

El Tratamiento de Datos Personales mediante sistemas de Videovigilancia

En el Perú desde el año 2013, mediante la Ley N° 30120 se incluyó, como instrumento de vigilancia en el sistema de seguridad ciudadana, las imágenes y voces registradas a través de las cámaras de seguridad ubicadas en la parte externa de inmuebles, de propiedad de las personas naturales y jurídicas, públicas y privadas.

Sin embargo, el sistema de videovigilancia no solo adquirió relevancia en el apoyo a la seguridad ciudadana, sino también en la supervisión del empleador a sus trabajadores, en la protección de menores, en el sistema financiero, entre otros.

En ese contexto, era necesario definir los lineamientos para el uso adecuado de estos dispositivos, debido a que las imágenes y/o voces registradas en las cámaras de seguridad son consideradas datos personales, conforme lo señala la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento, Decreto Supremo N° 003-2013-JUS.

En atención a ello, el 17 de marzo del 2020 entró en vigencia la Directiva N° 01-2020-JUS/DGTAIPD formulada por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales perteneciente al Ministerio de Justicia y Derechos Humanos (MINJUSDH), la cual tiene como objetivo establecer disposiciones para el tratamiento de los datos personales captados a través de un sistema de cámaras ya sea en tiempo real o en visualización de grabaciones de imágenes, vídeos o audios.

El sistema de videovigilancia que permite el tratamiento de datos personales a través de las grabaciones de imágenes y/o voces se considera un banco de datos personales, por lo que debe quedar inscrito en la Dirección de Protección de Datos Personales, unidad orgánica perteneciente al MINJUSDH. En esa línea, los sistemas que no almacenan imágenes ni voces, sino que consisten exclusivamente en la reproducción y emisión de imágenes en tiempo real, no son considerados bancos de datos, por lo que no es necesario su registro; sin embargo, no quedan exentos del cumplimiento de las demás obligaciones señaladas en la norma, en lo que resulte pertinente.

Por ello, el titular del banco de datos es el encargado del tratamiento adecuado de los datos personales, por lo que será el responsable de garantizar la seguridad, integridad y confidencialidad de la información, no permitiendo el acceso, difusión, copia o visualización de imágenes por terceros no autorizados.

Las pautas señaladas en la Directiva además de enfatizar en la importancia de la seguridad del sistema de videovigilancia, también resalta el principio de proporcionalidad, en virtud del cual el uso de cámaras será legítimo cuando no exista un medio menos invasivo o igual de eficaz para alcanzar la finalidad perseguida.

En ese sentido, el sistema de videovigilancia en los establecimientos comerciales, restaurantes, lugares de ocio, entre otros, sólo puede ser visual, está prohibida la grabación de las conversaciones. Por otro lado, la grabación de sonido solo está permitida en el centro laboral cuando exista riesgo para la seguridad de las instalaciones, bienes o personas. En caso de entornos escolares, sí se permite la videovigilancia en espacios públicos o comunes como accesos y pasillos, patio de recreo, incluso en las aulas cuando exista riesgo para la seguridad y los derechos fundamentales de los menores. Mientras tanto, cuando se trata de entidades financieras, si una cámara se ubica en la puerta de entrada, debe limitarse a captar el acceso vigilado, sin captar más proporción de la vía pública que la necesaria para efectos de la labor de vigilancia; lo que se condice con el respeto a los derechos fundamentales de terceros, por ello las cámaras instaladas en espacios privados no pueden obtener imágenes de espacios públicos, salvo que resulte imposible evitarlo.

En ningún caso se admite la instalación de sistemas de videovigilancia en servicios higiénicos, vestuarios, y en el centro laboral no se permite en lugares destinados al descanso o esparcimiento de los trabajadores, comedores o análogos.

Con referencia al principio de información, cada acceso a una zona videovigilada debe tener un cartel o anuncio visible comunicando al usuario quién es el titular del banco de datos personales, el lugar donde puede ejercer su derecho de acceso a las grabaciones y ante quién puede solicitarlo; sin perjuicio de la política de privacidad que puede estar disponible a través de medios informáticos, digitalizados o impresos.

En cuanto a la autorización del usuario para el tratamiento de sus datos personales, en principio se debe contar con su consentimiento; sin embargo, no será necesario si existe una norma con rango de ley que permita las grabaciones sin su consentimiento, como sucede

en el centro laboral, donde el empleador se encuentra facultado para supervisar las actividades de sus trabajadores. A su vez, tampoco se requerirá el consentimiento del titular del dato personal, cuando exista una orden judicial o un requerimiento de las grabaciones de la Policía Nacional del Perú o el Ministerio Pública, en razón del ejercicio de sus funciones. Por otro lado, el consentimiento debe ser expreso cuando las imágenes captadas tengan fines comerciales o publicitarios.

Sobre el plazo de almacenamiento de las grabaciones será desde 30 días como mínimo hasta 60 días como máximo, salvo excepciones que justifiquen plazos diferentes, como sucede por ejemplo con las entidades educativas, donde el plazo para conservar las imágenes es máximo 30 días; o, en la comisión de presuntas infracciones laborales y/o accidentes de trabajo donde el plazo puede ser hasta 120 días. De cualquier manera, cuando exista una justificación o la existencia de un interés legítimo, el plazo puede ser mayor al establecido por la norma y transcurrido el plazo de almacenamiento, según sea el caso, se debe eliminar los archivos en un plazo máximo de dos días.

Finalmente, el titular del dato personal debe cumplir determinados requisitos formales para acceder a una copia de las grabaciones, donde será necesario que el titular o encargado del banco de datos utilice máscaras de privacidad o difumine imágenes que afecten derechos de terceros, salvo que el solicitante acredite su legítimo interés para contar con las imágenes completas, a fin de usarlo como prueba en algún proceso administrativo o judicial. En el mismo sentido, no se aplicarán las máscaras de privacidad cuando se identifiquen hechos que configuren indicios razonables de la comisión de una falta o delito, en ese caso el titular del banco de datos debe entregar inmediatamente las grabaciones al Ministerio Público o Policía Nacional del Perú.

Por **Patricia Vera** - Miembro del Comité de Protección de Datos de la World Compliance Association Capítulo Perú