



PERÚ

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 del Bicentenario del Perú: 200 años de Independencia"

OPINIÓN CONSULTIVA N° 045-2021-JUS/DGTAIPD

ASUNTO : Cumplimiento del deber de informar sobre el tratamiento de datos a través de sistemas de videovigilancia con fines de control laboral

REFERENCIA : Hoja de Trámite Nro. 085675-2020MSC

FECHA : 11 de noviembre de 2021

I. ANTECEDENTES

1. Mediante el documento de la referencia se solicita a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD) precise el alcance de la Directiva Nro. 01-2020-JUS/DGTAIPD, referida al tratamiento de datos personales mediante sistemas de videovigilancia, en lo que respecta a las facultades de control del empleador sobre sus trabajadores utilizando esta herramienta cuando estos últimos prestan sus servicios en vehículos de titularidad corporativa, formulando las siguientes preguntas:
 - a. ¿En los casos de videovigilancia laboral en vehículos, cuyo espacio es reducido, se cumple con el deber de informar si únicamente se informa al trabajador a través de avisos informativos, con lo cual no es necesario el uso del cartel informativo?
 - b. ¿Cuáles son las infracciones y sanciones que se imponen por el incumplimiento a las disposiciones de la Directiva sobre Videovigilancia?

II. MARCO NORMATIVO DE ACTUACIÓN

2. La Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, la DGTAIPD) es la encargada de ejercer la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP)¹ y la Autoridad Nacional de Protección de Datos Personales (en adelante, la ANPD)².

¹ Decreto Legislativo Nro. 1353, 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 07 de enero de 2017; Decreto Supremo Nro. 013-2017-JUS, que aprueba el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (publicado el 22 de junio de 2017); y Decreto Supremo Nro. 019-2017-JUS, que aprueba el Reglamento del Decreto Legislativo Nro. 1353 (publicado el 15 de setiembre de 2017).

² Ley Nro. 29733, Ley de Protección de Datos Personales, artículo 32.



BICENTENARIO
PERÚ 2021

"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 ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

Scipión Llona 350, Miraflores
Central Telefónica: (511) 204-8020
www.minjus.gob.pe

- Entre sus funciones se encuentra absolver las consultas que las entidades o las personas jurídicas o naturales le formulen respecto a la aplicación de las normas de transparencia y acceso a la información pública, así como de la normativa sobre protección de datos personales.
- En esa medida, esta Dirección General emite la presente Opinión Consultiva en el ámbito de la interpretación en abstracto de las normas y no como mandato específico de conducta para un caso en concreto.

III. ANÁLISIS

A. Sobre el deber de informar respecto al tratamiento de datos personales

- La Constitución Política del Perú establece en el artículo 2, numeral 6, 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", es decir, toda persona tiene derecho a la autodeterminación informativa, y por lo tanto a la protección de sus datos personales.
- El Tribunal Constitucional, máximo intérprete de la Constitución Política del Perú, ha definido el derecho a la autodeterminación informativa en la STC 04739-2007-PHD/TC (fundamento 2-4) de la siguiente forma:

"[e]l derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal. Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen (...). En este orden de ideas, el derecho a la autodeterminación informativa protege al titular del mismo frente a posibles abusos o riesgos derivados de la utilización de los datos, brindando al titular afectado la posibilidad de lograr la exclusión de los datos que considera "sensibles" y que no deben ser objeto de difusión ni de registro; así como le otorga la facultad de poder oponerse a la transmisión y difusión de los mismos".

- En esa línea, no se puede ejercer un control efectivo de la información personal sin que se conozca cómo se van a utilizar los datos recopilados, qué tratamiento se les va a dar, con quiénes se va a compartir.
- La Ley N° 29733, Ley de Protección de Datos Personales (LPDP), tiene como objeto, conforme el artículo 1 "garantizar el derecho fundamental a la protección de los datos



personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen."

9. Para ello, entre otras disposiciones, señala en el Título III los derechos que tiene el titular del dato personal para poder ejercer control sobre su información personal:
 - Derecho de información del titular de datos personales (artículo 18 de la LPDP).
 - Derecho de acceso del titular de datos personales (artículo 19 de la LPDP).
 - Derecho de actualización, inclusión, rectificación y supresión (artículo 20 de la LPDP).
 - Derecho a impedir el suministro (artículo 21 de la LPDP).
 - Derecho de oposición (artículo 22 de la LPDP).
 - Derecho al tratamiento objetivo (artículo 22 de la LPDP).
10. Los citados derechos no se ejercen de la misma manera, puesto que mientras el derecho de acceso, actualización, inclusión, rectificación, supresión, impedimento de suministro y oposición requieren de una solicitud del titular del dato personal; el derecho de información y el derecho al tratamiento objetivo no requieren necesariamente de la solicitud del titular, sino que el solo hecho de no otorgarlos ya genera una vulneración al bien jurídico protegido.
11. El artículo 18 de la LPDP recoge el deber-derecho de informar de forma previa al titular del dato personal sobre el tratamiento que se realizará sobre sus datos personales:

"Artículo 18. Derecho de información del titular de datos personales. -

El titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.

Si los datos personales son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad, las que deben ser fácilmente accesibles e identificables.

(...)" (el subrayado es nuestro)

12. De la norma citada se desprende que los titulares de los datos personales tienen derecho a ser informados sobre el tratamiento que se realizará a su información personal, debiendo pormenorizarse sobre factores como la identidad y domicilio del titular del banco de datos, la finalidad de la recopilación, los datos personales de obligatoria entrega para efectuar el tratamiento, las consecuencias de proporcionar sus datos personales y de su



negativa a hacerlo, la transferencia y destinatarios de los datos personales, el banco de datos en donde se almacenarán los datos personales, el tiempo de conservación de los datos personales y el procedimiento para el ejercicio de los derechos señalados en el Título III de la LPDP.

13. El artículo 18 de la LPDP presenta una obligación que debe cumplir el titular del banco de datos personales³ o responsable del tratamiento⁴, tanto en aquellos casos que se encuentre obligado a solicitar el consentimiento del titular del dato personal, de acuerdo al artículo 5 de la LPDP, como en aquellos en los que no se requiere el consentimiento por existir otra circunstancia de legitimación que exceptúe de tal obligación, de acuerdo al artículo 14 de la LPDP.
14. Es preciso mencionar que el artículo 14 de la LPDP solo exonera al titular del banco de datos personales de la obligación de solicitar el consentimiento, por lo que debe de cumplir con las demás disposiciones, entre ellas, con el deber de informar.
15. Asimismo, es necesario enfatizar en que para considerarse que se ha protegido el derecho de información, lo detallado en el artículo 18 de la LPDP debe informarse de modo previo al tratamiento de datos, es decir, no se necesita observar una solicitud del titular del dato personal; lo contrario, significaría la configuración de un impedimento para el ejercicio efectivo del derecho.
16. Sin embargo, lo dicho no implica que el titular del dato personal no pueda solicitar información de forma posterior a la recopilación de sus datos personales respecto a la información señalada en el artículo 18. En ese sentido, el artículo 60 del Reglamento de la LPDP establece los mecanismos para que el titular del dato puede requerir dicha información en cualquier momento:

“Artículo 60.- Derecho a la información.

El titular de datos personales tiene derecho, en vía de acceso, a que se le brinde toda la información señalada en el artículo 18 de la Ley y el numeral 4 del artículo 12 del presente reglamento.

La respuesta contendrá los extremos previstos en los artículos citados en el párrafo anterior, salvo que el titular haya solicitado la información referida sólo a alguno de ellos.

Será de aplicación para la respuesta al ejercicio del derecho a la información, en lo que fuere pertinente, lo establecido en los artículos 62 y 63 del presente reglamento.”

17. La sola recopilación de datos sin el cumplimiento de informar lo señalado en el artículo 18 de la LPDP vulnera el bien jurídico protegido, puesto que no permite al titular del dato conocer cómo van a utilizar su información, y por lo tanto impiden el control sobre sus datos personales.

³ La LPDP, artículo 2, numeral 17 define al **Titular del banco de datos personales** como “Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad.”

⁴ El Reglamento de la LPDP, artículo 2, numeral 14 define al **Responsable del tratamiento** como “Es aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales.”



18. Dicho incumplimiento es considerado una infracción grave, en los términos del artículo 132, numeral 2, literal a), del Reglamento de la LPDP; a saber: "a) No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales de acuerdo a lo establecido en el Título III de la Ley N° 29733 y su Reglamento", que, de acuerdo al artículo 39 de la LPDP, se sanciona con una multa entre más de cinco a cincuenta unidades impositivas tributarias.

B. Cumplimiento del deber de informar respecto al tratamiento de datos a través de sistemas de videovigilancia

19. El deber de informar debe cumplirse de forma previa al tratamiento de datos. Al respecto, la LPDP, artículo 2, numeral 19, 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".
20. La videovigilancia es un tratamiento de datos, puesto que consiste en el monitoreo y captación de imágenes, videos o audios, que pueden ser almacenados a través de su grabación. Por lo tanto, de presentarse, debe ser informada a los titulares de datos.
21. Sin embargo, dadas las particularidades del tratamiento de datos realizado a través de sistemas de videovigilancia, la ANPD aprobó la Directiva N° 01-2020-JUS/DGTAIPD para el "Tratamiento de Datos Personales Mediante Sistemas de Videovigilancia, a través de la Resolución Directoral Nro. 02-2020-JUS/DGTAIPD.
22. Atendiendo a lo establecido en el numeral 19 del artículo 2 de la LPDP, la Directiva Nro. 01-2020-JUS/DGTAIP define el tratamiento de datos personales a través de sistemas de videovigilancia, como "cualquier operación o procedimiento técnico automatizado o no, que permita 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, videos o audios".
23. En ese marco, la Directiva establece en el artículo 6.7 que, para cumplir con el deber - derecho de información en los casos de tratamiento de datos personales a través de sistemas de videovigilancia se debe colocar un cartel informativo en los accesos al espacio videovigilado, y de no poder colocar toda la información señalada en el artículo 18 de la LPDP en el cartel, se debe indicar al titular del dato personal dónde encontrar la información adicional:



"Derecho de información"

6.7. Debe informarse sobre la captación y/o grabación de las imágenes, para tal fin se debe colocar en las zonas videovigiladas al menos un distintivo informativo ubicado en un lugar suficientemente visible, tanto en espacios abiertos como cerrados.

Si la información prevista en el artículo 18 de la LPDP no puede ser colocada en su integridad en el cartel informativo, en el espacio videovigilado debe tenerse a disposición de los interesados, ya sea a través de medios informáticos, digitalizados o impresos, la información mínima requerida para garantizar sus derechos, regulada en el punto 6.12 de la presente directiva.

Si el lugar vigilado dispone de varios accesos, el cartel se coloca en todos ellos, en un lugar visible, para que la información contenida en el mismo también lo sea".

24. El cartel informativo que se coloca en los accesos al espacio videovigilado debe tener las siguientes características:

"Características del cartel informativo"

6.11 Cada acceso a la zona videovigilada debe tener un cartel o anuncio visible con fondo amarillo o cualquier otro que contraste con el color de la pared y que lo haga suficientemente visible. Su contenido mínimo debe indicar (Anexo 1):

6.11.1 La identidad y domicilio del titular del banco de datos personales.

6.11.2 Ante quién y cómo se pueden ejercitar los derechos establecidos en la LPDP.

6.11.3 Lugar dónde puede obtener la información contenida en el artículo 18 de la LPDP.

6.11.4 En lo que se refiere a las dimensiones, los elementos gráficos podrán tener, como mínimo, las siguientes: 297 x 210 mm. Cuando el espacio en que se vaya a ubicar el cartel informativo no lo permita, este debe adecuarse al espacio disponible, de tal forma que cumpla su finalidad informativa." (el subrayado es nuestro)

25. La información adicional al cartel informativo, contenida en un aviso informativo, respecto al tratamiento de datos personales a través de sistemas de videovigilancia, debe estar disponible, ya sea a través de medios informáticos, digitalizados o impresos, y debe contener la información requerida para garantizar el derecho reconocido en el artículo 18 de la LPDP, conforme el artículo 6.12 de la Directiva:

"Características del informativo adicional del sistema de videovigilancia"

6.12 El informativo adicional del sistema de videovigilancia (Anexo 2) debe estar disponible, ya sea a través de medios informáticos, digitalizados o impresos, y debe contener la información requerida para garantizar el derecho reconocido en el artículo 18 de la LPDP:

6.12.1 La identidad y domicilio del titular del banco de datos personales y del encargado del tratamiento, de ser el caso.

6.12.2 La finalidad.

6.12.3 Las transferencias y destinatarios de los datos personales.

6.12.4 El plazo durante el cual se conservarán los datos personales.

6.12.5 El ejercicio de los derechos de información, acceso, cancelación y oposición de los datos."

26. Visto lo anterior, el responsable del tratamiento deberá utilizar carteles informativos, teniendo en cuenta el espacio disponible, y tener a disposición de los interesados, a



través de medios informáticos, digitalizados o impresos, el informativo adicional o aviso informativo que debe contener la información requerida para garantizar el derecho reconocido en el artículo 18 de la LPDP.

C. Videovigilancia para el control laboral

27. El artículo 9 del Decreto Supremo N°. 003-97-TR, Texto Único Ordenado de la Ley de Productividad y Competitividad Laboral reconoce las facultades de dirección y control del empleador con respecto a los trabajadores al disponer que "(...) el trabajador presta sus servicios bajo dirección de su empleador, el cual tiene facultades para normar reglamentariamente las labores, dictar las órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente, dentro de los límites de la razonabilidad, cualquier infracción o incumplimiento de las obligaciones a cargo del trabajador".
28. Así, en virtud del poder de dirección, los empleadores, personas físicas o jurídicas, públicas o privadas, simples o compuestas tendrán, entre otros, el derecho a controlar el efectivo cumplimiento de las obligaciones laborales de sus trabajadores⁵ y, para tal efecto, puede utilizar los mecanismos que considere pertinentes, siempre que estos no vulneren o afecten los derechos fundamentales de los trabajadores.
29. En este orden de ideas, resulta válido el uso de los sistemas de videovigilancia por parte del empleador si este observa criterios de razonabilidad y proporcionalidad; y, en lo que al derecho de protección de datos se refiere, se respeta lo establecido en la normativa legal que existe sobre la materia, es decir, la LPDP, su reglamento, y lo dispuesto por la Directiva N° 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia.
30. En ese marco, para realizar videovigilancia laboral no basta con cumplir con informar lo señalado en el artículo 18, sino que se deben de respetar los demás principios y disposiciones de la LPDP, tales como el principio de proporcionalidad, conforme lo señalado en el artículo 7 de la 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."

31. En ese marco, la Directiva establece lo siguiente:

"Principio de proporcionalidad

7.13 El control laboral a través de sistemas de videovigilancia sólo se realiza cuando sea pertinente, adecuado y no excesivo para el cumplimiento de tal fin.

7.14 Asimismo, la instalación de las cámaras o, en todo caso, su ámbito de captación debe restringirse a los espacios indispensables para satisfacer las finalidades de control laboral.

⁵ Sentencia del Tribunal Constitucional español Nro. 206/1987, de 21 de diciembre, fundamento jurídico 2 (RTC 1987\206).



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

7.15 En ningún caso se admite la instalación de sistemas de grabación o captación de sonido ni de videovigilancia en los lugares destinados al descanso o esparcimiento de los trabajadores, como vestuarios, servicios higiénicos, comedores o análogos.

7.16 La grabación videovigilada con sonido en el lugar de trabajo sólo se admitirá 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 y siempre respetando el principio de proporcionalidad y finalidad."

32. Por lo tanto, deberá evaluarse en cada caso concreto la proporcionalidad del tratamiento de videovigilancia para el control laboral. Por ejemplo, resulta proporcional el uso de la videovigilancia laboral en aquellos casos en los que los trabajadores deben de cumplir con medidas de seguridad, como el uso de implementos de seguridad o uso correcto de máquinas en los casos de trabajos de riesgo.
33. Respecto al cumplimiento de deber de informar en los casos de videovigilancia laboral, la Directiva establece en el artículo 7.10 lo siguiente:

"Deber de Informar

7.10. El empleador se encuentra obligado a informar a sus trabajadores de los controles videovigilados, a través de carteles (o en su defecto de los avisos informativos mencionados en la presente directiva); ello, sin perjuicio de informar de manera individualizada a cada trabajador, si se considera pertinente."

34. Es pertinente advertir que el citado artículo establece que el empleador está obligado a informar a los trabajadores de la existencia de sistemas de videovigilancia a través del cartel de videovigilancia.
35. Solo en caso no resulte posible colocar el cartel informativo por las condiciones propias del ejercicio de la prestación, tal como el seguimiento mediante drones de actividades laborales al aire libre, respetando el principio de proporcionalidad, podrá entregarse la información sólo a través de un aviso en formato físico o electrónico, conforme lo señalado en el artículo 7.30, 7.31 y 7.32 de la Directiva:

"Responsabilidad del titular y/o encargado del tratamiento

7.30 El titular del banco de datos personales, responsable o el encargado del tratamiento debe informar de acuerdo a lo señalado en el punto 6.8 de esta directiva a las personas que serán controladas mediante los sistemas de videovigilancia a través de drones. Este deber alcanza también a aquellas personas o entidades que brinden el servicio de videovigilancia a través de drones de forma complementaria a la que preste el servicio principal. Dicha información debe entregarse en formato físico o electrónico, al momento de suscribir el contrato de videovigilancia con la entidad o persona que brinde este servicio a través de drones o de forma singularizada en el documento de contratación; además, debe estar a disposición de quien lo requiera. 7.31 Debe utilizarse los sistemas de carteles o folletos cuando sea factible. En caso de utilizar el cartel o el folleto se debe indicar gráficamente (dibujo) el medio utilizado (Anexo 3), aplicándose, en lo que resulte pertinente, de forma mínima lo establecido en el punto 6.11 de esta directiva.

7.32 Los titulares de bancos de datos personales, responsables o encargados de tratamiento, en caso cuenten con una página web, deben publicar información que permita conocer los



diferentes tipos de operaciones realizadas o las que se proponen realizar en el futuro cercano con los datos captados."

36. En esa línea, respecto a los vehículos corporativos, en principio, lo que corresponde es colocar el cartel informativo de videovigilancia atendiendo a los espacios que el propio vehículo proporciona. Al respecto es importante recordar que las dimensiones del cartel, tal como lo refiere el artículo 6.14 de la Directiva Nro. 01-2020-JUS/DGTAIP, es meramente referencial, con lo cual, cuando el espacio en que se vaya a ubicar el cartel informativo no permita que este tenga el tamaño indicado en la directiva, este debe adecuarse al espacio disponible, de tal forma que cumpla su finalidad informativa.
37. Por lo tanto, sólo en aquellos casos en que el vehículo móvil no cuente con un espacio adecuado que permita cumplir con el deber de informar a través del uso del cartel informativo, siendo en la mayoría de los casos vehículos unipersonales que no permiten otro pasajero, por ejemplo, motocicletas, bicicletas, etc., podrá obviarse su uso. De darse este caso, el empleador cumplirá con el derecho-deber de informar proporcionando al trabajador la información a través de medios informáticos, digitalizados o impresos que deben contener la información requerida para garantizar el derecho reconocido en el artículo 18 de la LPDP.
38. Al respecto, es importante no olvidar que los vehículos corporativos pueden ser utilizados para efectos de transportar a otras personas, por ejemplo, otros trabajadores, o personas externas al centro laboral, tales como clientes de la entidad. Por lo que, si las cámaras de videovigilancia van a captar imágenes o audios de estas personas, deberán ser informadas conforme lo señalado en la Directiva, es decir a través de carteles de videovigilancia, que a su vez indiquen dónde encontrar aquella información que no pudo colocarse en el cartel.

IV. CONCLUSIONES

1. Para la recopilación de datos a través de sistemas de videovigilancia debe de cumplirse con el deber de informar de forma previa sobre las características del tratamiento de datos, conforme lo señalado en el artículo 18 de la LPDP.
2. Dadas las particularidades del tratamiento de datos a través de sistemas de videovigilancia, conforme a la Directiva N° 01-2020-JUS/DGTAIPD para el "Tratamiento de Datos Personales mediante Sistemas de Videovigilancia", se cumple con informar si se coloca un cartel informativo en los accesos a los espacios videovigilados, que a su vez indique dónde encontrar la información que no pudo colocarse en el cartel, siguiendo las especificaciones señaladas en la Directiva.
3. La videovigilancia con fines de control laboral debe realizarse solo cuando sea proporcional a la finalidad, así como también debe de ser informada al trabajador de forma previa.





PERÚ

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 del Bicentenario del Perú: 200 años de Independencia"

4. En los casos de videovigilancia laboral, si el espacio no permite colocar el cartel, como por ejemplo lo sistemas de videovigilancia de actividades al aire libre a través de drones, podrá informarse a los trabajadores a través de otro medio.
5. En el caso de la videovigilancia al interior de vehículos corporativos que permiten transportar a personas, tales como trabajadores que no estén a cargo del vehículo o a personas externas al centro laboral, se debe colocar el cartel informativo al interior del mismo, teniendo en cuenta la dimensión del espacio, el cual debe indicar dónde encontrar el aviso o informativo adicional.
6. No cumplir con el deber de informar sobre el tratamiento de datos personales de forma previa a la recopilación se sanciona con una multa entre más de cinco unidades impositivas tributarias (UIT) hasta cincuenta unidades impositivas tributarias (UIT), al ser una infracción grave.

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



BICENTENARIO
PERÚ 2021

"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 ingresando Tipo de Documento, Número, Remitente y Año, según corresponda."

Scipión Llona 350, Miraflores
Central Telefónica: (511) 204-8020
www.minjus.gob.pe