falta grave, al haber infringido los deberes esenciales que emanan de un contrato de trabajo [...]»<sup>30</sup>

También la Defensoría del Pueblo ha tenido la ocasión de analizar el impacto del derecho a la libertad de expresión a través del Facebook, dentro del marco de las relaciones laborales. Por ello, ha considerado que las opiniones o ideas difundidas por un trabajador o sindicato bajo este tipo de herramientas

---

<sup>28</sup> PODER JUDICIAL. Expediente N° 14190-2015-0-1801-JR-CI-01. Sentencia del 09 de octubre de 2017, fundamento séptimo.

<sup>29</sup> LEY DE PRODUCTIVIDAD Y COMPETITIVIDAD LABORAL (DECRETO LEGISLATIVO N° 728). Artículo 25.- Falta grave es la infracción por el trabajador de los deberes esenciales que emanan del contrato, de tal índole, que haga irrazonable la subsistencia de la relación. Son faltas graves: f) Los actos de violencia, grave indisciplina, injuria y faltamiento de palabra verbal o escrita en agravio del empleador, de sus representantes, del personal jerárquico o de otros trabajadores, sea que se cometan dentro del centro de trabajo o fuera de él cuando los hechos se deriven directamente de la relación laboral. [...]

<sup>30</sup> CORTE SUPREMA DE JUSTICIA DE LA REPÚBLICA. Casación N° 19856-2016-LIMA ESTE. Sentencia del 19 de setiembre de 2017, fundamento décimo primero.

virtuales merece especial atención, sobre todo por la relevancia pública que muchas veces subyacen en el contenido de las expresiones.

De esta manera, en el caso de un procedimiento disciplinario instaurado contra un dirigente sindical por haber hecho públicas sus declaraciones en el Facebook oficial del sindicato sobre las actuaciones internas de su entidad empleadora, se resaltó que «las publicaciones difundidas a través de la página de Facebook del mencionado sindicato, tendrían como finalidad dar cuenta de hechos de interés, no solo para sus miembros sino también para los trabajadores vinculados a la Superintendencia Nacional de Migraciones. Ello en tanto informó acerca de un conflicto suscitado entre estos y una alta funcionaria. En consecuencia, estimamos que estas son de interés general y, por lo tanto, se encuentran protegidas por el derecho a la libertad de expresión.»<sup>31</sup>

Como se puede apreciar, gracias al influjo de las nuevas tecnologías informativas, el ejercicio de la libertad de expresión se ha dinamizado hacia escenarios virtuales, en donde el adecuado o inadecuado empleo de las redes sociales personales tiene efectos jurídicos en el ámbito de protección de los derechos de las personas.

#### **4.6 Acceso a documentos vinculados con la Ley de Geolocalización:**

Mediante el Decreto Legislativo N° 1182 se aprobó la norma que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

Sin embargo, toda vez que la precita normativa habilita a las autoridades policiales tener acceso a los datos de localización o geolocalización de los teléfonos móviles o dispositivos electrónicos personales, un ciudadano solicitó ante el Ministerio del Interior que le proporcione información relacionada con el sustento y su aplicación.

Específicamente, requirió: i) Copia del protocolo de acceso a los datos de localización y geolocalización; ii) Información estadística sobre la aplicación de dicho protocolo; iii) Copia de los informes sustentatorios elaborados por el Ministerio del Interior para la aprobación del Decreto; y, iv) Copia de las auditorías operativas realizadas por la Inspectoría General del Ministerio del Interior y la Policía Nacional en cumplimiento del mismo Decreto. No obstante, el pedido fue denegado porque la entidad pública consideró que se trataba de una información de carácter reservada.

Cuando el caso fue ventilado en sede judicial, el juez del proceso resaltó que en relación a los protocolos «la ciudadanía tiene derecho de conocer, qué datos de localización y geolocalización retienen los operadores, así como el tiempo determinado de su retención, pues la actuación de quiénes participan debe circunscribirse al procedimiento establecido, de lo contrario se incurrirá

---

<sup>31</sup> DEFENSORÍA DEL PUEBLO. Memorando N° 12-2018-DP/AAC, del 19 de enero de 2018. Anexo, índice III.

en responsabilidad por utilizar indebidamente los datos de localización o geolocalización de acuerdo al artículo 7 del Decreto Legislativo 1182.»<sup>32</sup>

Lo anterior permite inferir que, en abstracto, los «datos relativos al tráfico»<sup>33</sup> de la información, tales como el origen, el destino, la hora y la duración de la comunicación, constituyen información de naturaleza pública (elementos de la geolocalización); lo que no puede predicarse respecto al contenido de esos datos registrados en los teléfonos móviles u otros dispositivos electrónicos, que forman parte de la privacidad informativa de las personas.

## 5. Conclusiones

- El Estado peruano ha iniciado acciones para adecuar su funcionamiento a las exigencias que plantea el moderno gobierno electrónico, lo cual contribuirá en garantizar una mayor transparencia en la administración de recursos públicos y la participación de los ciudadanos a través de la tecnología.
- Es necesario fomentar espacios donde predomine un debate plural, abierto y tolerante sobre diversos temas de relevancia pública, sea mediante plataformas tradiciones o en aquellas de soporte virtual.
- El Plan Estratégico de Desarrollo Nacional Bicentenario 2021 contiene lineamientos de política, prioridades y objetivos, para el desarrollo armónico y sostenido del país, respecto a transparencia, la rendición de cuentas y libertad de expresión. Sin embargo, para lograr estos objetivos se requiere fortalecer la conectividad a través del acceso a internet, y políticas de telecomunicaciones en condiciones de mayor calidad y menores tarifas a los sectores mayoritarios del país.
- El Perú cuenta con un marco normativo importante relativo al derecho de acceso a la información pública y protección de datos personales. Sin embargo, aún resultan insuficientes para encarar los nuevos retos que impone el almacenamiento, procesamiento, otorgamiento o tratamiento de aquella información contenida en suministros informáticos o vía internet.
- Garantizar un amplio uso de las tecnologías de la información sobre los derechos de libertad de expresión, acceso a la información, transparencia y protección de datos personales, exige también una adecuada protección por parte del Estado para controlar o sancionar aquellas conductas ilícitas que supongan el empleo de estos mecanismos para la comisión de delitos informáticos.
- Ante la ausencia de normas que regulen en forma sistemática y ordenada las libertades y derechos comunicativos e informativos en el ámbito digital, la jurisprudencia ha ido construyendo y trazando importantes criterios de

---

<sup>32</sup> PODER JUDICIAL. Expediente N° 3811-2017-0-1801-JR-CI-05. Sentencia del 30 de octubre de 2017, fundamento décimo primero.

<sup>33</sup> CONVENIO SOBRE LA CIBERDELINCUENCIA. Budapest: 2001. Artículo 1. Definiciones.- A los efectos del presente Convenio: d. Por “Datos relativos al tráfico” se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

aplicación directa para solucionar controversias de relevancia constitucional. Sin embargo, aun resultan variables e insuficientes para brindar un tratamiento jurídico vinculante hacia otras situaciones análogas.

**Adjuntía en Asuntos Constitucionales  
Defensoría del Pueblo**