# OPINIÓN CONSULTIVA N° 20-2025-DGTAIPD

ASUNTO : Consulta sobre acceso de imágenes y grabación captadas por las cámaras de videovigilancia ubicadas en bien de dominio público

REFERENCIA : Hojas de Trámite N° 338119-2022MSC y N° 338830-2022MSC

FECHA: 09 de mayo de 2025

## I. ANTECEDENTES

1. Mediante Oficios N°080-2022-GA-ICL/MML y N°081-2022-GA-ICL/MML, la Gerencia de Administración del Instituto Catastral de Lima (en adelante, el "ICL") solicita a esta Dirección General emitir opinión sobre el acceso de imágenes y grabación captadas por las cámaras de videovigilancia ubicadas en el bien de dominio público del ICL.

2. En específico, se consulta lo siguiente:
   *"1. ¿Un trabajador puede solicitar copia de grabaciones del sistema de vigilancia de la institución, de sus movimientos dentro del centro de trabajo de determinadas fechas, sin indicar o sustentar el motivo de su solicitud?*
   *2. ¿La entidad se encuentra en la obligación de entregar mediante acceso a la información pública a toda persona, las imágenes y videos captados por las cámaras de videovigilancia ubicadas dentro del bien de dominio público sin presentarse una comisión de un presunto delito o falta, o que el solicitante no indique la motivación de su solicitud?"*

## II. MARCO NORMATIVO DE ACTUACIÓN

2. El artículo 32 de la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, la "LPDP"), crea la Autoridad Nacional de Protección de Datos Personales (en adelante, la "ANPD"), que se rige por dicha ley, su reglamento y las normas pertinentes del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado mediante Decreto Supremo N° 013-2017-JUS (en adelante, "ROF del MINJUS").

3. Entre las funciones de la ANPD, previstas en el artículo 33 de la LPDP, se encuentra la de absolver consultas sobre protección de datos personales y emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la cual es vinculante[1].

[1] **Ley N° 29733, Ley de Protección de Datos Personales**
**"Artículo 33. Funciones de la Autoridad Nacional de Protección de Datos Personales**

4. Por su parte, el ROF del MINJUS, establece en su artículo 70 que la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la "DGTAIPD") es el órgano de línea encargado de ejercer la ANPD, por lo que tiene entre sus funciones absolver consultas sobre protección de datos personales y emitir opinión técnica respecto de proyectos normativos que se refieran a los ámbitos de su competencia. [2]

5. Por ende, esta Dirección General, en su calidad de órgano de línea del Ministerio de Justicia y Derechos Humanos sobre el que recae la ANPD, emite la presente Opinión Consultiva en el ámbito de la interpretación abstracta de las normas y no como mandato específico de conducta para un caso en concreto.

## III. ANÁLISIS

### *A. El derecho de acceso del titular de datos personales a sus datos captados en sistemas de videovigilancia*

1. El numeral 16 del artículo 2 de la LPDP define como titular de datos personales a aquella *"persona natural a quien corresponde los datos personales*".

2. El numeral 4 del artículo 2 de la LPDP define a los datos personales como *"toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados."*

3. Asimismo, el Reglamento de la Ley de Protección de Datos Personales, aprobado a través del Decreto Supremo N° 16-2024-JUS (en adelante, el "Reglamento de la

---

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:
(…)
10. Absolver consultas sobre protección de datos personales y el sentido de las normas vigentes en la materia, particularmente sobre las que ella hubiera emitido.
11. Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los datos personales, la que es vinculante.
(…)"

[2] **Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos**
**"Artículo 71.- Funciones de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales**
Son funciones de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales las siguientes:
(…)
d) Emitir opinión técnica respecto de los proyectos de normas que se refieran total o parcialmente a los ámbitos de su competencia. En materia de protección de datos personales la opinión técnica es vinculante.
e) Absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto de la aplicación de normas de transparencia y acceso a información pública; así como sobre protección de datos personales.
(…)"

LPDP"), desarrolla - en su artículo 2, numeral 4 - la definición de datos personales, señalando que es *"Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados."*

4. El sistema de videovigilancia[3] se encuentra definido en la Directiva N° 01-2020-JUS/DGTAIPD para el Tratamiento de Datos Personales Mediante Sistemas de Videovigilancia, aprobada mediante Resolución Directoral Nº02-2020-JUS/DGTAIPD (en adelante, la "Directiva de Videovigilancia") como un conjunto de una o más personas y equipos tecnológicos -compuesto por una o varias cámaras de video localizadas estratégicamente e interconectadas entre sí - que permiten el tratamiento de datos personales. Complementariamente, la videovigilancia[4] implica el monitoreo y captación de imágenes, videos o audios de lugares, personas u objetos; señalando que la información captada puede o no ser objeto de almacenamiento a través de su grabación.

5. En este orden de ideas, las imágenes y voces de una persona captadas a través de cámaras y/o sistemas de videovigilancia constituyen datos personales, toda vez que permiten identificarla o hacerla identificable, siendo de aplicación la LPDP y su Reglamento, así como la Directiva de Videovigilancia para garantizar un adecuado tratamiento de los datos personales a través de dichos sistemas.

6. En el artículo 19 de la LPDP se regula el derecho de acceso del titular de datos personales, señalando que *"el titular de los datos personales tiene derecho a obtener información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública y privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quien se realizó la recopilación, así como las transferencias realizadas o que se prevén hacer de ellos".*

7. Complementariamente, sobre el derecho de acceso el artículo 75, inciso 75.1, del Reglamento de la LPDP establece lo siguiente:

> "75.1 El titular de datos personales tiene derecho a que se le comunique de forma clara, expresa e indubitablemente con lenguaje sencillo lo siguiente:
> 1. Sus datos personales objeto de tratamiento;
> 2. La forma en que sus datos personales fueron recopilados;
> 3. Las razones que motivaron la recopilación de los datos personales;
> 4. La indicación de a solicitud de quién se realizó la recopilación; y,
> 5. Las transferencias realizadas o que se prevén hacer con los datos personales.

[3] Artículo 5.22 de la Directiva de Videovigilancia
[4] Artículo 5.27 de la Directiva de Videovigilancia

8. Este derecho de acceso es un derecho personalísimo[5], en tanto puede ser ejercido únicamente por el titular de dato personal en ejercicio de su facultad de control y decisión sobre su información para evitar y/o contrarrestar posibles abusos y/o tratamientos no autorizados respecto de sus datos personales.

9. Todo titular de datos personales puede ejercer su derecho de acceso ante el titular del banco de datos personales o responsable del tratamiento que utiliza sus datos personales para obtener información que sobre sí mismo sea objeto de tratamiento y, en general para requerir detalle de las condiciones y generalidades de su tratamiento. Para ello, el titular del dato solicitante acreditará su identidad con la presentación de una copia de su DNI o documentación que acredite la representación en caso de poder otorgarlo a tercero para presentar la solicitud en su nombre, conforme a lo establecido en el artículo 49 de la LPDP.[6]

10. En concordancia con el artículo 19 de la LPDP, la Directiva de Videovigilancia, en sus artículos 6.30 y 6.31, regula el derecho de acceso de los titulares de datos personales captados por sistemas de videovigilancia, acotándose que este derecho reviste de características singulares debido a las particularidades de los sistemas empleados.

11. En este sentido, el artículo 6.31[7] de la Directiva de Videovigilancia, regula, entre otros,

---

[5] **LPDP:**
**"Artículo 47.- Carácter personal.**
Los derechos de información, acceso, rectificación, cancelación, oposición y tratamiento objetivo de datos personales sólo pueden ser ejercidos por el titular de datos personales, sin perjuicio de las normas que regulan la representación."

[6] **LPDP**
**"Artículo 49.- Legitimidad para ejercer los derechos.**
El ejercicio de los derechos contenidos en el presente título se realiza:
1. Por el titular de datos personales, acreditando su identidad y presentando copia del Documento Nacional de Identidad o documento equivalente. El empleo de la firma digital conforme a la normatividad vigente, sustituye la presentación del Documento Nacional de Identidad y su copia.
2. Mediante representante legal acreditado como tal.
3. Mediante representante expresamente facultado para el ejercicio del derecho, adjuntando la copia de su Documento Nacional de Identidad o documento equivalente, y del título que acredite la representación.
Cuando el titular del banco de datos personales sea una entidad pública, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, conforme al artículo 115 de la Ley Nº 27444, Ley del Procedimiento Administrativo General.
4. En caso se opte por el procedimiento señalado en el artículo 51 del presente reglamento, la acreditación de la identidad del titular se sujetará a lo dispuesto en dicha disposición."

[7] **Directiva de Videovigilancia**
**"Derecho de Acceso**
6.31 Dadas las particularidades propias de los sistemas de videovigilancia, el derecho de acceso reviste características singulares:
6.31.1 El titular del dato personal debe precisar la fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen requerida. Asimismo, de ser necesario, aportará una imagen actualizada de sí mismo que permita al titular o encargado del tratamiento verificar su presencia en el registro.
6.31.2 Con la finalidad de no afectar la protección de datos personales de terceros, el titular del dato personal puede escoger entre las siguientes alternativas para acceder a su información:
**a) Acceso mediante un escrito:**

lo siguiente:

- La información que debe precisar el titular del dato que solicite el acceso a sus imágenes y/o audio captados, como la fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen requerida (numeral 1)
- Establece que el ejercicio del derecho de acceso no puede afectar la protección de datos personales de terceros, en cuyo caso el titular del banco de datos debe utilizar máscaras de privacidad para difuminar las imágenes de terceros, así como implementar un mecanismo de protección para el archivo (cifrado, contraseña u otros) (literal "b" del numeral 2)
- No procede la difuminación de imágenes o aplicación de máscaras de seguridad de terceras personas cuando se acredite el legítimo interés del titular del dato personal que lo solicita. Se entiende por legítimo interés, el acopio de información

---

El titular del dato personal presentará una solicitud escrita a la dirección física o electrónica que aparece en el cartel o documento informativo, adjuntando e indicando lo señalado en el numeral 6.31.1.

La respuesta emitida por el titular del banco de datos personales o por el encargado del tratamiento debe detallar los datos requeridos que son objeto de tratamiento, sin afectar derechos de terceros.

**b) Entrega de las imágenes, vídeos o audios:**

El titular del dato personal debe entregar un CD en blanco o dispositivo análogo al titular del banco de datos personales o al encargado de tratamiento con el fin de que este grabe su información. En este supuesto, el titular o encargado del tratamiento debe utilizar máscaras de privacidad para difuminar la imagen o cualquier otro medio que impida la afectación de terceros, así como implementar un mecanismo de protección para el archivo (cifrado, contraseña u otros).

**c) Visualización en sitio:**

El titular del dato personal debe acercarse físicamente a las instalaciones del titular del banco de datos o responsable del tratamiento para acceder directamente a su información.

Para ello, debe presentar previamente una solicitud en la dirección física o electrónica que aparece en el cartel o documento informativo, indicando fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen; así como una imagen actualizada de sí mismo que permita al titular del banco de datos personales o responsable del tratamiento advertir su presencia en el registro.

Se debe dejar constancia de lo visualizado y entregar la misma al titular del dato personal, una vez culminada la visualización.

6.31.3 Adicionalmente, se entrega al titular de los datos personales información precisa sobre la finalidad de la recolección de los datos, sobre la inscripción del banco de datos, el lugar donde se produjo el registro o captación de su imagen, el tiempo en que la misma se produjo y el destino de los datos.

6.31.4 Si se ejerce el derecho de acceso ante el responsable de un sistema que únicamente reproduce imágenes sin registrarlas, debe ponerse esta situación a conocimiento del titular del dato personal.

6.31.5 No procede la difuminación de imágenes o aplicación de máscaras de seguridad de terceras personas cuando se acredite el legítimo interés del titular del dato personal que lo solicita. Se entiende por legítimo interés, el acopio de información para ejercer el derecho de defensa, formular denuncia administrativa o penal o similares.

6.31.6 En el supuesto que el responsable o encargado del tratamiento no aplicara la máscara de seguridad o algún mecanismo de difuminación de imágenes que impidiera la afectación de terceros, aduciendo falta de capacidad técnica o económica, será la autoridad administrativa que valorará este alegato en cada caso en concreto.

6.31.7 Si el titular del banco de datos o responsable del tratamiento es declarado un activo crítico nacional conforme a la normativa de la materia o si se tratara de áreas de alto riesgo para la seguridad, se deberá acordar con el titular del dato personal otro mecanismo idóneo para dar acceso a su información. De no existir ningún medio posible, podrá ser denegada su solitud por el titular del banco de datos personales o el responsable del tratamiento, debiendo hacerlo de forma motivada."

para ejercer el derecho de defensa, formular denuncia administrativa o penal o similares (numeral 5)

12. Esta Dirección reitera lo señalado en la Opinión Consultiva N°08-2022-JUS/DGTAIPD[8], respecto a que las imágenes de terceros no pueden entregarse en atención al ejercicio del derecho de acceso si no aparece en tales imágenes la persona solicitante, puesto que dicho derecho es personalísimo. Por tanto, para que proceda la entrega de imágenes de un tercero a una persona que alega tener legítimo interés en su obtención y no aparezca en tales imágenes, deberá gestionar su solicitud a través de las autoridades pertinentes en el marco de los procedimientos legales correspondientes.

13. Respecto al uso de los sistemas de vigilancia para control laboral, cabe señalar que, el tratamiento de datos personales de los trabajadores por parte del empleador resulta válido en tanto dicho tratamiento sea proporcional y razonable para efectos de supervisión del cumplimiento de las labores y obligaciones a cargo del trabajador, siempre que los mecanismos empleados no resulten excesivos para dicho fin, debiendo cumplir con el deber-derecho de informar conforme a lo establecido en el artículo 18 de la LPDP. Se cumple con este deber de informar con la colocación del cartel y/o aviso informativo en las zonas videovigiladas, según lo establecido en la cláusula 6.17 y Anexo 2 de la Directiva de Videovigilancia.

14. Es en observancia del principio rector de proporcionalidad[9] que, la Directiva de Videovigilancia en sus cláusulas 7.13 a 7.16 limita el uso del sistema de videovigilancia para control laboral a espacios indispensables para tal fin, excluyendo la instalación y uso de dichos sistemas en lugares de descanso o esparcimiento (vestuario, servicios higiénicos, comedor o análogos), admitiendo la grabación con sonido en el lugar de trabajo únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo siempre que se respete los principios de proporcionalidad y finalidad.

15. Conforme a lo establecido en la cláusula 7.18 de la Directiva de Videovigilancia establece que las imágenes y/o voces grabadas se almacenan por un plazo de treinta (30) días y hasta un plazo máximo de sesenta (60) días, salvo disposición distinta en las normas laborales. Asimismo, señala que durante dicho plazo, el titular del banco de datos o encargado del tratamiento debe cuidar que la información sea accesible sólo ante las personas que tengan legítimo derecho a su conocimiento y manteniendo así la reserva necesaria respecto a las imágenes y/o voces.

---

[8] Opinión Consultiva disponible en https://www.gob.pe/institucion/anpd/informes-publicaciones/2725905-oc-n-08-2022-jus-dgtaipd-sobre-el-derecho-de-acceso-en-sistemas-de-videovigilancia

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

16. En cuanto a la existencia de imágenes vinculadas a la comisión de presuntas infracciones laborales y/o accidentes de trabajo, el artículo 7.21 de la Directiva de Videovigilancia establece que estas deben ser conservadas por el plazo de ciento veinte (120) días, contados a partir de su conocimiento, salvo la existencia de alguna finalidad que justifique su conservación o de interés legítimo, tiempo dentro del cual el empleador podrá iniciar las acciones legales pertinentes.

17. El artículo 7.2.2 de la Directiva de Videovigilancia señala que el trabajador imputado de alguna inconducta o incumplimiento laboral podrá solicitar el acceso a las grabaciones o a una copia digital de las mismas que contengan información sobre tales imputaciones, pudiendo utilizarlas como medio de prueba. El empleador debe difuminar aquellas imágenes de terceros no involucrados con la conducta o incumplimiento que aparezcan en las grabaciones.

18. De lo expuesto, se colige que cualquier persona puede en ejercicio de su derecho de acceso solicitar copia de sus imágenes captadas mediante sistemas de videovigilancia en tanto las imágenes se encuentren disponibles (según los plazos de conservación establecidos). Para ello, el titular debe cumplir con acreditar su identidad y especificar en su solicitud la fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen requerida, no siendo necesario motivar su solicitud en tanto él mismo aparezca en la imagen. En este caso, el titular del banco de datos y/o responsable del tratamiento debe difuminar las imágenes y/o voz de terceros que aparezcan en la grabación que se acceda.

19. Esta Dirección considera que, únicamente, procederá motivar la solicitud de acceso a las imágenes de sistemas de videovigilancia cuando el titular del dato que aparezca en la grabación requiera la identificación de los terceros que también aparecen en ella, debiendo acreditar su legítimo interés ante el titular del banco de datos personales y/o responsable del tratamiento.

20. Finalmente, para los casos en los que la solicitud de acceso provenga de un trabajador imputado de alguna inconducta o incumplimiento laboral, rigen los mismos requisitos de especificación que permitan facilitar la ubicación de la imagen requerida; debiendo el empleador difuminar aquellas imágenes de terceros no involucrados con la conducta o incumplimiento que aparezcan en las grabaciones.

### *B. Sobre las imágenes y videos captados por las cámaras de videovigilancia ubicadas en bienes de dominio público*

21. Las imágenes, videos o audios captados por cámaras de videovigilancia ubicados en bienes de dominio público no constituyen información de acceso público por configurar información confidencial, conforme ha sido desarrollado en las Opiniones

Consultivas Nº 55-2020-JUS/DGTAIPD[10], N° 04-2021-JUS/DGTAIPD[11] y N° 033-2022-JUS/DGTAIPD[12].

22. Conforme a lo señalado en las opiniones mencionadas, la restricción al acceso a las grabaciones de las cámaras de videovigilancia puede ser regulada por el Decreto Legislativo Nº 1218, que regula el uso de cámaras de videovigilancia en bienes de dominio público (en adelante, el "Decreto Legislativo Nº 1218"). Ello en tanto, el numeral 6 del artículo 17 del Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública (en adelante, el "TUO de la LTAIP") contempla la posibilidad de que se creen otros supuestos de exclusión (esto es, supuestos adicionales de información confidencial) a través de la Constitución o una norma con rango de Ley[13].

23. Justamente, el Decreto Legislativo Nº 1218 establece la obligación de mantener reserva y confidencialidad del contenido las cámaras y/o sistemas de videovigilancia[14].

24. En tal sentido, en su artículo 14, dispone que ante la presencia de indicios razonables de la comisión de un delito o falta, el propietario o poseedor de cámaras de

---

[10] Opinión Consultiva disponible en https://www.gob.pe/institucion/antaip/informes-publicaciones/1472623-oc-n-55-2020-dgtaipd-absolucion-de-consulta-sobre-la-accesibilidad-de-las-imagenes-videos-y-o-audios-captados-por-camaras-de-videovigilancia-ubicadas-en-bienes-de-dominio-publico

[11] Opinión Consultiva disponible en https://www.gob.pe/institucion/antaip/informes-publicaciones/1773924-oc-n-04-2021-jus-dgtaipd-sobre-la-difusion-o-entrega-de-la-informacion-obtenida-a-traves-de-las-camaras-de-videovigilancia-imagenes-videos-o-audios

[12] Opinión Consultiva disponible en https://www.gob.pe/institucion/anpd/informes-publicaciones/3837286-oc-n-033-2022-jus-dgtaipd-sobre-la-accesibilidad-a-la-informacion-contenida-en-las-grabaciones-de-las-camaras-de-videovigilancia-de-las-entidades-publicas-y-si-estas-pueden-contener-informacion-de-caracter-secreto-reservado-o-confiden

[13] De acuerdo al Tribunal Constitucional los supuestos de excepción también pueden plantearse a través de decretos legislativos, toda vez que estas normas tienen rango de ley, constituyen un acto legislativo y son pasibles de control por el Congreso de la República. Sentencia recaída en el Expediente N° 0005-2013-PI/TC, fundamento jurídico 19.

[14] **Decreto Legislativo Nº 1218, artículos 4 y 13.b:**

**"Artículo 4.- Reglas**

Son reglas para el uso de cámaras de videovigilancia:

(…)

d. Reserva.- Todo funcionario o servidor público que conozca de imágenes, videos o audios captados por las cámaras de videovigilancia está obligado a mantener reserva de su contenido."

" **Artículo 13.- Obligaciones en la captación y grabación de imágenes, videos o audios**

Todas las personas naturales o jurídicas, entidades públicas o privadas propietarias o poseedoras de cámaras de videovigilancia que capten o graben imágenes, videos o audios deben observar lo siguiente:

(…)

b. Cualquier persona que por razón del ejercicio de sus funciones dentro de instituciones públicas o privadas, tenga acceso a las grabaciones deberá observar la debida reserva y confidencialidad en relación con las mismas."

videovigilancia que capte o grabe imágenes, videos o audios debe informar y entregar dicha información a la Policía Nacional del Perú o al Ministerio Público de forma inmediata, para la investigación o represión del delito, debiendo estos últimos garantizar la confidencialidad de la identidad de la persona que realice dicha entrega.

25. Esta disposición guarda relación con lo establecido en los artículos 6.14 de la Directiva de Videovigilancia respecto a la entrega inmediata a la Policía y al Ministerio Público de imágenes videos o audios que presenten indicios razonables o una supuesta comisión de un delito o falta para la identificación de los presuntos responsables. Asimismo, el artículo 6.35.2. de la Directiva de Videovigilancia dispone que ante un requerimiento de las grabaciones por parte de la Policía o del Ministerio Público, en razón del ejercicio de las competencias asignadas por ley, en aquellos supuestos necesarios para la prevención, investigación, detección o represión de infracciones penales o delitos; dicho requerimiento debe ser motivado.

26. De lo expuesto, se desprende que las imágenes, videos o audios de grabaciones captadas por sistemas de videovigilancia ubicados en bienes de dominio público no pueden ser entregados a cualquier persona a través de una solicitud de acceso a la información pública por encontrarse revestido de reserva a quienes conocen el contenido de tales grabaciones. Quedan exceptuados los sujetos habilitados para acceder a la información contenida en el régimen de excepciones, de conformidad al artículo 18 del TUO de la LTAIP: Comisión Investigadora del Congreso de la República, el Poder Judicial (el juez en un determinado caso), el Contralor General de la República (dentro de una acción de control de su especialidad); el Defensor del Pueblo (para la defensa de derechos humanos) y el Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (para el cumplimiento de funciones de la UIF Perú).

## IV. CONCLUSIONES

1. El derecho de acceso es un derecho personalísimo, pudiendo ser ejercido únicamente por el titular de dato personal para controlar y decidir sobre su propia información.

2. En virtud del derecho de acceso, cualquier persona puede solicitar copia de sus imágenes captadas mediante sistemas de videovigilancia en tanto las imágenes se encuentren disponibles. Para ello, el titular debe cumplir con acreditar su identidad y especificar en su solicitud la fecha, rango de horas, lugar o cualquier otra información que permita facilitar la ubicación de la imagen requerida, no siendo necesario motivar su solicitud en tanto él mismo aparezca en la imagen grabada.

3. En caso la solicitud de acceso provenga de un trabajador imputado de alguna inconducta o incumplimiento laboral, rigen los mismos requisitos de especificación que permitan facilitar la ubicación de la imagen requerida.

4. El titular del banco de datos y/o responsable del tratamiento debe resguardar el derecho a la protección de datos personales de terceros que aparezcan en las imágenes y/o grabaciones solicitadas, difuminando las imágenes de terceros para evitar que sean identificados.

5. Únicamente se deberá motivar la solicitud de acceso a las imágenes de sistemas de videovigilancia cuando el titular del dato que aparezca en la grabación requiera la identificación de los terceros que también aparecen en ella, debiendo acreditar su legítimo interés ante el titular del banco de datos personales y/o responsable del tratamiento.

6. Las imágenes, videos o audios captados por cámaras de videovigilancia ubicados en bienes de dominio público no constituyen información de acceso público por configurar información confidencial (supuesto contemplado en el inciso 6 del artículo 17 del TUO de la LTAIP).

7. El Decreto Legislativo Nº 1218 que regula el uso de cámaras de videovigilancia en bienes de dominio público dispone reserva y confidencialidad de la información, permitiéndose únicamente su entrega inmediata al Ministerio Público y a la Policía Nacional de Perú, según corresponda, ante la existencia de indicios razonables de la comisión de un delito o falta para la identificación de los presuntos responsables.

8. El tratamiento de datos personales captados por sistemas de videovigilancia por motivos del resguardo de la seguridad ciudadana no abarca la entrega abierta a terceros no autorizados para las acciones de prevención, investigación, detección o represión de infracciones penales o delitos.

**María Alejandra González Luna**
Director General (e)[15]
Dirección General de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales

[15] Designación temporal, por el periodo del 5 al 12 de mayo de 2025, mediante la Resolución Jefatural N.° 137-2025-JUS-OGRRHH de 24 de abril de 2025