HIPER DERECHO
Liberando la tecnología

Lima, 5 de septiembre de 2019

Eduardo Luna Cervantes
Director General
Dirección General de Transparencia, Acceso a la Información Pública, y Protección de Datos Personales
Ministerio de Justicia y Derechos Humanos
Presente. —

Asunto: Comentarios al Proyecto de Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia

Hiperderecho es una asociación civil peruana sin fines de lucro dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por abogados y especialistas en tecnología. Como parte de nuestro trabajo, estudiamos todas las iniciativas de política pública que puedan impactar el ejercicio de derechos y libertades en estos ámbitos.

Saludamos la iniciativa de su institución por la elaboración de esta directiva y su sometimiento a consulta pública. Representa una respuesta oportuna a un creciente aspecto en polémica sobre cómo la tecnología está impactando el derecho de todos los peruanos a la protección de sus datos personales.

Existen diferentes normas sobre seguridad ciudadana que crean obligaciones para actores privados y públicos de instalar y operar cámaras de este tipo, y es previsible que en los próximos años se produzca un incremento exponencial en su número y ubicación a nivel nacional. Por ende, resulta necesario conocer qué procedimientos deben seguir quienes usen estas tecnologías y cómo los sujetos sometidos a la videovigilancia (directa o indirecta, continua o casual) pueden hacer uso de su derecho a la protección de sus datos personales.

Comentarios

1. Desarrollo del principio de proporcionalidad

En la Directiva, se establecen diferentes principios orientadores, entre ellos el de Proporcionalidad que señala:

> El tratamiento de los datos personales debe ser adecuado, pertinente y no excesivo en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras (...).

No obstante, a lo largo del texto de la Directiva, este principio no es desarrollado de forma extensiva, perdiendo la oportunidad de entrar en detalle sobre cuestiones que consideramos importantes. Uno de los elementos que debería considerarse es la inclusión de una tabla de referencia que permita conocer qué tipo de cámaras de videovigilancia resultan "proporcionales" al menos para los fines claramente establecidos en la Directiva: seguridad, entornos escolares y control laboral.

Por ejemplo, el Proyecto de Reglamento de la Ley N° 30120 y el Decreto Legislativo N° 1218, normas que crean obligaciones sobre el uso e instalación de cámaras de videovigilancia, incluyen entre sus artículos estándares mínimos para la instalación de nuevas cámaras, con el fin de que las grabaciones obtenidas resulten útiles para las autoridades. Solo por citar uno de estos requisitos, se exige que estas deben poseer "Captura de imágenes en resolución de alta definición o con una resolución equivalente a 1920 por 1080 píxeles por pulgada, y que permita la identificación de rostros de personas de manera nítida". Además, se especifica que en bienes de dominio público o centros comerciales "se instalan videocámaras tipo "domo" buscando que tengan movimiento horizontal de 360 grados, vertical de 180 grados y capacidad de acercamiento o alejamiento de captación de un área o un objeto en forma manual o automática, más conocido como "zoom." Finalmente, se hace una diferenciación sobre las cámaras que se colocan en vehículos de transporte público, las cuales tienen una menor resolución, son fijas y poseen funciones de visión nocturna y micrófono.[1]

Pese a que el anterior Reglamento no se encuentra aprobado y por lo tanto no está en vigor ninguna de sus disposiciones, no escapa de nuestra observación que en el futuro este texto podría aprobarse tal cual o con modificaciones. Esto a su vez podría suponer nuevos retos de interpretación para la normativa de protección de datos respecto de la proporcionalidad del tratamiento en contextos de videovigilancia. Por ello, sugerimos encarecidamente que se incluya, aunque sea a modo orientativo (es decir, no obligatorio) una tabla de referencia que describa a partir de sus características técnicas (tamaño, funcionalidades, nivel de detalle de captura, tecnología, etc.) a las cámaras de videovigilancia que sean mínimamente compatibles con el principio de proporcionalidad en las diferentes situaciones establecidas en la Directiva.

2. Plazo de conservación de los datos almacenados de videovigilancia

La Directiva establece por regla general, respecto al plazo:

> Las imágenes y voces grabadas se almacenan por un plazo no mayor de sesenta (60) días, salvo disposición distinta en normas sectoriales. Durante ese plazo, el titular del banco de datos o encargado del tratamiento de los datos debe asegurar la reserva y confidencialidad de la información, no permitiendo la difusión, copia o visualización de imágenes por terceros no autorizados (...).

[1] Decreto Supremo que aprueba el Reglamento del uso de las cámaras de videovigilancia dispuesto por la Ley N° 30120 y el Decreto Legislativo N° 1218. Enlace: http://spij.minjus.gob.pe/Graficos/Peru/2018/Abril/01/RM-485-2018-IN.pdf

Al respecto, consideramos que no existe sustento para establecer dicho plazo o que este no ha sido explicado de forma suficiente en el preámbulo de la Directiva. Consideramos que el plazo general debería ser el mínimo exigible, siendo en este caso el que se asigna en la Directiva al tratamiento en Entornos Escolares, es decir, treinta (30) días. De hecho, el Proyecto de Reglamento de la Ley N° 30120 y el Decreto Legislativo N° 1218 (pendiente de entrar en vigencia) establecen dicho plazo, tras el cual todo material que no ha sido requerido por las autoridades debe ser destruido o borrado. Solo en el caso de la Ley N° 30037 se da el caso que dicha conservación se da por un plazo mayor, pero este es circunstancial y no fijado de forma previa.[2]

Creemos que proponer un plazo de 60 días para la conservación de los datos es una medida que no contribuye sustancialmente para los fines legítimos por los cuales se permite la videovigilancia, es decir: la seguridad y el control laboral en el ámbito de dirección del empleador. Primero, porque ya existen en todas las normas relacionadas a la seguridad la disposición de que los responsables de las cámaras den parte inmediato a las autoridades sobre la posible comisión de faltas o delitos. Segundo, porque ocurre lo mismo en el caso de los trabajadores, cuyas posibles faltas a la normativa laboral o interna de la empresa deberían ser supervisadas de forma proactiva por el empleador, para lo cual el plazo de 30 días resulta más que suficiente. Tercero porque, ante el aviso de que ha ocurrido un incidente que requiere la revisión de imágenes y/o audio almacenados en bancos de datos, los titulares de estos bancos ya se encuentran facultados para extender el tratamiento bajo el amparo de las leyes.

Existe también un argumento económico en contra de un plazo tan largo: Obligar a conservar por 60 días todo lo que una cámara de videovigilancia puede grabar. repercute negativamente en la economía de quienes poseen u operan las cámaras, pues deben contratar mejores cámaras, servicios de almacenamiento más grandes y, en ciertos casos, asumir nuevos costos para cumplir con los derechos ARCO aplicables en un plazo tan extendido. Esto se agrava si se tiene en cuenta que existen varias leyes actualmente vigentes que obligan a ciertos sujetos a instalar y operar las cámaras de vigilancia, incluso haciendo de ello un requisito para realizar trámites como obtener licencias y permisos de operación. Ir más allá de lo mínimo indispensable puede no suponer un problema para grandes empresas, pero puede ser crítico para MYPES e incluso para personas naturales sobre las que recaen las obligaciones legales antes referidas.

En el preámbulo del Proyecto de Reglamento de la Ley N° 30120 y el Decreto Legislativo N° 1218 se expresa el temor de que la obligación de instalar cámaras pueda ser considerada barrera burocrática. Por ende, para evitar esta situación, se toman ciertas medidas como establecer requisitos mínimos para las cámaras, que haga que su adquisición no resulte

[2] Decreto Supremo que aprueba el Reglamento de la Ley Nº 30037, Ley que previene y sanciona la violencia en los Espectáculos Deportivos:
Artículo 39.- Sistemas de video vigilancia
(...)
39.5. Los organizadores de espectáculos deportivos deben conservar y remitir la información obtenida de las cámaras de vigilancia a la Policía Nacional del Perú hasta el último día hábil del mes siguiente a la realización del espectáculo deportivo. Si no pudiera remitirse la grabación por imposibilidad del calendario será entregada el primer día hábil del mes siguiente.

demasiado onerosa para los sujetos obligados. No obstante, establecer un plazo tan largo de conservación podría abonar a la hipótesis de que esta medida es una barrera burocrática.

3. Vigilancia a través de *drones*

De la misma forma que en el punto 1 de nuestros comentarios, nos gustaría que se estableciera, aunque sea a modo de referencia, una tabla de características mínimas que cumplen con el principio de proporcionalidad en el caso de los drones. No obstante, consideramos que sería ideal que el establecimiento de normativa relacionada a los drones en el ámbito de protección de los datos personales sea tratado en otro documento, en el cual se aborde específicamente las connotaciones que tiene el uso de estos dispositivos en general y no solo en el ámbito de la videovigilancia. Esta normativa debe necesariamente abarcar no solo drones sino también la vigilancia que se lleva a cabo a través de helicópteros y globos aerostáticos.

4. Cámaras de vigilancia con reconocimiento facial incorporado

Invitamos a su despacho considerar la creciente realidad del uso de cámaras de vigilancia en espacios públicos y privados que, además, incorporan tecnologías de reconocimiento facial. Esta tecnología representa un nivel de registro de datos superior al de las cámaras de vigilancia comunes porque, además de registrar la imagen de cualquier persona, tiene la posibilidad de individualizarla en función a sus datos biométricos contra un registro previo interno (visitantes anteriores, personas de interés) o externo (de alguna base de datos comercial o pública).

Esta tecnología representa la posibilidad de que se generen bases de datos de desplazamientos de personas por la ciudad, de visitas frecuentes a ciertos establecimientos, monitoreo de marchas y protestas públicas, entre otros. En estos casos, consideramos que debe de ser estricta la aplicación de los principios de legalidad, proporcionalidad y de minimización de riesgo para evitar que se generen bases de datos de hábitos, preferencias y comportamientos innecesarias o que abran un escenario de riesgo importante para la población. Particularmente, el posible uso indiscriminado de estas tecnologías por parte de las municipalidades y Policía Nacional debe de ser previamente considerado en función de sus eficacia, protocolos de protección de datos, necesidad y proporcionalidad.

Agradecemos su atención y esperamos estos comentarios puedan enriquecer este ejercicio participativo que viene promoviendo su institución.

Miguel Morachimo Rodríguez
Director Ejecutivo

Carlos Guerrero Argote
Director de Políticas Públicas

Asociación Civil Hiperderecho
Email: miguel@hiperderecho.org