Benites, Vargas & Ugaz
ABOGADOS

Alerta Competencia y Laboral

Año 2020 N° 1

Fecha: 16/01/2020

Ministerio de Justicia y Derechos Humanos aprueba *"Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia"*

El 16 de enero de 2020, se publicó en el Diario Oficial el Peruano la Resolución Directorial N° 02-2020-JUS/DGTAIPD, mediante la cual se aprueba la "Directiva de Tratamiento de Datos Personales mediante Sistemas de Videovigilancia", de conformidad con lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales (en adelante, LPDP) y su Reglamento. A continuación, detallamos sus aspectos más relevantes:

- **Ámbito de aplicación:** Las disposiciones de la Directiva se aplican a las personas naturales y jurídicas que realicen tratamiento de datos personales a través de sistemas de videovigilancia o dispositivos análogos, lo cual comprende: grabación, captación, trasmisión, conservación o almacenamiento de imágenes o voces, incluida su reproducción o emisión en tiempo real o cualquier otro tratamiento relacionado con fines de seguridad, control laboral y otros.

  Respecto a las entidades de la Administración Pública, sólo estarán sujetas a las disposiciones que le resulten aplicables conforme a las normas comunes de derecho público.

  El tratamiento no aplica, tratándose de:

  (i) Datos de personas naturales identificada o identificables que se encuentren almacenados en bases de datos creados para fines relacionados con la vida privada o familiar; o, bases de datos que sean utilizadas en cumplimiento de las competencias de las entidades públicos o para la investigación y represión del delito.
  (ii) Imágenes en el ámbito personal y doméstico, incluyendo el uso de cámara "*on board*" y los sistemas de videoportería (salvo que graben imágenes de modo constante y sean accesibles por internet o emisiones por televisión en circuito cerrado), y se traten de zonas comunes y/o vía pública colindante.
  (iii) Imágenes vinculadas al ejercicio del derecho a la libertad de información y expresión por los medios de comunicación.
  (iv) Sistemas con cámaras o videocámaras simuladas o desactivadas. En este caso aplica la directiva de medidas de seguridad del sistema.

- **Sobre la legitimidad para el tratamiento de datos:** Existe legitimidad cuando: se cuente con el consentimiento del titular de los datos personales; una norma con rango de ley habilite captar los datos sin el consentimiento del titular; o, se dé alguna circunstancia de excepción al consentimiento prevista en la LPDP.

- **Principios aplicables:**

  (i) **Principio de Proporcionalidad:** El uso de cámaras o videocámaras debe ser el medio menos invasivo o igual de eficaz para alcanzar la finalidad perseguida. Deberá existir, por ende, una adecuación medio-fin.

  (ii) **Principio de Seguridad:** El responsable del tratamiento debe adoptar las medidas técnicas y organizativas para garantizar la seguridad de los datos y evitar su alteración, pérdida, tratamiento o acceso no autorizado. En caso de sistemas de videovigilancia de personas jurídicas conectados o que puedan ser conectadas a una central de alarmas o control deben cumplir con lo previsto en el Decreto Legislativo N°1213.

- **Registro de banco de datos de videovigilancia:** Se deberá solicitar la inscripción del banco de datos personales de videovigilancia a la Dirección de protección de Datos personales.

- **Sobre el cartel informativo:** La zona de vigilancia debe tener un cartel o anuncio visible con fondo amarillo o cualquier otro que contraste con el color de la pared. Debe contener: (i) la identidad y domicilio del titular del Banco de Datos Personales, (ii) información ante quién y cómo puede ejercerse los derechos establecidos en la LPDP, y (iii) el lugar donde puede obtenerse la información contenida en el artículo 18 de la LPDP. Los elementos gráficos deben tener como mínimo 297x210 mm.

  En caso la información no pueda ser colocada en su integridad en el cartel, se deberá tener a disposición de los interesados, ya sea a través de medios informáticos digitalizados o impresos, la información mínima requerida para garantizar sus derechos.

- **Sobre el plazo de conservación o almacenamiento de la información:** Las imágenes y/o voces grabadas se almacenan por un plazo mínimo de treinta (30) días y un plazo máximo de sesenta (60), salvo disposición distinta en normas sectoriales. Durante ese plazo, el titular del Banco de Datos Personales o encargado del tratamiento, debe asegurar la reserva y confidencialidad de la información, no permitiendo la difusión, copia o visualización de imágenes a tercero no autorizados, salvo que el contenido presente indicios razonables de la comisión de un delito o falta, lo cual debe ser informado de manera inmediata a la Policía Nacional o Ministerio Público.

- **Sobre la cancelación definitiva de la información:** Transcurrido el plazo de conservación y no habiendo requerimiento de alguna autoridad competente, la información debe ser eliminada en el plazo máximo de dos (2) días hábiles.

- **Sobre la Confidencialidad:** Éste deber podrá materializarse a través de un documento en el que las partes determinen la obligación de no divulgar determinada información. Debe ser suscrito entre las personas encargadas del tratamiento o que tiene acceso a los sistemas de vigilancia y el titular del Banco de Datos Personales.

- **Los derechos de los Titulares de los Datos Personales:**

  (i) **Derecho de acceso**: Los titulares de los datos pueden acceder a la información mediante una solicitud escrita, a través de la entrega de un CD en blanco o dispositivo análogos, o directamente acercándose a las instalaciones del titular del Banco de Datos Personales.

(ii) **Derecho de Cancelación y Oposición**: Su ejercicio procederá en los supuestos que sea materialmente posible y responda a criterios fundamentados y motivados.

- **Imposibilidad del ejercicio del derecho de rectificación:** Dado que las imágenes captadas reflejan un hecho objetivo, no puede ser modificado a petición del titular del dato personal.

- **Tratamientos específicos:** en espacios públicos de uso privado, como establecimientos comerciales, restaurantes, lugares de ocio, entre otras, se debe tener en consideración lo siguiente:
  (i) El uso de sistemas de videovigilancia no aplica tratándose de baños y vestidores.
  (ii) En caso de lugares de ocio solo aplica, si no existe un método de seguridad menos invasivo e igual de eficaz. No pueden ser usados con fines comerciales.
  (iii) El uso de las grabaciones o imágenes no aplica para cuestiones comerciales o promocionales salvo consentimiento de los titulares.

En el caso de Entidades Financieras: lo captado o grabado deber ser utilizado para fines de seguridad. Si el encargado del tratamiento no es una empresa especializada, debe ser el responsable especializado en la materia. La cámara que graba la puerta de entrada debe limitarse al acceso vigilado.

En el caso de Control Laboral: El empleador se encuentra facultado para realizar controles o tomar medidas para vigilar el ejercicio de las actividades laborales de sus trabajadores a través de los sistemas de videovigilancia. A continuación, esbozaremos los principales puntos de la Directiva:

Tema	Detalle
Excepción al consentimiento	El empleador se encuentra facultado para realizar controles o medidas para vigilar el ejercicio de la actividad laboral a través de sistemas de videovigilancia.
Deber de informar	• Trabajadores régimen común: Empleador debe informar mediante carteles o avisos informativos. • Trabajadores del hogar: Acreditar cumplir con informar de forma razonable.
Finalidad de los sistemas de videovigilancia	Finalidad limitada al control y supervisión de la relación laboral, no pueden ser fines distintos, salvo excepciones o consentimiento.
Principio de proporcionalidad	Debe ser pertinente, adecuado y no excesivo para el cumplimiento del fin.
Prohibición de uso de imágenes	Salvo consentimiento, imágenes no pueden ser utilizadas con fines comerciales o publicitarios.
Cancelación de imágenes y/o voces	Las voces y/o imágenes deberán conservarse por el plazo de 30 hasta 60 días. En caso de que las imágenes y/o voces den cuenta una

	comisión de presunta infracción y/o accidente de trabajo, deben ser conservadas por el plazo de 120 días.
Tutela directa de los trabajadores	Los trabajadores deben ser informados sobre el procedimiento para ejercer su derecho de acceso, cancelación y oposición.
Transferencia de datos personales	En caso de transferir datos personales de trabajadores a un tercero, debe informar de ello a los trabajadores y cuando corresponda, solicitar su consentimiento.

En el caso del Entorno Escolar: Los centros educativos deben instalar el cartel o distintivo que informe a la comunidad educativa de la existencia de cámaras u dispositivos análogos en lugares visibles como abiertos. El cartel debe señalar dónde poder obtener la información. Asimismo, la zona de vigilancia de las cámaras deberá ser la mínima imprescindible y debe resguardar la protección y defensa del interés superior del niño, niña y adolescente, no abarca espacios privados que puedan afectar la imagen o intimidad de forma desproporcionada. El acceso es restringido al director o la persona responsable del tratamiento.

En el caso de los drones: La persona encargada de controlar los drones, debe contar con formación especializada en el manejo de los mismos. El deber de garantizar la reserva, confidencialidad y cumplimiento de las demás obligaciones no solo abarca a la persona que controla, sino también, a las personas o entidades que brinden el servicio de videovigilancia por drones, quienes deben informar de manera física o electrónica a las personas que serán controladas mediante este sistema. Si cuentan con una página web, deben publicar la información que permita conocer los diferentes tipos de operaciones realizadas con los datos captados por los drones, o los que piensan realizar en el futuro cercano.

La presente Directiva es aplicable a los sesenta (60) días calendarios desde su publicación en el Diario Oficial El Peruano, y se puede encontrar su texto completo en el siguiente enlace: https://www.minjus.gob.pe/wp-content/uploads/2020/01/Directiva-N%C2%B0-01-2020-DGTAIPD-1.pdf

Nuestro equipo Competencia & PI: Fabricio Sánchez Concha, John-André Flores Uribe, Alexandra Espinoza Montero y Fátima Vega Pinedo.

Nuestro equipo Laboral: Jorge Luis Acevedo, Carla Benedetti, Karla Zuta, Willman Meléndez, María Eugenia Tamariz, Franklin Altamirano, Roberto Vílchez, Carlos Ciriaco, Vanessa Verano, Natalia Peña, Giancarlo Ángeles, Dominick Vera, Briyith Saavedra, Ginneth Martínez y Alfredo Torres.

Av. 28 de Julio 1044, oficina 602, Miraflores – Perú / Teléfono: (511) 615-9090 / Fax: (511) 615-9091 / e-mail: bvu@bvu.pe
Fray Bartolomé de las Casas 478, Urb. San Andrés, Trujillo / Teléfono: (044) 60-8866/ Fax: (044) 60-8867 / e- mail: bvutrujillo@bvu.pe
José Robles Arnao 1060 – Urb. San Francisco, Huaraz / Telefax: (043) 72-4408 / e-mail: uespinoza@bvu.pe