SPDTSS
SOCIEDAD PERUANA DE DERECHO DEL TRABAJO Y DE LA SEGURIDAD SOCIAL

Videovigilancia laboral a la luz del desarrollo normativo y los pronunciamientos en consulta de la autoridad nacional de protección de datos personales

Occupational video surveillance considering the regulatory development and the pronouncements in consultation of the National Authority for the Protection of Personal Data

REBECA KARINA APARICIO ALDANA*
Universidad San Ignacio de Loyola
(Lima, Perú)
Contacto: raparicio@usil.edu.pe
https://orcid.org/0000-0002-7145-3731

RESUMEN: En el presente artículo, la autora se detiene a esbozar de forma sucinta y descriptiva los principales pronunciamientos que respecto a la videovigilancia con fines de control y supervisión laboral ha realizado la Autoridad Nacional de Protección de Datos Personales, con la finalidad de ilustrar al lector sobre estas decisiones administrativas. En este sentido, es preciso advertir que el objeto de este documento no es realizar un análisis exhaustivo y profundo de las opiniones consultivas o de la Directiva Nro. 01-2020-JUS/DGTAIP referida al tratamiento de datos personales mediante sistemas de videovigilancia, sino simplemente reseñar su contenido e identificar sus principales conclusiones, en lo que respecta al uso de la videovigilancia como medio tecnológico de control de los trabajadores por parte del empleador.

PALABRAS CLAVE: Protección de datos, videovigilancia, control, supervisión laboral y Autoridad Nacional de Protección de Datos Personales.

ABSTRAC: In this article, the author stops to make a succinct and descriptive outline of the main pronouncements that the National Authority for the Protection of Personal Data has made regarding video surveillance for labor control and supervision purposes, with the purpose of illustrating the reader about these administrative decisions. In this sense, it should be noted that the purpose of this document is not to carry out an exhaustive and in-depth analysis of the advisory opinions or of Directive No. 01-2020-JUS/DGTAIP referring to the processing of personal data through video surveillance systems, but rather

* Doctora en Derecho sobresaliente C*um Laude por unanimidad* por la Universidad Rey Juan Carlos – España y ganadora del Premio extraordinario de Doctorado. En esa misma casa de estudios es Máster en Derecho del Trabajo y la Seguridad Social; es, además: Licenciada en Derecho por la Universidad de Alcalá – España (homologación) y especialista en Derecho de Protección de Datos Personales por la Universidad Nacional de Educación a Distancia de España y Experta por la Agencia Española de Protección de Datos Personales. Asimismo, es abogada, Máster en Derecho Constitucional y Especialista en Derecho Administrativo Sancionador por la Universidad de Piura (Perú). Ex asesora jurídica de la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos (Perú).

simply review its content and identify its main conclusions, regarding the use of these technological tools as a means of controlling workers by the employer.

KEYWORDS: Data protection, video surveillance, labor control, labor supervision, National Authority of Personal Data Protection.

Recibido: 05/08/2022 **Aceptado:** 12/09/2022 **Publicado en línea:** 28/09/2022

I. VIDEOVIGILANCIA COMO MEDIO DE CONTROL LABORAL RECOLECTOR DE DATOS PERSONALES

Resulta innegable el importante aumento de instalación de cámaras u otros dispositivos con fines de videovigilancia por parte de las empresas para asegurar la seguridad de sus instalaciones y bienes; así, como, para vigilar o supervisar la prestación laboral de sus trabajadores. Estos sistemas permiten la captación, grabación, almacenamiento de imágenes y sonido, lo que supone un tratamiento de datos personales, debido a que esta información registrada por las cámaras resulta un medio razonable para identificar o hacer identificable a una persona natural.

El derecho a la autodeterminación informativa o de protección de datos personales implica que titular de los datos personales tiene una la facultad de control sobre estos, de tal manera que cada persona se encuentra facultada para ejercer dominio sobre la información personal que le pertenece y la forma en que tales datos son tratados o administrados por terceros, garantizando al titular de los datos personales que estos sólo sean utilizados por otros cuando exista una base jurídica que justifique su tratamiento.

El artículo 2, numeral 6 de la Constitución Política del Perú dispone que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados no suministren información que afecte la intimidad personal y familiar. Este derecho constitucional ha sido desarrollado normativamente por la Ley Nro. 29733, de Protección de Datos Personales (LPDP) y su reglamento contenido en el Decreto Supremo Nro. 003-2013/JUS.

La videovigilancia es un sistema que permite la captación y, de ser el caso, la grabación de imágenes y sonido, su uso implica un registro de datos personales que puede afectar a las personas que son captadas o grabadas por sistemas instalados por terceros, quienes, a través de estos instrumentos tecnológicos, tratan esta información.

Como ya se ha dicho, los sistemas de videovigilancia permiten identificar o hacer identificables a las personas que son captadas o grabadas a través los mismos. Por ello, frente al registro y potencial afectación, los titulares de los datos personales tienen la atribución y facultad de ejercer el derecho constitucional de protección de datos personales, que supone el poder de controlar el uso que los terceros den a la información captada o registrada, a través de estos sistemas.

Cabe señalar que en las relaciones laborales el derecho de protección de datos tiene connotaciones propias dado que la mayoría de los tratamientos de datos personales de los trabajadores que realiza el empleador deviene de la propia naturaleza de la prestación y, por lo tanto, el tratamiento de datos de los trabajadores dentro de la relación laboral configura uno de los supuestos de tratamiento necesario para la ejecución del contrato. Debido al poder de dirección empresarial regulado en el artículo 9 del Texto Único Ordenado la Ley de Productividad y Competitividad Laboral, aprobado por Decreto Supremo Nro. 003-1997-TR (en adelante TUO de la LPCL), el empleador se encuentra facultado a realizar controles y a tomar medidas para vigilar el ejercicio de las actividades laborales de sus trabajadores.

En este orden de ideas, la videovigilancia es una forma de ejercer el poder de dirección que le faculta al empleador a realizar un control sobre el cumplimiento de la prestación laboral a través de la captación y grabación de imágenes y sonido con la finalidad de verificar si efectivamente los trabajadores están cumpliendo adecuadamente las labores que le han sido encomendadas.

En este sentido, si bien de acuerdo con lo en el artículo 5 de LPDP el principio rector del tratamiento de datos personales es el principio del consentimiento, en el caso de las relaciones laborales, todos aquellos tratamientos de datos personales de los trabajadores realizados en virtud del ejercicio de su prestación o de las facultades propias del empleador, incluida la actividad de videovigilancia laboral, se podrán realizar sin necesidad de su consentimiento.

Ello de acuerdo con lo establecido en el artículo 14, inciso 5 de la referida norma en el cual se establece que:

> *No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos: (…)*
>
> *5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.*

Así, dado que en las relaciones generadas en virtud de un contrato de trabajo, el derecho de protección de datos tiene connotaciones particulares, en principio, el tratamiento de datos personales (imagen y voz) de los trabajadores, a través de sistemas de videovigilancia dirigidos a controlar la actividad laboral, sin consentimiento, por parte del empleador es lícito, lo cual no significa que el empresario cuente con una facultad omnímoda sobre el uso de este medio de control y vigilancia laboral, por ello, esta herramienta audiovisual, al igual que cualquier otra facultad de control del empleador, debe ajustarse al respeto de los derechos fundamentales de los trabajadores y vendrá delimitada, en virtud de las específicas circunstancias y los particulares fines que rodean su uso (Aparicio, 2016, p. 139).

En este sentido, la no necesidad de consentimiento del trabajador para el tratamiento de sus datos personales debido a la relación laboral no enerva el resto de las obligaciones que le corresponden al empleador en su calidad de responsable del tratamiento de los datos personales. Así, por ejemplo, el empleador, en tanto titular del banco de datos personales o responsable del tratamiento de los datos personales de sus trabajadores, debe de cumplir con lo dispuesto en el artículo 18 de la LPDP que impone como obligación de los titulares de los bancos de datos personales o responsables de su tratamiento, informar sobre la finalidad del este a sus titulares.

II. DIRECTIVA DE VIDEOVIGILANCIA Y CONTROL LABORAL

En el Perú, de acuerdo con lo establecido en el artículo 33 de la LPDP, la Autoridad Nacional de Protección de Datos Personales (ANPDP) tiene como función realizar todas las acciones necesarias para la garantía y respeto del derecho

de protección de datos personales y, para ello, ejerce funciones administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.

Justamente, atendiendo a su función normativa la ANPDP publicó la Resolución Directoral Nro. 02-2020-JUS-DGTAIPD que aprueba la Directiva Nro. 01-2020- JUS/DGTAIP[1] sobre el tratamiento de datos personales por medio de sistemas de videovigilancia. Entre los objetivos de esta disposición se encuentra el regular el tratamiento de datos personales captados a través de sistemas de videovigilancia con fines de control laboral, de conformidad con lo establecido en la LPDP y su reglamento.

Por ello, esta norma reglamentaria regula las particularidades propias del tratamiento de datos obtenidos a través de sistemas de videovigilancia con fines laborales en sus numerales 7.9 a 7.25, destacando, por ejemplo, la excepción del consentimiento, en lo que se refiere a la posibilidad de los empleadores de realizar controles videovigilados o tomar medidas para vigilar el ejercicio de las actividades laborales de sus trabajadores. Ahora como se ha señalado, el hecho de que el empleador no se encuentre obligado a solicitar el consentimiento de los trabajadores no significa que no tenga el deber de cumplir con informarles sobre este tipo de tratamientos, a través de carteles[2] (o en su defecto de los avisos informativos)[3]; ello, sin perjuicio de informar de manera individualizada a cada trabajador, si se considera pertinente.

1 https://www.gob.pe/institucion/minjus/normas-legales/441859-02-2020-jus-dgtaipd

2 **Directiva Nro. 01-2020-JUS/DGTAIP:**
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.

3 **Directiva Nro. 01-2020-JUS/DGTAIP:**
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.

Resulta interesante, a ese respecto, la mención específica que se hace en esta directiva respecto de prestación realizada por las trabajadoras del hogar, señalando que, en este tipo de relaciones laborales, para verificar el cumplimiento del deber de informar, bastará con que los empleadores acrediten de forma razonable que han cumplido con el deber de informar contenido en el artículo 18 de la LPDP.

La directiva también hace referencia al cumplimiento del principio de finalidad en el tratamiento de datos con fines de control laboral a través de sistemas de videovigilancia haciendo hincapié en que el tratamiento de los datos de los trabajadores, en este supuesto, debe limitarse a las finalidades propias del control y supervisión de la prestación laboral, de tal forma que no pueden utilizarse los medios o el sistema de videovigilancia para fines distintos, salvo que se cuente con el consentimiento del trabajador o se trate de alguna de las excepciones señaladas en el artículo 14 de LPDP[4].

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.

4 **Artículo 14 de la LPDP. Limitaciones al consentimiento para el tratamiento de datos personales.**
No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:
1. Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley. 4. Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5. Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6. Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7. Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea

Además, esta disposición señala que son fines legítimos para el control y la supervisión de la prestación laboral, la protección de bienes y recursos del empleador; la verificación de la adopción de medidas de seguridad en el trabajo; y, aquellos otros que la legislación laboral y sectorial prevea. Al respecto, resulta importante advertir la valía de este reconocimiento, pues es reiterada la doctrina jurisprudencial comparada, en donde se ha puesto en tela de juicio, por parte de los trabajadores, el uso de lo captado por las cámaras de videovigilancia con fines de seguridad, cuando estas han registrado, por ejemplo, apropiaciones de bienes de la empresa o de obligaciones de resguardo de la seguridad, asegurando que lo visualizado y almacenado en los sistemas de videovigilancia con fines de seguridad, no responde a una finalidad de control o supervisión de las actividades laborales y que, por lo tanto, lo captado por las cámaras no puede ser utilizado como prueba lícita por el empleador para efectos de sancionar al trabajador por un incumplimiento laboral, pues la finalidad de la captación sería distinta a la de supervisar las actividades de los trabajadores.

Sin embargo, por ejemplo, la jurisprudencia española, ha resuelto en más de una oportunidad, considerando como prueba válida de un incumplimiento laboral que justifica la sanción de trabajadores, el uso de imágenes captadas por cámaras con fines de seguridad cuando estas registran a trabajadores apropiándose de bienes de la empresa o vulnerando la seguridad de esta, permitiendo, por ejemplo, el ingreso de personas no autorizadas al centro o lugar de trabajo.

política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.

8. Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9. Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10. Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11. En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12. Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13. Otros que deriven del ejercicio de competencias expresamente establecidas por Ley.

Así, por ejemplo, la Sentencia del Tribunal Constitucional español nro. 39/2016 (Pleno), de 3 de marzo, que enjuició un supuesto en el que las cámaras de videovigilancia se habían instalado en una tienda, captando la imagen de la trabajadora apropiándose de dinero. Para ocultar dicha apropiación, la empleada realizó operaciones falsas de devoluciones de venta de prendas. La trabajadora fue despedida. La cámara estaba situada en el lugar donde se desarrollaba la prestación laboral, enfocando directamente a la caja. En un lugar visible del escaparate del establecimiento se había colocado el distintivo informativo. Por estas razones, el más alto interprete de la constitucionalidad español declaró válida la prueba.

Por su parte, la Sentencia del Tribunal Supremo español nro. 817/2021, de 21 de julio de 2021, rec. 4877/2018 declara válida la prueba captada por unas cámaras de seguridad de acceso al recinto ferial de IFEMA (Feria de Madrid), cuya existencia era conocida por el trabajador quien se desempeñaba como vigilante de seguridad. El trabajador fue despedido por el incumplimiento de su deber de realizar las requisas de vehículos (controles de seguridad aleatorios en accesos al recinto y a los estacionamientos públicos) y su declaración como efectuadas en sus partes o registros diarios entregados a la empresa, es decir, por falsear tales partes e incumplir su prestación laboral durante el periodo de quince días del mes de febrero de 2017.

Con la afirmación realizada por la directiva peruana de que el incumplimiento de las obligaciones de seguridad o de protección de bienes y recursos del empleador es un fin legítimo de supervisión de la prestación laboral a través de sistemas de videovigilancia, la autoridad administrativa deja en claro que si se les informa a los trabajadores que las cámaras tendrán por finalidad el control de la actividad laboral, la realización de estas conductas calzará perfectamente con un incumplimiento de sus obligaciones y, en consecuencia, podrán ser utilizadas por el empleador como prueba de un infracción de los deberes de trabajo, por parte de alguno de sus trabajadores.

Asimismo, consideramos que, de colocarse cámaras con fines exclusivos de seguridad, dado que estos incumplimientos laborales, tal como las califica la directiva, son al mismo tiempo, infracciones de seguridad, pueden ser utilizados como prueba válida en un procedimiento disciplinario o de despido del trabajador registrado cometiendo esta inconducta, pues las cámaras de seguridad estarían cumpliendo, efectivamente, con los fines para los cuales fueron instaladas:

detectar problemas de seguridad en las instalaciones de la empresa empleadora. Así, «si el trabajador es sorprendido por la cámara cuando se apropia de una cantidad o de un producto se está dentro de la finalidad asignada al medio del control y sería absurdo sostener que la finalidad no se cumple porque se registra un incumplimiento laboral» (Desdentado y Muñoz, 2012, p. 70), con lo cual «si la finalidad declarada por las cámaras de vídeo por la empresa es de seguridad, la actuación de la empresa sancionando a quien sea sorprendido cometiendo hurtos no debe considerarse como un uso desviado o hallazgo casual sino, al contrario, como un uso enteramente finalista» (Goñi, 2014).

Ello, sin perjuicio de que, en lo que respecta en exclusiva al derecho de protección de datos[5], al no haberse informado de que las cámaras de seguridad también serían utilizadas para fines de control laboral, la empresa que haga uso de ellas para esos fines pueda ser sancionada por incumplimiento del derecho – deber de informar regulado en el artículo 18 de la LPDP[6].

La directiva también advierte de la aplicación del principio de proporcionalidad en el uso de sistemas de videovigilancia para fines de control de los trabajadores afirmando que este tipo de medidas de supervisión laboral sólo debe ser implementada por el empleador cuando sea pertinente, adecuada y no excesiva para el cumplimiento de tal fin. El uso de instalaciones de cámaras o videocámaras sólo debe permitirse cuando no exista un medio menos invasivo. Las imágenes deben conservarse únicamente por el tiempo imprescindible para la finalidad para la cual se recabaron. Además, debe valorarse el uso de "máscaras de privacidad", de tal forma que se evite captar o grabar imágenes excesivas.

5 Con respecto, por ejemplo, al derecho a la intimidad existirán otras obligaciones para utilizar lo registrado por cámaras con fines de seguridad para control laboral, como la existencia previa de indicios razonables de incumplimiento. Sin embargo, la explicación de este requisito desborda el contenido del presente artículo, por lo que sólo dejamos esta cuestión esbozada, para un posterior análisis en una investigación futura.

6 Al respecto, resulta interesante la afirmación contenida en la Sentencia del Tribunal Europeo de Derechos Humanos(Gran Sala) 17 octubre 2019 (*López Ribalda II*), que incluso considera legítima la colocación de cámaras de seguridad ocultas por parte del empleador con la finalidad de captar un incumplimiento laboral de sus trabajadores cuando se tengan indicios razonables de la posible comisión de la falta, no exista otro medio para obtener prueba de esta y el tiempo de uso de la medida sea el estrictamente necesario para captar al trabajador realizando el incumplimiento, en donde señala, en su fundamento 135, que el hecho de que la prueba no fuera nula desde la perspectiva de la impugnación judicial de la sanción disciplinaria impuesta al trabajador, no impide que la empresa pueda ser responsable en el ámbito de la legislación de protección de datos.

Asimismo, la directiva señala que, si el empleador debe transferir los datos personales de sus trabajadores captados mediante videovigilancia a un tercero por motivos no laborales, debe informar de ello a los trabajadores, conforme la LPDP y su reglamento. De igual modo, cuando corresponda, debe solicitar su consentimiento.

Esta norma reglamentaria establece algunos límites al uso de cámaras de videovigilancia laboral al restringir su ámbito de captación a los espacios indispensables para satisfacer las finalidades de control laboral señalando que 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. Ello debido a que utilizar en estos espacios sistemas de control videovigilado podría resultar desproporcionado.

Al respecto, consideramos que el empleador debe tener en cuenta el número de cámaras que pretende utilizar, así como el tipo de estas, ya que no es lo mismo la captación de datos personales a través de cámaras dispuestas a captar imagen y sonido; que las que permiten captar sólo imágenes; Por ello, en nuestra opinión, con el fin de salvaguardar otros derechos fundamentales de los trabajadores como el derecho a la intimidad o libertad sindical, la directiva advierte que 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.

También deberá tenerse en cuenta si se captan datos personales a través de cámaras fijas o por medio de cámaras móviles o sistemas de grabación a 360 grados; para ello debe atenderse a los espacios y los objetivos específicos que el empleador pretende conseguir con la colocación de las cámaras de videovigilancia.

Asimismo, con el objeto de evitar un uso arbitrario e indiscriminado de la imagen del trabajador y salvaguardar que la finalidad de la recogida de esta información sea respetada, esta disposición dispone una prohibición de uso de las imágenes para fines comerciales o publicitarios, salvo que se cuente con el consentimiento de los trabajadores.

La directiva recalca que los trabajadores deben estar informados sobre el procedimiento implementado por el empleador para ejercer sus derechos de acceso, cancelación y oposición. Cabe advertir que, en el caso de tratamiento de datos a través de sistemas de videovigilancia, el derecho de rectificación no puede ser ejercido, ello debido a que este derecho supone modificar alguno de nuestros datos personales. Este hecho resulta completamente imposible en la videovigilancia (modificar las grabaciones a petición del usuario) ya que por la naturaleza de los datos -imágenes o voces tomadas de la realidad que reflejan un hecho objetivo-, se trataría del ejercicio de un derecho de contenido imposible.

Con respecto al almacenamiento de lo captado de por las cámaras de videovigilancia, la directiva dispone que las imágenes y/o voces grabadas se almacenan por un plazo de treinta (30) días y hasta un plazo máximo de sesenta (60) días, salvo disposición distinta en las normas laborales. Durante ese plazo, el titular del banco de datos o encargado del tratamiento debe cuidar que la información sea accesible sólo ante las personas que tengan legítimo derecho a su conocimiento y manteniendo así la reserva necesaria respecto a las imágenes y/o voces.

Una vez transcurrido el plazo señalado en el párrafo anterior y no habiendo requerimiento de alguna autoridad competente para entregar o visualizar el contenido de la grabación, se deben eliminar los archivos en el plazo máximo de dos (02) días hábiles, salvo disposición distinta en norma sectorial.

Ahora, de acuerdo con lo establecido en el numeral 7.20 de la referida disposición reglamentaria el plazo máximo previsto para la eliminación de la información no será aplicable cuando exista alguna finalidad o interés legítimo que justifique su conservación, así como la concurrencia de alguna contingencia de orden técnico que justifique razonablemente el aplazamiento de la eliminación de esta por un período determinado o determinable.

En caso de la captación de imágenes y/o voces sin editar que den cuenta de la comisión de presuntas infracciones laborales y/o accidentes de trabajo, esta norma señala que deben ser conservadas por el plazo de ciento veinte (120) días, contados a partir de su conocimiento, salvo la existencia de alguna finalidad que justifique su conservación o de interés legítimo, tiempo dentro del cual el empleador podrá iniciar las acciones legales pertinentes. Asimismo, destaca que si el empleador, en base a lo captado por los sistemas de videovigilancia, decida

imputar una falta grave a un trabajador, deberá proceder de conformidad con lo establecido en las normas laborales.

Este plazo resulta más que razonable atendiendo al procedimiento disciplinario que el conocimiento por parte del empleador, a través del uso de sistemas de videovigilancia, de una falta laboral puede acarrear. Así, una vez conocida la falta por el empleador, la jurisprudencia peruana ha señalado que un plazo proporcional y razonable para la imputación de cargos al trabajador es el de 30 días naturales[7]. Luego de imputados los cargos, de acuerdo con lo dispuesto en el artículo 31 del TUO de la LPCL, el trabajador tiene 6 días para presentar sus descargos. Transcurrido dicho plazo, con los descargos o sin ellos, de acuerdo con lo señalado también por la jurisprudencia, el empleador tiene como plazo razonable 33 días para notificar la sanción o carta de despido[8], todo ello con la finalidad de no vulnerar el principio de inmediatez.

Por su parte el trabajador, según lo dispuesto en el artículo 36 del TUO de la LPCL tiene el plazo de 30 días naturales para demandar la existencia de despido nulo, arbitrario o indirecto. Cabe advertir que existen varios plenos jurisdiccionales en los cuales se señala que el plazo de caducidad de la acción por despido debe descontar todos los días de paralización de labores de los trabajadores del Poder Judicial[9].

Asimismo, la directiva dispone que el trabajador podrá solicitar el acceso a las grabaciones o a una copia digital de las mismas que contengan información sobre una inconducta o incumplimiento laboral que se le haya imputado, pudiendo utilizar esta grabación como medio de prueba. El empleador deberá resguardar el derecho de terceros que, sin estar involucrados con la inconducta o incumplimiento, de manera directa o indirecta, puedan aparecer en registros

7 Casación Nro. 677-2006-La Libertad, de 9 de septiembre de 2006 de la Sala Transitoria de Derecho Constitucional y Social de la Corte Suprema de la República del Perú, fundamentos jurídicos 11 y 12, que constituyen precedente de observancia obligatoria en el modo y forma previsto por la ley.

8 Casación Nro. 1917-2003-Lima, de 27 de marzo de 2006 de la Primera Sala Transitoria de Derecho Constitucional y Social de la Corte Suprema de la República del Perú, fundamentos jurídicos 3 y 4, que constituyen precedente de observancia obligatoria en el modo y forma previsto por la ley.

9 Pleno Jurisdiccional Laboral 1999, realizado en Trujillo, el 14 de agosto de 1999. Acuerdo Nro. 1. En el mismo sentido: Pleno Jurisdiccional Distrital Laboral 2017, realizado en Arequipa. Tema Nro. 1: El computo de plazo de caducidad teniendo en cuenta los días de paralización de labores de los trabajadores del Poder Judicial y Pleno Jurisdiccional Nacional en Materia Laboral y Procesal Laboral 2017, realizado en Trujillo, los días 11 y 12 de agosto de 2017. Tema Nro. 1: La suspensión de plazo por huelga de trabajadores del Poder Judicial.

captados; ello se hará adoptando las medidas técnicas necesarias para difuminar su imagen e impedir su identificación.

III. PRONUNCIAMIENTOS A TRAVÉS DE OPINIONES CONSULTIVAS DE LA ANPDP PERSONALES SOBRE VIDEOVIGILANCIA LABORAL

En más de una ocasión, la ANPDP se ha pronunciado con respecto a consultas formuladas por los administrados referidas al uso de sistemas de videovigilancia para efectos del control laboral de los trabajadores. Entre estos pronunciamientos destacan dos opiniones consultivas bastante interesantes: La primera contenida en la Opinión Consultiva Nro. 045-2021-JUS/ DGTAIPD, de 11 de noviembre de 2021[10], en la cual la Autoridad Nacional de Protección de Datos Personales responde a una pregunta referida a cómo debe de cumplirse el derecho - deber de informar en el caso de videovigilancia laboral en vehículos cuyo espacio es reducido.

La autoridad señala que, en 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.

Asimismo, en la opinión se afirma que, 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.

10 https://www.gob.pe/institucion/anpd/informes-publicaciones/2369735-oc-n-45-2021-jus-dgtaipd-cumplimiento-del-deber-de-informar-sobre-el-tratamiento-de-datos-a-traves-de-sistemas-de-videovigilancia-con-fines-de-control-laboral

Además, la ANPDP advierte que, es importante no olvidar que los vehículos corporativos pueden ser utilizados para efectos de transportar a otras personas distintas al trabajador cuya prestación consiste en conducir el vehículo como, 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.

El segundo pronunciamiento es el referido al tratamiento de datos a través de cámaras de videovigilancia en espacios de trabajo compartidos (cowork) y contenida en la Opinión Consultiva Nro. 02-2021-JUS/DGTAIPD, de 12 de febrero de 2021[11].

En esta la ANPDP señala que en un contrato de *coworking*, en lo que respecta a la videovigilancia de seguridad y control laboral, será la empresa de *coworker* (arrendataria del espacio) la responsable del tratamiento o titular de los bancos de datos personales y, por lo tanto, responsable del cumplimiento de las obligaciones; así, en su calidad de tal, y en virtud de lo dispuesto en la LPDP, su reglamento, y la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD, tiene la obligación de inscribir el banco de datos de videovigilancia en el Registro Nacional de Banco de Datos (numeral 6.9)[12].

11 https://www.gob.pe/institucion/anpd/informes-publicaciones/1834826-oc-n-02-2021-jus-dgtaipd-sobre-tratamiento-de-datos-a-traves-de-camaras-de-videovigilancia-en-espacios-de-trabajo-compartidos-cowork

12 **Registro de banco de datos de videovigilancia**

6.9 La persona natural, jurídica o entidad pública que utilice un sistema de videovigilancia o cualquier dispositivo que permita el tratamiento de datos para dicho fin, debe solicitar la inscripción del banco de datos personales respectivo a la Dirección de Protección de Datos Personales, unidad orgánica de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, encargada de la administración del Registro Nacional de Protección de Datos Personales.

6.10 Los sistemas que no almacenan imágenes, sino que consisten exclusivamente en la reproducción y emisión de imágenes en tiempo real, no son considerados bancos de datos. Sin embargo, esto no los exime del cumplimiento de las demás obligaciones contenidas en la LPDP, su reglamento y la presente directiva, en lo que resulte aplicable.

Por su parte, la empresa de *coworking* (arrendadora del espacio) es la encargada del tratamiento, ya que brinda el servicio a raíz de una relación jurídica determinada; y, como tal, debe cumplir con las obligaciones propias de esta condición, de acuerdo con lo dispuesto en los numerales 6.17 y siguientes de la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD[13].

Respecto a la obligación de informar sobre las características del tratamiento realizado mediante sistemas de videovigilancia, conforme el artículo 18 de la LPDP, esta opinión consultiva afirma que, dadas las particularidades del contrato de coworking, la empresa de coworking (arrendadora) será la encargada de tratamiento de la videovigilancia de los distintos *coworkers* o arrendatarios.

En ese sentido, la Autoridad Nacional de Protección de Datos señala que es posible que en la puerta de ingreso al edificio de propiedad de la empresa coworking, donde se encuentran las oficinas o espacios arrendados por las empresas *coworkers*, se coloque un solo cartel informativo, y no un cartel por cada *coworker* o arrendatario. Al respecto, cabe resaltar que dicho cartel debe cumplir

13 **Formalidades que debe seguir el encargado del tratamiento**

6.17 Cuando una persona natural, jurídica o entidad pública ha instalado o pretende instalar un sistema de cámaras de videovigilancia, pero encarga a otra la gestión del sistema con utilización de los equipos o acceso a las imágenes o voces, debe de suscribirse un contrato, convenio o documento similar en el que se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos y categorías de interesados, las obligaciones y derechos que correspondan, así como el destino de los datos al finalizar la prestación.

6.18 El contrato, convenio o documento similar atiende a las circunstancias concretas de la prestación del servicio. El encargado está obligado, en mérito de él, a cumplir con las condiciones técnicas y organizativas necesarias para respetar las obligaciones establecidas en la LPDP; a observar los requisitos legales que lo habilitan para prestar el servicio; a seguir las instrucciones del responsable del tratamiento o del titular del banco de datos; a realizar las acciones necesarias para asistir al responsable o titular del banco de datos en el cumplimiento de su deber de responder frente el ejercicio de los derechos señalados en la LPDP; y, en general, de colaborar en el cumplimiento de las obligaciones del titular del banco de datos.

6.19 El encargado del tratamiento debe garantizar al responsable que el acceso a los datos sólo se realizará por personas debidamente autorizadas debiendo adoptar las medidas de seguridad necesarias para asegurar el adecuado uso del sistema y tratamiento de los datos personales.

6.20 El encargado del tratamiento del sistema de videovigilancia debe notificar, sin dilación, al responsable del tratamiento acerca de la existencia de una violación o brecha de seguridad.

6.21 De acuerdo con lo establecido en el artículo 37 del RLPDP, es posible la subcontratación con terceros, debiendo asumir la persona natural o jurídica subcontratada las mismas obligaciones que se establezcan para el titular del banco de datos, responsable o encargado del tratamiento, según corresponda, de acuerdo con lo establecido en el artículo 38 del RLPDP.

con lo dispuesto en el numeral 6.11 de la Directiva antes mencionada y con lo contenido en el numeral 6.12 de esta misma norma referida a las características del informativo adicional del sistema de videovigilancia.

Asimismo, la opinión consultiva aclara que el control de seguridad en las instalaciones es distinto al control laboral de las actividades realizadas por los trabajadores de las empresas de *coworker*. Al respecto, el control de seguridad se refiere al mantenimiento del orden y la custodia de los bienes e instalaciones de la empresa de *coworking*, de los bienes de las empresas *coworkers* y de las personas que ingresen a las oficinas como, clientes, proveedores, visitantes de las instalaciones, etc. Mientras que la finalidad del control laboral supone la supervisión de las obligaciones laborales de los trabajadores subordinados a la empresa de *coworke*r por parte de esta.

Por lo tanto, concluye que atendiendo al contexto de la actividad de *coworking* que supone compartir espacios de trabajo entre varias personas naturales o jurídicas, en el caso de que una o varias de las empresas de *coworker* decidan utilizar los sistemas de videovigilancia no sólo para fines de seguridad, sino también para fines laborales, estas deberán informar expresa y específicamente a sus trabajadores, titulares de los datos personales captados a través de sistemas de videovigilancia, que estos serán utilizados también para fines de supervisión y control laboral.

Por último, advierte que el control laboral a través de sistemas de videovigilancia sólo será legítimo cuando se realice atendiendo al principio de proporcionalidad, de acuerdo con lo dispuesto en el artículo 7 de la LPDP y el numeral 7.13 y siguientes de la Directiva Nro. 01-2020-JUS/DGTAIP sobre tratamiento de datos personales mediante sistemas de videovigilancia, aprobada por Resolución Directoral Nro. 02-2020-JUS/DGTAIPD.

REFERENCIAS

Aparicio Aldana, R.K. (2016). *Derecho a la Intimidad y a la propia imagen en las relaciones laborales,* Thomson Reuters – Aranzadi.

Desdentado Bonete, A y Muñoz Ruiz, A.B. (2012). *Control informático, videovigilancia y protección de datos en el trabajo,* Lex Nova.

Goñi Sein, J.L. (2014). «Los derechos fundamentales inespecíficos en la relación laboral individual. ¿Necesidad de una reformulación?», Ponencia temática presentada al *XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, celebrado en Pamplona el 29-30 de mayo de 2014. Organizado por la Asociación Española de Derecho del Trabajo y de la Seguridad Social, en colaboración con el área de conocimiento de Derecho del Trabajo y de la Seguridad Social de la Universidad Pública de Navarra, en http://academica-e.unavarra.es/bitstream/handle/2454/10903/Jose_Luis_Gon%CC%83i.pdf?sequence=1