



“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

OPINIÓN CONSULTIVA N° 011-2023-JUS/DGTAIPD

ASUNTO : Sobre la accesibilidad a las imágenes, videos y/o audios captados por cámaras de videovigilancia ubicadas en bienes de dominio público, la aplicación de la excepción referida a datos personales como imágenes y audios de funcionarios y servidores públicos, la calificación de acto violatorio de derechos humanos y la responsabilidad por difusión de información protegida

REFERENCIA : Oficio 009 -2023-DP/AAC (HT.000317598-2022)

FECHA : 21 de marzo de 2023

I. ANTECEDENTES

1. Mediante el documento de la referencia, el señor Alberto Cruces Burga, Adjunto en Asuntos Constitucionales (e) de la Defensoría del Pueblo, formuló a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DGTAIPD) las siguientes consultas:
 1. *Ante una solicitud o pedido para acceder a las imágenes de videovigilancia obtenidas por la Defensoría del Pueblo:*
 - a. *¿La institución debe entregar todas las imágenes?*
 - b. *¿Se debe entregar la imagen y voces solo de funcionarios/as públicos que, en el ejercicio de sus funciones, aparecen en las grabaciones?*
 2. *En caso la Defensoría del Pueblo determine que las imágenes de cámaras de videovigilancia contienen presuntas violaciones a los derechos humanos y en base al interés público, ¿puede difundirlas de forma proactiva o en respuesta a una solicitud en concreto?*
 3. *¿Corresponde algún tipo de responsabilidad para el poseedor de las imágenes que decida entregarla por considerarla de interés público? ¿De qué tipo?*

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

II. MARCO NORMATIVO DE ACTUACIÓN

2. De conformidad con el artículo 4 inciso 4 del Decreto Legislativo 1353¹ que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública (en adelante, ANTAIP), esta Autoridad tiene la función de 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 la información pública.
3. En tanto, el artículo 33 inciso 10 de la Ley de Protección de Datos Personales (en adelante, LPDP) encarga a la Autoridad Nacional de Protección de Datos Personales (en lo sucesivo, ANPD) absolver consultas sobre protección de datos personales.
4. En esa medida, esta Dirección General, en tanto órgano de línea del Ministerio de Justicia y Derechos Humanos sobre el que recae la ANTAIP y la ANPD², emite la presente opinión, en mérito a la normativa citada, en el ámbito de la interpretación en abstracto de las normas; es decir, como pauta de interpretación general y no como mandato específico de conducta para un caso concreto.
5. Por tal razón, los criterios interpretativos adoptados por dichas Autoridades no se encuentran vinculados a situación particular alguna ni relevan el cumplimiento de las obligaciones que corresponden a las entidades, como la referida a evaluar la accesibilidad o inaccesibilidad a la información en cada caso concreto, la cual es competencia exclusiva de estas por encontrarse en su posesión y bajo su control, máxime si el plazo de absolución de consulta es superior al plazo para atender las solicitudes de acceso a la información³ y la normativa no ha previsto como un supuesto de prórroga la espera de su pronunciamiento⁴.
6. En ese sentido, en el marco de lo dispuesto en el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública (en adelante, TUO de la LTAIP) y la LPDP, esta Dirección General se pronunciará sobre los siguientes aspectos:
 - Sobre el tratamiento de datos personales derivado de la videovigilancia y su conformidad legal.
 - La accesibilidad de las imágenes, videos y/o audios captados por cámaras de videovigilancia ubicadas en bienes de dominio público.

¹ Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de gestión de intereses, publicado el 7 de enero de 2017.

² Artículo 70 del Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, aprobado por Decreto Supremo 013-2017-JUS.

³ Artículo 7 del Reglamento del Decreto Legislativo 1353.

⁴ Artículo 10, inciso g) del TUO de la LTAIP y artículo 15-B del Reglamento de la LTAIP.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

- Sobre la legitimidad del tratamiento de datos personales de funcionarios y/o servidores públicos por sistemas de videovigilancia y su permeabilidad con el régimen de excepciones de la LTAIP.
- Sobre la calificación de acto violatorio de derechos humanos de la LTAIP: el carácter no protegido de la información relacionada a la violación de derechos humanos.
- Sobre la responsabilidad por la difusión o entrega de información protegida: a propósito del régimen sancionador de la LTAIP y la LPDP.

III. ANÁLISIS

A. Sobre el tratamiento de datos personales derivado de la videovigilancia y su conformidad legal

7. La LPDP tiene como objeto garantizar el derecho fundamental a la protección de los datos personales, previsto en la Constitución Política del Perú, artículo 2, numeral 6, que señala que toda persona tiene derecho *“a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.”*
8. 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.”*
9. Asimismo, el Reglamento de la Ley de Protección de Datos Personales, aprobado a través del Decreto Supremo N° 003-2013-JUS (en adelante, el “Reglamento de la LPDP”), desarrolla - en su artículo 2, numeral 4 - la definición de datos personales, señalando que es *“aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.”*
10. Por su parte, el numeral 19 del artículo 2 de la LPDP define tratamiento de datos personales como *“cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales”*.
11. La LPDP desarrolla los principios rectores para el tratamiento de los datos personales, entre ellos, el principio de consentimiento que se encuentra recogido en el artículo 5

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

de la LPDP y que establece que para todo tratamiento de datos debe mediar consentimiento de su titular.

12. No obstante, el artículo 14 de la LPDP dispone una serie de excepciones que permite realizar tratamiento de datos sin obligación de obtención previa del consentimiento, como las siguientes:
- Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias. (LPDP, artículo 14, numeral 1)
 - Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público. (LPDP, artículo 14, numeral 2)⁵
 - Cuando se hubiera aplicado un procedimiento de anonimización o disociación. (LPDP, artículo 14, numeral 8)
 - Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales (LPDP, artículo 14, numeral 9)
 - Cuando deriven del ejercicio de competencias expresamente establecidas por Ley (LPDP, artículo 14, numeral 13)
13. Cabe mencionar que el artículo 14 de la LPDP establece las circunstancias que constituyen excepción a la obligación de solicitar el consentimiento, pero no exonera del cumplimiento de los demás principios o disposiciones, tales como el principio de proporcionalidad⁶, legalidad⁷, seguridad⁸, deber de confidencialidad⁹, entre otros.

⁵ El artículo 17 del Reglamento de la LPDP establece las fuentes accesibles al público.

⁶ 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.”

⁷ LPDP

“Artículo 4. Principio de legalidad

El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.”

⁸ LPDP

“Artículo 9. Principio de seguridad

El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.”

⁹ LPDP

“Artículo 17. Confidencialidad de datos personales

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.

El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

14. La captación y almacenamiento de imágenes o voz que identifiquen o permitan identificar a una persona a través de sistemas de videovigilancia constituyen tratamientos de datos personales, por lo que deben realizarse de acuerdo a las disposiciones de la LPDP y su reglamento.
15. Dada la particularidad del tratamiento de datos personales a través de sistemas de videovigilancia, la ANPD aprobó, a través de la Resolución Directoral N° 02-2020-JUS/DGTAIPD, la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia (en adelante La Directiva de Videovigilancia)¹⁰, que tiene como objetivo “establecer las disposiciones para el tratamiento de datos personales captados a través de sistemas de videovigilancia con fines de seguridad, control laboral y otros, de conformidad con lo establecido en la Ley N° 29733 y su reglamento.”
16. Es decir, a través de la Directiva de Videovigilancia, la ANPD desarrolla cómo cumplir con la LPDP y su reglamento cuando se realice tratamiento de datos mediante sistemas de videovigilancia.
17. La Directiva de Videovigilancia en el artículo 5.4, define al tratamiento de datos personales mediante sistemas de videovigilancia a *“cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de la imagen o voz, captados por medio de un sistema de cámaras fijas o móviles ya sea en tiempo real o en visualización de grabaciones de imágenes, vídeos o audios.”*
18. Asimismo, establece, en el artículo 6.3, en qué casos existe legitimación para el tratamiento de datos mediante sistemas de videovigilancia:

“6.3 Existe legitimidad para el tratamiento de datos personales mediante sistemas de videovigilancia cuando se cuente con alguno de los siguientes supuestos:
6.3.1 Se cuente con el consentimiento del titular de los datos personales.
6.3.2 Una norma con rango de ley habilite a captar los datos sin el consentimiento de los titulares.
6.3.3 Se dé alguna de las circunstancias previstas en el artículo 14 de la LPDP.”
19. Es necesario señalar que el Decreto Legislativo N° 1218, Decreto Legislativo que regula el uso de las cámaras de videovigilancia, de acuerdo al artículo 1, regula “el uso de cámaras de videovigilancia en bienes de dominio público, vehículos de servicio de

ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.”

¹⁰ Disponible en: <https://www.gob.pe/institucion/anpd/informes-publicaciones/1938476-directiva-para-el-tratamiento-de-datos-personales-mediante-sistemas-de-videovigilancia>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

transporte público de pasajeros y establecimientos comerciales abiertos al público con un aforo de cincuenta (50) personas o más, como instrumento de vigilancia ciudadana, para la prevención de la violencia y del delito, así como el control y persecución del delito o falta en el marco del Sistema Nacional de Seguridad Ciudadana.”

20. En ese marco, el artículo 13 del Decreto Legislativo 1218 establece obligaciones en la captación y grabación de imágenes, videos o audios a través de sistemas de videovigilancia:

“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:

- a. Cuando aparezcan personas identificables deben observar los principios y disposiciones de la normativa de protección de datos personales.
 - 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.”
21. Por lo tanto, a decir de la normativa citada, prescindiendo del consentimiento de los titulares del derecho, y en el contexto de labores de videovigilancia, existe plena habilitación legal para el tratamiento (captación, grabación, almacenamiento, cuando menos) de datos personales (imagen y voz) por parte de personas naturales o jurídicas, entidades públicas o privadas propietarias o poseedoras de cámaras de videovigilancia. Esta habilitación –claro está– se sujeta a los límites preconfigurados en la normativa citada, tanto de modo explícito, a decir de los supuestos de hecho descritos en ella¹¹, como en términos abstractos, por los principios generales que recoge: finalidad, proporcionalidad, seguridad.

B. Sobre la accesibilidad de la información captada en labores de videovigilancia

22. La información registrada en labores de videovigilancia es perfectamente accesible, en términos materiales, siempre que exista un soporte desde el cual reproducir en copia la información o visionarla en sitio. La accesibilidad viene dada por la acción de algunos actores muy bien determinados:
- El propio titular del dato personal. Su acceso está regulado en el numeral 6.31 de la Directiva N° 01-2020-DGTAIPD y antes por el artículo 19 de la LPDP. Es de destacar también que el artículo 4 del Reglamento del Decreto Supremo N° 1218, aprobado por el Decreto Supremo N° 007-2020-IN, hace una remisión expresa, en

¹¹ Espacios públicos de uso privado (baños, vestuarios), entornos escolares íntimos, lugares destinados al descanso o esparcimiento de trabajadores; entre otros. Ver numerales 7.1, 7.5 y 7.15 de la citada Directiva N° 01-2020-JUS/DGTAIPD.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

- lo que se refiere a la Protección de Datos Personales, a las disposiciones de la Ley N° 29733, su reglamento y normativa¹².
- La Policía Nacional-Ministerio Público. Su acceso está respaldado por sus propias leyes orgánicas o como consecuencia de ser los receptores de la información que, por deber, están llamados a entregar los titulares del banco de datos personales o responsable del tratamiento de datos personales realizado por sistemas de videovigilancia, conforme a lo previsto en los artículos 14 y 15 del Decreto Legislativo N° 1218.¹³
 - Los sujetos expresamente habilitados por el artículo 18 del TUO de la LTAIP, en el marco de sus competencias y funciones.¹⁴
23. Por lo señalado, es notorio que en la relación arriba anotada está ausente el titular del derecho de acceso a la información pública regulado en la LTAIP.¹⁵ Y es que, a juicio de esta Autoridad Nacional, en línea con lo señalado antes¹⁶, esta información no es de acceso público.
24. En efecto, el artículo 4, literal d) del Decreto Legislativo N° 1218 establece como una regla para el uso de las cámaras de videovigilancia a la reserva, indicado que “*todo*

¹² LPDP

“Artículo 33.- Funciones de la Autoridad Nacional de Protección de Datos Personales

La Autoridad Nacional de Protección de Datos Personales ejerce las funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras siguientes:

12. Emitir las directivas que correspondan para la mejor aplicación de lo previsto en esta Ley y en su reglamento, especialmente en materia de seguridad de los bancos de datos personales, así como supervisar su cumplimiento, en coordinación con los sectores involucrados.”

¹³ El artículo 159 de la Constitución Política y el artículo 1 de su Ley Orgánica, aprobada por Decreto Legislativo N° 052 establecen como una de las atribuciones del Ministerio Público, conducir desde su inicio la investigación del delito. Con tal propósito, la Policía Nacional está obligada a cumplir los mandatos del Ministerio Público en el ámbito de su función. Por su parte, los artículos 60 y 61 del Nuevo Código Procesal Penal, aprobado por el Decreto Legislativo N° 957, señalan que, en razón de su función de perseguir el delito, el Ministerio Público debe conducir la investigación preparatoria, practicar y ordenar los actos de investigación que correspondan, así como solicitar al juez las medidas que considere necesarias cuando correspondan, salvo que pudiese afectarse la seguridad nacional, entre otros.

Por su parte, el artículo 67 del Nuevo Código Procesal Penal, en el marco de la función de investigación de la Policía, se encuentra facultada, inclusive por propia iniciativa, tomar conocimiento de los delitos y dar cuenta inmediata al fiscal, sin perjuicio de realizar las diligencias de urgencia e imprescindibles para impedir sus consecuencias, individualizar a sus autores y partícipes, reunir y asegurar los elementos de prueba que puedan servir para la aplicación de la ley penal. Similar función desarrollará tratándose de delitos dependientes de instancia privada o sujetas a ejercicio privado de la acción penal.

¹⁴ TUO de la LTAIP

“Artículo 18.- (...) La información contenida en las excepciones señaladas en los artículos 15, 16 y 17 son accesibles para el Congreso de la República, el Poder Judicial, el Contralor General de la República; el Defensor del Pueblo y el Superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.”

¹⁵ Su acceso, como se sabe, está regulado en el artículo 2, inciso 5 de la Constitución; y, particularmente, en la LTAIP.

¹⁶ Opinión Consultiva N° 55-2020-DGTAIPD. “Sobre la accesibilidad de las imágenes, videos y/o audios captados por cámaras de videovigilancia ubicadas en bienes de dominio público”. Disponible en: <https://bit.ly/3EPrRx0>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

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 (subrayado agregado). A primera vista, la norma citada no dispone que la información en cuestión sea reservada o que tenga tal carácter (y, en esa medida, crearía una excepción al acceso), sino que en caso un funcionario o servidor público conozca dicha información su obligación es mantenerla en reserva.

25. Esta primera lectura podría incluso respaldarse con jurisprudencia del Tribunal Constitucional, que determina que las excepciones al acceso a la información pública, para ser válidas, deben estar previstas en la ley (aunque también en Decretos Legislativos) **de forma expresa y estricta**¹⁷, es decir, ser claras y específicas, así como no generar dudas sobre su existencia. Además, deben perseguir objetivos legítimos, ser estrictamente necesarias; y, ser proporcionales con el grado de restricción del derecho de acceso a la información pública.¹⁸
26. Siguiendo esta lectura, el artículo 4, literal d) del Decreto Legislativo N° 1218 no establecería una excepción o limitación al acceso, de acuerdo con los parámetros constitucionales señalados *ut supra*, sino únicamente una “**obligación de reserva**” (o *no divulgación*) sobre los funcionarios y servidores públicos que conozcan la información referida a *imágenes, videos o audios captados por las cámaras de videovigilancia*. Ello al igual que lo señalado, por ejemplo, entre otras normas, en el artículo 241.2, numeral 5 del Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, que establece como uno de los deberes de las entidades que realizan actividad de fiscalización “guardar reserva sobre la información obtenida en la fiscalización”¹⁹.
27. Sin embargo, esta lectura es equivocada. A juicio de esta Autoridad Nacional, el escenario público captado en imágenes y voces de personas, es decir, videovigilado,

¹⁷ Sentencia recaída en el Expediente 00005-2013-PI/TC, fundamento jurídico 29.

¹⁸ Así, a modo de ejemplo, puede verse la excepción creada por la Décimo Cuarta Disposición Complementaria Final de la Ley 30225, Ley de Contrataciones del Estado, respecto a los bancos de preguntas, en los siguientes términos: “**Décimo Cuarta.** La información contenida en el banco de preguntas utilizado para la rendición del examen para la certificación de los profesionales y técnicos de los órganos encargados de las contrataciones, y en el banco de preguntas para la evaluación de árbitros para su inscripción en el Registro Nacional de Árbitros que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE), se encuentra sujeta a la excepción al ejercicio del derecho de acceso a la información, por calificar como información confidencial, (subrayado y negritas agregados)”. Esta excepción especial creada por la normativa de contrataciones públicas válidamente puede oponerse (y, en concordancia con el artículo 17 inciso 6 del TUO de la LTAIP) ante una solicitud de acceso a la información pública, por ser expresa y estricta. Es evidente y no deja un margen de interpretación sobre el tipo de información que pretende cautelarse.

¹⁹ Al respecto, esta Autoridad sostuvo que dicha norma “(...) no prescribe expresamente que toda la información obtenida en el marco de la actividad de fiscalización está exceptuada del acceso público, sino establece un deber general y especial de discreción para la autoridad fiscalizadora que accede a dicha información, lo cuales deben cumplirse en armonía con las obligaciones de transparencia desarrolladas en la normativa de transparencia y acceso a la información pública” (subrayado agregado). Opinión Consultiva N° 19-2020-JUS/DGTAIPD. “Sobre el carácter público de la información obtenida en el marco de la actividad administrativa de fiscalización de la potestad fiscalizadora de la Administración Pública”. Disponible en: <https://bit.ly/3Yn0AZW>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de
Transparencia, Acceso
a la Información Pública y
Protección de Datos Personales

“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

no puede ser de dominio público por regla general y no puede serlo por la alta incidencia sobre la seguridad, orden público y privacidad de las personas involucradas.

28. En efecto, la escena pública es ese espacio urbano o rural donde se desenvuelve la vida social; donde se dan las interacciones entre las personas y donde se pone de manifiesto –sea que se observen o no– valores o bienes jurídicos fundamentales de la sociedad como el orden público²⁰ o la seguridad ciudadana²¹.
29. El Estado tiene un compromiso frente a la sociedad para que impere el orden público y la seguridad ciudadana y es por ello que, en ese esquema, resulta razonable la limitación de derechos. Como lo dice el propio Tribunal Constitucional, *“el Estado puede establecer medidas limitativas o restrictivas de la libertad de los ciudadanos con el objeto que, en el caso específico de la defensa de valores como la paz o de principios como la seguridad, se evite la consumación de actos que puedan producir perturbaciones o conflictos. De allí que en resguardo del denominado orden material –elemento conformante del orden público– el Estado procure la verificación de conductas que coadyuven al sostenimiento de la tranquilidad pública, el sosiego ciudadano, etc.”*²²
30. Una de esas medidas es la videovigilancia en espacios públicos. Ella sola es ya una intromisión –aunque legitimada– en la esfera personal de los individuos que se convierten en objetivos involuntarios de ella; en la medida que hay captación de imágenes (y a veces voces) sin su consentimiento, lo que produce una afectación –aunque sea razonable y proporcional– sobre su privacidad y autodeterminación informativa.

²⁰ En palabras del Tribunal Constitucional, “El orden público es el conjunto de valores, principios y pautas de comportamiento político, económico y cultural en sentido lato, cuyo propósito es la conservación y adecuado desenvolvimiento de la vida coexistencial. En tal sentido, consolida la pluralidad de creencias, intereses y prácticas comunitarias orientadas hacia un mismo fin: la realización social de los miembros de un Estado. El orden público alude a lo básico y fundamental para la vida en comunidad, razón por la cual se constituye en el basamento para la organización y estructuración de la sociedad.” (Sentencia recaída sobre el Expediente N° 3283-2003-AA/TC, fundamento jurídico 28).

²¹ En palabras del Tribunal Constitucional, se trataría de “(...), un estado de protección que brinda el Estado y en cuya consolidación colabora la sociedad, a fin de que determinados derechos pertenecientes a los ciudadanos puedan ser preservados frente a situaciones de peligro o amenaza o reparados en caso de vulneración o desconocimiento. Derechos como la vida, la integridad, la tranquilidad, la propiedad o la libertad personal suelen los principales referentes que integran el contenido de la seguridad ciudadana en atención a lo que del Estado y la colectividad se espera, siendo evidente que, por sus alcances, se trata fundamentalmente de un bien jurídico de relevancia antes que de un tributo o libertad a título subjetivo. (...). En el Estado social de derecho, por otra parte, es incuestionable la existencia de roles vitales en relación con la consecución de grandes objetivos. Vista la seguridad ciudadana como uno de esos roles en los que todo Estado se compromete, no cabe discusión alguna respecto del papel relevante que le toca cumplir y la especial posición que el ordenamiento constitucional le suele otorgar. (Sentencia recaída sobre el Expediente N° 3482-2005-PHC/TC, f.j. 13-14).

²² STC, recaída sobre el Expediente N° 3283-2003-AA/TC, f.j. 29.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”



BICENTENARIO
DEL PERÚ
2021 - 2024





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

31. Si esto es así, como creemos que lo es, cobra sentido que la ANPD haya advertido en el pasado que esta visualización de imágenes no pueda estar a disposición de cualquier vecino en tiempo real²³, como aparentemente pretendían algunas comunas capitalinas, a decir de publicitados anuncios en sus distritos.²⁴ La videovigilancia con fines de seguridad ciudadana supone un tratamiento de datos personales que no puede realizar cualquiera, sino sólo aquellos que cuentan con legitimidad legal para ello, como el propio personal de la municipalidad dedicado a labores de seguridad en el distrito, amén del cumplimiento de las funciones previstas en la Ley Orgánica de Municipalidades.²⁵
32. Esta posición, luego, ha sido reafirmada en la Opinión Consultiva N° 55-2020-JUS/DGTAIPD, donde esta Autoridad sostuvo que las imágenes, videos o audios captados por cámaras de videovigilancia ubicados en bienes de dominio público no constituyen información pública por formar parte de las excepciones y ser información confidencial. Ello en virtud del Decreto Legislativo N° 1218, que regula el uso de cámaras de videovigilancia (en adelante, Decreto Legislativo 1218) en concordancia

²³ Ver nota de prensa del Ministerio de Justicia y Derechos Humanos del 22 de agosto de 2019: <https://www.gob.pe/institucion/minjus/noticias/50061-minjusdh-plantea-directiva-para-uso-de-cameras-de-videovigilancia-conforme-a-la-ley-de-proteccion-de-datos-personales>

²⁴ En efecto, desde una imputación realizada por la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, el año 2018 (Resolución Directoral N° 03-2018-JUS/DGTAIPD-DFI), es claro que –para el órgano instructor de la ANPD– permitir a vecinos de un distrito acceder a imágenes captadas por las cámaras de videovigilancia de una municipalidad, en tiempo real, configura un tratamiento no proporcional a la finalidad que justifica la vigilancia y resguardo de la seguridad ciudadana.

²⁵ Ley 27972, Ley Orgánica de Municipalidades

“Artículo 85. - Seguridad Ciudadana

Las municipalidades en seguridad ciudadana ejercen las siguientes funciones:

1. Funciones específicas exclusivas de las municipalidades provinciales:
 - 1.1 Establecer un sistema de seguridad ciudadana, con participación de la sociedad civil y de la Policía Nacional, y normar el establecimiento de los servicios de serenazgo, vigilancia ciudadana, rondas urbanas, campesinas o similares, de nivel distrital o del de centros poblados en la jurisdicción provincial, de acuerdo a ley.
 - 1.2 Ejercer la labor de coordinación para las tareas de defensa civil en la provincia, con sujeción a las normas establecidas en lo que respecta a los Comités de Defensa Civil Provinciales.
2. Funciones específicas compartidas de las municipalidades provinciales:
 - 2.1 Coordinar con las municipalidades distritales que la integran y con la Policía Nacional el servicio interdistrital de serenazgo y seguridad ciudadana.
 - 2.2 Promover acciones de apoyo a las compañías de bomberos, beneficencias, Cruz Roja y demás instituciones de servicio a la comunidad.
3. Funciones específicas exclusivas de las municipalidades distritales:
 - 3.1 Organizar un servicio de serenazgo o vigilancia municipal cuando lo crea conveniente, de acuerdo a las normas establecidas por la municipalidad provincial respectiva.
 - 3.2 Coordinar con el Comité de Defensa Civil del distrito las acciones necesarias para la atención de las poblaciones damnificadas por desastres naturales o de otra índole.
 - 3.3 Establecer el registro y control de las asociaciones de vecinos que recaudan cotizaciones o administran bienes vecinales, para garantizar el cumplimiento de sus fines.”

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

con lo señalado en el artículo 17 inciso 6 del TUO de la LTAIP que admite la creación de excepciones en virtud de Decretos Legislativos²⁶.

33. Más aún, respecto a la captación de imágenes (o voces) sobre la comisión de un delito o falta, a través de cámaras de videovigilancia, la entidad propietaria o poseedora de las mismas debe entregar dicha información a las autoridades policiales o fiscales competentes (en aplicación del artículo 14 del Decreto Legislativo 1218), a efectos de coadyuvar en la investigación o represión del delito. Ello, en virtud de que esta información debe estar en manos de aquellos a quienes les corresponde utilizarla o tratarla para los fines antes descritos. Y no otros.²⁷
34. Ahora bien, cierto es que el Decreto Legislativo N° 1218 no establece de manera expresa que esta información (captada por cámaras de videovigilancia) se califique como una excepción al acceso a la información pública. Un deber de reserva, tal cual como se recoge en el citado dispositivo, no podría equipararse a una calificación jurídica definitiva de confidencialidad, según se anota en el párrafo 26 de la presente Opinión Consultiva.
35. Sin embargo, este Despacho que ejerce por encargo de las leyes sustantivas, ambas autoridades nacionales, no puede eximirse de su deber de interpretar, a propósito de las consultas que recibe y así lo exigen, el sentido de las normas que concurren a la interpretación de las normas bajo su ámbito competencial y de los fines constitucionales que persiguen. En otros términos, esta Autoridad debe necesariamente pronunciarse si bajo la excepción prevista en el artículo 17, numeral 6, del TUO de la LTAIP²⁸, puede entenderse que la información captada por cámaras de videovigilancia, objeto de regulación por el Decreto Legislativo N° 1218, es o no, en términos generales y en abstracto, de naturaleza confidencial; y, por ende, no accesible por regla.

²⁶ Al respecto, esta Autoridad ha sostenido que dicho dispositivo legal admite la posibilidad de crear otros supuestos de exclusión al derecho de acceso a la información pública (en estricto, supuesto de adicionales de información confidencial), a través de la Constitución o Ley aprobada por el Congreso de la República y también a través de decretos legislativos (es decir, no solo por leyes formales), por cuanto, este tipo de normas, aunque son emitidas por el Ejecutivo vía delegación, tienen rango legal, constituyen acto legislativo y son pasibles de control por el Congreso de la República. Opinión Consultiva N° 30-2019-JUS/DGTAIPD. “Respecto al acceso a la información contenida en actas de sesiones de un órgano colegiado y en actas de un procedimiento administrativo sancionador y las excepciones al acceso público en virtud de lo establecido en el inciso 6 del artículo 17 de la Ley 27806”. Disponible en: <https://bit.ly/3uueOtm>

²⁷ Para otros fines vinculados a sus propias competencias y funciones, está la habilitación para su acceso por parte de las entidades descritas en el citado artículo 18 del TUO de la LTAIP.

²⁸ TUO de la LTAIP

“Artículo 17.- Excepciones al ejercicio del derecho: Información confidencial

El derecho de acceso a la información pública no podrá ser ejercido respecto de lo siguiente:

(...).

6. Aquellas materias cuyo acceso esté expresamente exceptuado por la Constitución o por una Ley aprobada por el Congreso de la República.”

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

36. La información que capta una cámara de videovigilancia es variada. Puede captar objetos inanimados, la acción e interacción de personas u otros seres vivos, sucesos de la naturaleza, lo que incluye a la flora del lugar. Pero la información captada en razón de salvaguardar el orden público y la seguridad ciudadana, se centra en la interacción humana.
37. En efecto, si el espacio público es ese escenario en el cual las personas interactúan entre ellas y su entorno, es claro que si se videovigila con fines de seguridad, hay una intromisión –aunque razonable y justificada– en la esfera personalísima de los individuos, en la medida que el propósito de esas cámaras es captar a personas (no a objetos inanimados), titulares del derecho a la privacidad (que no cesa del todo por el mero hecho de estar en un lugar público) y del derecho a la protección de datos personales, dado que su imagen y voz, son bienes que le pertenecen.
38. Si esto es así, es razonable que opere una presunción de confidencialidad sobre aquello que capte el lente de dichas cámaras²⁹; de lo contrario, estaríamos admitiendo que, por regla general, cualquier persona en el ejercicio de su derecho de acceso a la información pública (LTAIP) pueda acceder a la imagen y voz de cualquier otra por la mera circunstancia de haber sido captada por una cámara de una entidad pública, por citar un ejemplo. Y es que, el tratamiento de videovigilar puede provenir de una entidad pública, pero lo que capta (revista o no interés público) es un bien ajeno, la imagen o la voz de una persona.
39. Puede ocurrir que el interés público, en determinados contextos, derruya esta deferencia para con la privacidad y los datos personales de otro, y habilite a un individuo o entidad a divulgar esta información, si la tiene, pero lo que no se puede es aceptar la idea de que lo que prime en el escenario público, captado por videovigilancia, sea el principio de acceso y no el de confidencialidad. De ser así, no tendría que haber ningún reparo para que cualquiera visionara en tiempo real la videovigilancia de su distrito; y sobre ello ya se ha comentado cuál la posición de este Despacho.
40. En esta misma línea se ha pronunciado la Corte Constitucional de Colombia.³⁰ Lo hizo a propósito del cuestionamiento sobre la constitucionalidad del artículo 237 de la Ley 1801 de 2016, Código de Policía, que establece que la información, imágenes y datos de cualquier índole, captados y/o almacenados por los sistemas de video o los medios tecnológicos que estén ubicados en el espacio público o en lugares abiertos al público serán considerados como públicos y *de libre acceso*.

²⁹ Incluso si no capta “nada”, porque la mera información sobre el ángulo de registro de imágenes puede informar de “puntos de ciegos” a la lente, que bien podrían menoscabar objetivos de prevención del delito si esta información cayera en malas manos.

³⁰ Sentencia C-094/20.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

41. En dicha oportunidad, el Colegiado colombiano opinó que “atribuir la condición de pública a la información, datos o imágenes captados por cámaras instaladas en espacios públicos, supone una generalización de los datos e imágenes -la de público, sin considerar el contenido que se obtiene. En otras palabras, si bien podría considerarse que, como regla general, los datos captados en espacios públicos³¹ o semipúblicos³² son, en esencia, públicos, existe la posibilidad de que la información allí captada pueda ser semiprivada³³, privada³⁴ o reservada, por lo que permitir su libre acceso podría contravenir los postulados de la Constitución (...).”³⁵
42. En palabras sencillas, el derecho a la intimidad no tiene relevancia únicamente en espacios privados. En espacios públicos, semipúblicos y semiprivados hay una “esfera de protección que se mantiene vigente”³⁶. Y ello es así en la medida que la vida privada es un “espacio personal y ontológico”³⁷. A juicio de esta Autoridad Nacional, lo mismo puede decirse del derecho a la protección de datos personales o de autodeterminación informativa. La información, que es tratada como dato personal, puede ser catalogada como pública, semiprivada, privada y reservada (sensible)³⁸; y, por ello mismo, su tratamiento debe sujetarse a los principios rectores de la Ley de Protección de Datos

³¹ Según definidos por la propia Corte (Sentencia T-407 de 2012), como el “lugar de uso común en el que los ciudadanos ejercen numerosos derechos y libertades”. Este tipo de espacios, “se caracterizan por ser lugares de socialización, interacción, intercambio, integración y de encuentro para los ciudadanos (...)”.

³² Según la Corte (Sentencia T-407 de 2012), son “lugares de acceso relativamente abierto en los que diferentes personas se encuentran en determinado momento para realizar cierta actividad puntual dentro de un espacio compartido”.

³³ Según la Corte (Sentencia T-407 de 2012), se trata de “espacios cerrados en los que un conjunto de personas comparte una actividad y en los que el acceso al público es restringido”.

³⁴ Según la Corte (Sentencia T-574 de 2017), es el lugar en el que las personas desarrollan su personalidad y ejercen su intimidad de manera libre en un ambiente inalienable, inviolable y reservado. También apunta que, si bien el espacio privado se asocia con el concepto de domicilio, esta idea va más allá y abarca “además de los lugares de habitación, trabajo, estudio, todos aquellos espacios o recintos aislados en los que la persona normal y legítimamente pretenda desarrollar su propia vida privada, separada de los terceros y sin su presencia” (Sentencia C-041 de 1994).

³⁵ Párrafo 151.

³⁶ Corte Constitucional Colombiana, Sentencia T-787 de 2004, reiterada en la Sentencia T-634 de 2013.

³⁷ Es decir, un espacio de personalidad de los sujetos (Sentencia C-881 de 2014) que comprende, entre otros, espacios físicos, psicológicos y relacionales de los individuos.

³⁸ Sentencia C-094/20, párrafo 153.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

Personales, como lo son el principio de consentimiento³⁹, el principio de finalidad⁴⁰, el principio de proporcionalidad⁴¹ o el principio de seguridad.⁴²

43. Por lo tanto, una solución “a la colombiana” –que creemos acertada también para el caso de nuestro ordenamiento jurídico– es aplicar el principio de armonización concreta o, como lo llamamos aquí, principio de concordancia práctica⁴³, con el propósito de guardar la integridad de la Constitución.
44. Así, en determinados casos como los de videovigilancia regulados en el Decreto Legislativo N° 1218, donde trasunta un fin legítimo asociado a la seguridad ciudadana y a la preservación del orden público, no hará falta recabar el consentimiento de los captados en videocámara en un espacio público, por ejemplo; pero, a la par, no sería admisible un acceso indiscriminado a imágenes, toda vez que pueden haber datos captados que respondan a espacios semiprivados, privados o reservados de los individuos, lo que podría implicar una vulneración irrazonable y desproporcionada a la intimidad-vida privada de los mismos o, directamente, a su derecho a la protección de los datos personales.
45. Por ello, al igual que concluye la Corte Constitucional colombiana⁴⁴, este Despacho estima que, por regla general y en el ámbito general y abstracto de interpretación de

³⁹ LPDP

“Artículo 5. Principio de consentimiento

Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.”

⁴⁰ LPDP

“Artículo 6. Principio de finalidad

Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.”

⁴¹ 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.”

⁴² LPDP

“Artículo 9. Principio de seguridad

El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.”

⁴³ “En virtud del cual toda aparente tensión entre las propias disposiciones constitucionales debe ser resuelta “optimizando” su interpretación, es decir, sin “sacrificar” ninguno de los valores, derechos o principios concernidos, y teniendo presente que, en última instancia, todo precepto constitucional, incluso aquellos pertenecientes a la denominada “Constitución orgánica” se encuentran reconducidos a la protección de los derechos fundamentales, como manifestaciones del principio-derecho de dignidad humana, cuya defensa y respeto es el fin supremo de la sociedad y el Estado (artículo 1 ° de la Constitución)”. En: Sentencia del Tribunal Constitucional recaída en el Expediente N° 5854-2005-PA/TC, f.j. 12.

⁴⁴ Que termina por considerar la expresión “libre acceso” del cuestionado artículo 237 de la Ley 1801 en un sentido que conlleve al conocimiento de esta información sólo a las autoridades públicas y en los casos en los que esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

las normas –ámbito desde el cual opina–, no es accesible esta información por cualquier solicitante a través del ejercicio del derecho de acceso a la información pública regulado en la LTAIP.

C. Sobre la legitimidad en el tratamiento de datos personales de funcionarios y/o servidores públicos por sistemas de videovigilancia y la inaplicabilidad, en su caso, de la excepción al acceso a la información prevista en el artículo 17, inciso 5, de la LTAIP, en el contexto de escenarios públicos de desempeño funcional

46. La posición desarrollada en el acápite anterior está afinada en un supuesto genérico de interpretación de las normas. Pero la consulta, en uno de sus extremos, nos sitúa en un escenario más concreto: espacio público donde se desarrolla una protesta social y se capta imágenes de efectivos del orden (militares y/o policías) en el desempeño de sus funciones.
47. En el párrafo 39 de la presente, ya se advierte que, pese a la presunción (o regla general de) confidencialidad sobre las imágenes y voces captadas a través de sistemas de videovigilancia, materializada en el Decreto Legislativo N° 1218 como regla de reserva (artículo 4), puede ocurrir que, en determinados contextos, uno de los actores habilitados para el acceso a esta información (ver párrafo 22) encuentre en el *interés público* una razón que discurra en la dirección opuesta y que lo habilite jurídicamente a divulgar la información que conoce o tiene en su poder.
48. ¿Qué variable o elementos tienen que estar presentes en el llamado interés público para que advirtamos la presencia de una norma permisiva que habilite la divulgación de esta información que, en principio, es confidencial? No es un asunto que este Despacho pueda responder dados los límites en los que se circunscribe su función consultiva. Sin embargo, sí hay algunos aspectos que esta Autoridad ha señalado antes y que pueden resultar pertinentes traer a colación.
49. Esta Dirección General ha emitido diversos pronunciamientos⁴⁵ sobre la particularidad que reviste el tratamiento de datos personales de los funcionarios y/o servidores

que la misma sea útil para la realización de los fines identificados (seguridad ciudadana). Cfr: párrafo 156 de la Sentencia C-094/20.

⁴⁵ Opiniones de la DGTAIPD en materia de tratamiento de datos personales de funcionarios/servidores públicos:

- Opinión Consultiva N° 01-2021-JUS/DGTAIPD: Sobre publicidad de fotografías de funcionarios y servidores públicos en portales web de las entidades de la Administración Pública. Disponible en <https://www.gob.pe/institucion/anpd/informes-publicaciones/3822333-oc-n-01-2021-jus-dgtaipd-sobre-la-publicidad-de-fotografias-de-funcionarios-y-servidores-publicos-en-portales-web-de-las-entidades-de-la-administracion-publica>
- Opinión Consultiva N° 37-2019-JUS/DGTAIPD: Sobre el acceso de los datos de los funcionarios públicos a través de solicitudes de acceso a la información pública. Disponible en <https://www.gob.pe/institucion/anpd/informes-publicaciones/1374580-oc-n-37-2019-jus-dgtaipd-sobre-el->

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

públicos, en tanto existe interés público por parte de la ciudadanía en conocer y vigilar cómo se desempeña y se ejerce el cargo público al estar vinculado al uso de recursos del Estado. Consecuentemente, los datos personales de funcionarios y/o servidores públicos, en tanto no afecten la intimidad de su titular, podrían ser entregados ante una solicitud de acceso a la información pública, debiendo el poseedor de la información evaluar qué datos corresponden ser entregados y cuáles otros deben mantenerse en reserva, en observancia del inciso 5 del artículo 17 de la LTAIP.

50. El numeral 5 del artículo 17 del TUO de la LTAIP excluye del acceso a la información pública a *“La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso, solo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución Política del Perú”*. Cabe mencionar que esta excepción solo aplica a aquellos datos personales que, de exponerse al dominio público, comprometan o afecten la intimidad personal o familiar de su titular.
51. Mediante Opinión Consultiva N°044-2018-JUS/DGTAIPD, esta Dirección determinó que *“al tratarse de funcionarios o servidores públicos es necesario que puedan ser identificados por los ciudadanos, tanto para el control ciudadano como para el desarrollo de los procedimientos en los que fueran parte o de los servicios que solicitan. Por lo tanto, conforme a los principios de “razonabilidad” y de “proporcionalidad”, es razonable que se pueda entregar la imagen de un funcionario o servidor público contenida en su ficha personal o en el documento proporcionado por la entidad a efectos de ser identificado como funcionario o servidor público por los ciudadanos.”*
52. De igual manera en la Opinión Consultiva N° 37-2019-JUS/DGTAIPD, esta Dirección determinó que *“Tratándose de información sobre el funcionariado público o de personas que pretenden vincularse con el aparato estatal, se debe ponderar el apremiante interés público por conocer la información relacionada a los datos personales de estos para, a partir de ello, ejercer otros derechos como la vigilancia y participación ciudadana.”*

[acceso-a-los-datos-personales-de-los-funcionarios-publicos-a-traves-de-las-solicitudes-de-acceso-a-la-informacion-publica](#)

- Opinión Consultiva N° a 044-2018-JUS/DGTAIPD: Sobre si se debe entregar por acceso a la información pública las fotos que incluyen algunos diplomas que sustentan la información académica, así como las notas que los postulantes obtienen en cada curso entre otros. Disponible en www.gob.pe/institucion/anpd/informes-publicaciones/3822743-oc-n-44-2018-jus-dgtaipd-sobre-si-se-debe-entregar-por-acceso-a-la-informacion-publica-las-fotos-que-incluyen-algunos-diplomas-que-sustentan-la-informacion-academica-asi-como-las-notas-que-los-postulantes-obtienen-en-cada-curso-entre

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

53. Así también en la Opinión Consultiva N° 01-2021-JUS/DGTAIPD se hizo referencia al criterio desarrollado por el Tribunal Constitucional en la Sentencia recaída en el Expediente N° 03079-2014-PA/TC al señalar:

“61. (...) en el ámbito de la discusión del derecho a la intimidad de las personas con proyección pública, altos cargos públicos o simplemente funcionarios públicos, este Tribunal ya ha referido que el umbral de protección se ve reducido debido a que dichas personas, desde el momento en que han decidido asumir cargos públicos, se exponen, de manera voluntaria, a un mayor escrutinio público acerca del modo en que ejercen la función.”

(...)

86. Como se señaló previamente, en el caso del uso de las imágenes de funcionarios o servidores públicos, no será necesario obtener el consentimiento por parte de éstos, siempre y cuando dichas imágenes guarden relación con el cargo que desempeñan.

(...)

54. En el caso materia de consulta, respecto al tratamiento de las imágenes de funcionarios y/o servidores públicos (personal policial y militar) en el marco del cumplimiento de funciones en una manifestación social, cabe señalar que la captación de sus datos a través de las cámaras de videovigilancia responde a un evento de protesta o manifestación pública, en el cual su presencia se condice con el ejercicio de sus funciones, por lo que la expectativa de privacidad de los funcionarios y servidores se reduce considerablemente.
55. Las imágenes captadas en ese escenario concreto de protesta pública e intervención de las fuerzas del orden, pueden informar acerca de su desempeño funcional, lo que siempre es de interés público⁴⁶ y no forma parte de su vida privada, por lo que no constituye, en principio, información confidencial conforme el artículo 17, inciso 5, de la LTAIP.⁴⁷
56. No obstante, aún quedaría pendiente rebatir la confidencialidad que emana del Decreto Legislativo N° 1218 sobre toda la información captada por sistemas de videovigilancia; si allí, en razón del interés público, dadas las circunstancias concretas que deriven de un hecho registrado, una persona o entidad (de las habilitadas según párrafo 22), quiere encontrar una norma habilitadora para divulgar dicha información, será un asunto de su entera responsabilidad sustentar y, por defecto, será un asunto sobre el cual un juez o tribunal administrativo seguramente validará o no en términos argumentales. Es decir, estaríamos ante un caso concreto que obligue a decidir sobre

⁴⁶ Opinión Consultiva N° 31-2021-JUS/DGTAIPD. “Sobre la accesibilidad a la información contenida en las solicitudes de autorización para la ejecución de ensayos clínicos y referida a los datos personales de los participantes”. Disponible en: <https://bit.ly/3nRNJPf>

⁴⁷ A mayor abundamiento, cabe precisar que, si bien el artículo 15 del Código Civil dispone que la imagen y la voz no pueden ser aprovechadas (publicadas, expuestas o utilizadas) sin autorización de su titular, esta autorización no será necesaria cuando su utilización se justifique por la notoriedad de la persona, *por el cargo que desempeñe*, por hechos de importancia o interés público o por motivos de índole científica, didáctica o cultural y siempre que se relacione con hechos o ceremonias de interés general que se celebren en público.

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

la divulgación o no de la determinada información; y, sobre casos concretos este Despacho no tiene habilitación para opinar en el ejercicio de su función consultiva prevista en el artículo 4 del Decreto Legislativo N° 1353.

D. Sobre la calificación de acto violatorio de derechos humanos en el TUO de la LTAIP: el carácter no protegido de la información relacionada a la violación de derechos humanos

57. El artículo 18 cuarto párrafo del TUO de la LTAIP establece que *“las excepciones señaladas en los puntos 15 y 16 [que regulan los supuestos de información secreta y reservada] incluyen los documentos que se generen sobre estas materias y no se considerará como información clasificada, la relacionada a la violación de derechos humanos o de las Convenciones de Ginebra de 1949 realizada en cualquier circunstancia, por cualquier persona. (...)”* (subrayado agregado)
58. Por ende, si la información requerida se encuentra relacionada, entre otros aspectos, a la violación de derechos humanos realizada por cualquier persona, no podrá ser considerada como información clasificada. En la misma línea, el artículo 27 numeral 4 de la Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública, dispone que *“la Información relacionada con violaciones de los derechos humanos está sujeta a una alta presunción de divulgación, y en ningún caso podrá ser clasificada invocando razones de seguridad nacional”*.
59. Si bien el TUO de la LTAIP prohíbe considerar como información clasificada aquella relacionada a la violación de derechos humanos, no regula una definición para este tipo de información. Por ello, cabe formularse la siguiente interrogante ¿qué comprende la información relacionada a la violación de derechos humanos o qué características debe tener para ser calificada como tal?
60. Al respecto, de acuerdo con la doctrina especializada el término *“violación de derechos humanos”* supone la comisión de una determinada clase de actos atroces, tales como la tortura, la desaparición forzada o el asesinato por el Estado o sus agentes⁴⁸. La jurisprudencia de la Corte Interamericana de Derechos Humanos identifica como violaciones graves de los derechos humanos a la tortura, las ejecuciones sumarias, extralegales o arbitrarias y las desapariciones forzadas, las cuales están prohibidas por contravenir derechos reconocidos por el Derecho Internacional de los Derechos Humanos⁴⁹.
61. Por ende, la información relacionada a dichos actos atroces u otros cometidos por el Estado o sus agentes, que vulneran derechos reconocidos en instrumentos sobre

⁴⁸ Cfr. Rainer Huhle. *“La violación de los Derechos Humanos: ¿Privilegio de los Estados?”* (1993). Disponible en: <http://bit.ly/3EOkMx0>

⁴⁹ Caso Barrios Altos Vs. Perú. Sentencia de 14 de marzo de 2001, párrafo 41. Disponible en: <https://bit.ly/3kR8rkD>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

derechos humanos de ninguna manera pueden quedar excluidos del conocimiento público. Justamente, en la Opinión Consultiva N° 25-2019-JUS/DGTAIPD⁵⁰, esta Autoridad sostuvo que resulta esencial que, para garantizar el derecho a la información, los poderes públicos actúen de buena fe y realicen diligentemente las acciones necesarias para asegurar la efectividad de este derecho, especialmente cuando se trata de conocer la verdad de lo ocurrido en casos de violaciones graves de derechos humanos.

62. ¿Quién califica o debe calificar un acto como violatorio de los derechos humanos? En el ámbito que nos compete, en primer lugar, el poseedor; él es quien tiene a cargo la responsabilidad de divulgar o no la información que pretendería ser excluida del acceso o dominio público so pretexto de que la autoridad generadora de la información o una norma interpretada indebidamente la califique como tal. Esta calificación dada por el poseedor de la información, claro está, será también – ante la eventualidad de una controversia jurídica– validada o desacreditada por la autoridad normativa (juez o tribunal administrativo) que conozca la causa.

E. Sobre la responsabilidad por la difusión o entrega de información protegida: a propósito del régimen sancionador regulado por el TUO de la LTAIP y la LPDP

63. El artículo 18 quinto párrafo del TUO de la LTAIP dispone que *“los funcionarios públicos que tengan en su poder la información contenida en los artículos 15, 16 y 17 tienen la obligación de que ella no sea divulgada, siendo responsables si esto ocurre”*. Por ende, la difusión o entrega de información protegida, sin perjuicio del soporte que lo contienen, acarrearía responsabilidad en el poseedor de esta.
64. Si bien el TUO de la LTAIP y el Reglamento de la LTAIP han previsto un régimen sancionador aplicable a las acciones u omisiones que infrinjan la normativa de transparencia y acceso a la información pública⁵¹, este régimen no establece el tipo de responsabilidad en que incurre quien difunde o entrega información protegida por las excepciones ni el procedimiento para su determinación.
65. En todo caso, las acciones u omisiones que infrinjan otra normativa ajena a la transparencia y acceso a la información pública tampoco quedarían impunes, de hecho, de corresponder, serán sancionadas conforme a las normas y los procedimientos que le resulten aplicables. Si bien la norma básica para estos fines es el régimen disciplinario de la Ley N° 30057, Ley del Servicio Civil; y sus normas

⁵⁰ Sobre la interpretación del régimen de excepciones de la Ley 27806 en el ámbito de inteligencia, Sector Interior y el acceso a información clasificada por parte de los representantes del Ministerio Público. Disponible en: <https://bit.ly/3rNftqx>

⁵¹ Opinión Consultiva N° 27-2021-JUS/DGTAIPD. “Carácter especial del régimen sancionador en materia de transparencia y acceso a la información pública y las autoridades a cargo del procedimiento sancionador contra ex funcionarios y ex servidores públicos”. Disponible en: <https://bit.ly/3jcsyWz>

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

reglamentarias, pueden existir regulaciones especiales de acuerdo con los intereses, bienes jurídicos o derechos afectados.

66. Justamente, tratándose de la divulgación de datos personales, como imágenes y voces, cuya difusión o entrega supongan una afectación de la intimidad personal o familiar, la LPDP la puede sancionar en tanto esté vinculada con una infracción al deber de confidencialidad.⁵²
67. Por lo tanto, en caso un funcionario entregue información que debe mantenerse en reserva, podría vulnerar la LPDP, cometiendo una infracción grave, que puede ser sancionada hasta con 50 UIT⁵³, salvo medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública o se cuente con el consentimiento del titular del dato personal.

IV. CONCLUSIONES

1. Las imágenes y 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). Esta calificación, aún imperfecta en términos formales, responde a la naturaleza de la información registrada y de los derechos y finalidades públicas y constitucionales involucradas.
2. Por regla, sólo los actores resaltados en el párrafo 22 de la presente Opinión Consultiva, son los sujetos habilitados para su acceso. A ellos se les extiende el deber de confidencialidad sobre la información captada por sistemas de videovigilancia, máxime, cuando dicha información pueda afectar a otras personas o cuando revelen indicios razonables de la comisión de un delito o falta, pues en este último caso son las autoridades competentes (Policía Nacional y/o Ministerio Público) las destinatarias

⁵² LPDP

“Artículo 17. Confidencialidad de datos personales

El titular del banco de datos personales, el encargado y quienes intervengan en cualquier parte de su tratamiento están obligados a guardar confidencialidad respecto de los mismos y de sus antecedentes. Esta obligación subsiste aun después de finalizadas las relaciones con el titular del banco de datos personales.

El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado, expreso e inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la defensa nacional, seguridad pública o la sanidad pública, sin perjuicio del derecho a guardar el secreto profesional.”

⁵³ Reglamento de la LPDP

“Artículo 132.- Infracciones

Las infracciones a la Ley N° 29733, Ley de Protección de Datos Personales, o su Reglamento se califican como leves, graves y muy graves y se sancionan con multa de acuerdo al artículo 39 de la citada Ley.

(...)

2. Son infracciones graves:

g) Incumplir la obligación de confidencialidad establecida en el artículo 17 de la Ley N° 29733.

(...).”

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”





“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

naturales de la misma, y las que tienen trazado por ley el tratamiento que le darán en su propósito de perseguir el delito y las infracciones al orden público.

3. Un sujeto habilitado en el acceso a la información captada por sistemas de videovigilancia que considere necesario divulgar cierta información protegida sólo podrá hacerlo, en un caso concreto, bajo el entendimiento que existe una norma habilitadora y permisiva para hacerlo. La carga argumentativa de ello le corresponde a él, como sujeto poseedor. Y, en caso surja una controversia jurídica al respecto, dicha posición será refrendada o revocada por la autoridad normativa investida para ello (un juez o un tribunal administrativo).
4. La expectativa de privacidad y de protección de los datos personales de funcionarios y/o servidores públicos en el ejercicio de sus funciones se morigera notablemente; y, según el caso y el dato personal involucrado en él, puede incluso reducirse a la nada, vista la calidad del agente involucrado y el interés público que pueda despertar el hecho concreto registrado.
5. El tratamiento de las imágenes de personal policial y militar en el trámite de una protesta o manifestación social en un espacio público, en su afán de mantener el orden público y preservar la seguridad ciudadana, no supone una exclusión para su divulgación en razón de los datos personales involucrados, es decir, la no divulgación de dicha información no puede obedecer al supuesto de exclusión previsto en el artículo 17, inciso 5, de la LTAIP. Sin embargo, sí puede obedecer al supuesto que origina el inciso 6 de dicho artículo 17, dada la consideración *prima facie* sobre la confidencialidad que envuelve a la información captada por los sistemas de videovigilancia regulados en el Decreto Legislativo N° 1218.
6. La información relacionada a la violación de derechos humanos no puede ser considerada como información clasificada, en los términos del régimen de excepciones de la LTAIP. Por violación de derechos humanos debe entenderse actos atroces, tales como la tortura, la desaparición forzada o el asesinato cometidos por el Estado o sus agentes. Asimismo, cualquier otro acto cometido por el Estado o sus agentes que vulneran derechos reconocidos en instrumentos sobre derechos humanos. La calificación de dichos actos viene dada, de facto por el poseedor de la información que da cuenta de ellos; y, en términos jurídicos definitivos, por una autoridad normativa con competencia para ello.
7. El régimen sancionador de LTAIP no establece el tipo de responsabilidad en que incurre quien difunde o entrega información protegida por las excepciones ni el procedimiento para su determinación. El régimen sancionador de la LPDP sanciona el tratamiento de datos personales que pueda derivar de una infracción al deber de confidencialidad previsto en su artículo 17; dicha sanción puede significar una multa de hasta 50 UIT. La atribución de responsabilidad a un poseedor de imágenes que decide divulgarlas por considerarlas de interés público responde a una valoración en

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda.”



“Decenio de la igualdad de oportunidades para mujeres y hombres”

“Año de la unidad, la paz y el desarrollo”

concreto de un caso. Así, una respuesta concluyente sobre el mismo escapa a la valoración en abstracto y general que hace esta Autoridad en ejercicio de su función consultiva prevista en Ley.

Aprobado por:	Aprobado por:
Eduardo Luna Cervantes Dirección General de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales	María Alejandra González Luna Directora (e) de la Dirección de Protección de Datos Personales

Esta es una copia auténtica imprimible de un documento electrónico archivado por el Ministerio de Justicia y Derechos Humanos, aplicando lo dispuesto por el Art. 25 del D.S. 070-2013-PCM y la tercera Disposición Complementaria final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web: https://sgd.minjus.gob.pe/gesdoc_web/login.jsp e ingresando el Tipo de Documento, Número y Rango de Fechas de ser el caso o https://sgd.minjus.gob.pe/gesdoc_web/verifica.jsp e ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."