Protección de datos personales ante la expansión de la videovigilancia privada

por Claudia Pereiro*

La videovigilancia en edificios y fincas privadas ha crecido exponencialmente, alimentada por la necesidad de sentirnos seguros y por la accesibilidad de insumos producto de los avances tecnológicos. En este breve informe recopilaremos los elementos que en el ejercicio de nuestra profesión, e incluso en nuestra vida personal, debemos tener presentes, desde la doble perspectiva de ser celosos de nuestros datos personales y de ser responsables de los datos de terceros.

Videovigilancia, de acuerdo con el dictamen 10/010 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales —en adelante, URCDP o simplemente «Unidad Reguladora»—, se define como «toda grabación, captación, transmisión, conservación y almacenamiento de imágenes y, en algunos casos, de sonidos mediante la utilización de videocámaras u otro medio análogo» (Presidencia de la República, 2010). Tanto las imágenes como los sonidos —en especial, la voz— pueden constituir datos personales, en cuanto identifican o permiten la identificación de una persona. Por ello, son de aplicación las normas de protección de datos personales consagradas por la ley 18.331, del 11 de agosto de 2008, y su decreto reglamentario 414/009, de 31 de agosto de 2009; y en especial, todos los principios y obligaciones allí contenidos.

Los principios que corresponde considerar son:

1. *Principio del consentimiento*. Es preciso contar con el consentimiento del titular del dato.

* Escribana pública; integrante de las comisiones de Derecho Registral y de Derecho Informático y Tecnológico del Instituto de Investigación y Técnica Notarial de la AEU.

2. *Principio de finalidad* (protección de personas físicas, derecho de propiedad, prevención de delitos, etc.). Este principio implica que hay un propósito para el que se recaban los datos. Cumplida su finalidad, el dato debe ser suprimido.
3. *Principio de proporcionalidad*. Los datos recabados deben ser adecuados, no excesivos y proporcionales a la finalidad.
4. *Principio de seguridad y veracidad*. El responsable de los datos debe garantizar la seguridad de las imágenes y evitar su pérdida, modificaciones, tratamiento o acceso no autorizados.
5. *Principio de legalidad*. El tratamiento debe ser lícito y cumplir con la normativa vigente. Las bases de datos no deben tener finalidades violatorias de derechos humanos ni contravenir la moral pública.

Los responsables de las bases de datos de videovigilancia deben cumplir con las siguientes obligaciones:

1. Ser responsables por el cumplimiento de la normativa referida a la protección de datos personales.
2. Actuar con la debida reserva y adoptar las medidas de seguridad para garantizar que solo las personas autorizadas accedan a los datos.
3. Mantener la información en forma confidencial, en carácter de custodio.
4. Garantizar al titular del dato acceder a él. Para ello, deberá adoptarse un «distintivo o logo» para determinar al responsable ante quien se podrán ejercer los derechos —aplicación de los principios de información y transparencia—, así como su domicilio.
5. Registrar la base de datos en el registro a cargo de la Unidad Reguladora.

La URCDP publicó en enero de 2017, en su página web, una guía de videovigilancia en edificios, complejos y cooperativas en la que se especifican los recaudos a tener en cuenta (Presidencia de la República, 2018):

1. Las cámaras no pueden utilizarse en espacios públicos, locales sindicales, baños y vestuarios, entre otros, ni enfocarse hacia predios linderos. Recordemos que en el ámbito laboral no es posible invadir la intimidad y privacidad del trabajador.
2. No pueden captarse imágenes de la vía pública, a excepción de una franja mínima e imprescindible de acceso al lugar (aplicación del *principio de proporcionalidad*).
3. Una vez instalado el sistema de videovigilancia, debe registrarse la base de datos.
4. Operativo el sistema, deben colocarse los distintivos de área videovigilada en lugares visibles, con indicación del nombre del responsable y el lugar donde las personas pueden ejercer sus derechos. Frente

una solicitud de acceso, el responsable debe proteger la privacidad de otros sujetos que aparezcan en las imágenes, a través de la utilización de «máscaras» de seguridad o brindando la información por escrito. También deberá entregarse la información cuando así lo requiera la Policía o la Justicia.

5. Para instalar un sistema de videovigilancia es necesario que la resolución se adopte en la asamblea de copropietarios u órgano similar, por mayoría.
6. En el caso de edificios, complejos o cooperativas, las videocámaras pueden ser instaladas en espacios comunes como escaleras, ascensores, *hall* de entrada, pasillos y cualquier otro bien denominado «común» en el reglamento de copropiedad. En todos los casos, el número de cámaras debe ser proporcional al área a vigilar.
7. El sistema de grabación debe estar ubicado en un lugar de acceso restringido y solo accesible a personal autorizado.
8. Si se contrata un servicio de vigilancia que incluya videovigilancia, se recomienda la suscripción de un contrato entre la empresa y la copropiedad en el que se establezca quiénes son los encargados de acceder a la información y cuáles son las condiciones del servicio.[1]

Estos y otros criterios fueron dispuestos y compilados por la resolución 58/021, de 21 de diciembre de 2021, sobre «tratamiento de información obtenida por cámaras de videovigilancia» en los casos que nos convocan, como en otras situaciones, a saber: cámaras con finalidad personal o doméstica; con fines de seguridad pública; que se utilicen en ámbitos de actividad bancaria; que se utilicen en ámbitos laborales; implementadas en entidades públicas; usadas en vehículos y similares; usadas en instituciones educativas de Primaria y Secundaria, y drones (Presidencia de la República, 2021*b*).

Vivamos en ámbitos seguros. Apliquemos la tecnología para lograrlo, sin violentar los derechos de las personas.

1 Vé.: dictamen 22/021 de la URCDP: «Las empresas que prestan servicios de videovigilancia y realizan tratamiento de datos personales de sus clientes y de las personas que son captadas por sus sistemas serán consideradas responsables o encargados, según lo dispuesto por los literales *H* y *K* del artículo 4.º de la ley 18.331 […]. Aun cuando se encuentren fuera del territorio nacional, se encuentran sometidos a la ley uruguaya». En virtud de prestar servicios a habitantes del país, «deberán dar cumplimiento a las obligaciones de la ley 18.331 […], incluyendo el registro de sus bases de datos y brindando la información de contacto correspondiente ante la URCDP». «El alojamiento de las bases de datos en una nube en el exterior constituye una transferencia internacional de datos», por lo que es aplicable el artículo 23 de la ley 18.331 y la resolución 23/021 del Consejo (Presidencia de la República, 2021*a*).

Bibliografía referida

Presidencia de la República (2010). Dictamen 10/010 del Consejo Ejecutivo de la URCDP, de 16 de abril de 2010. Montevideo: Presidencia de la República, Agesic, URCDP. Recurso en línea. Recuperado de: ‹https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicación/publicaciones/dictamen-10010›.

— (2018). «Guía de videovigilancia en edificios y complejos habitacionales». Montevideo: Presidencia de la República, Agesic, URCDP. Recurso en línea. Recuperado de: ‹https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-de-videovigilancia-en-edificios-y-complejos-habitacionales›.

— (2021*a*). Dictamen 22/021 del Consejo Ejecutivo de la URCDP, de 14 de diciembre de 2021. Montevideo: Presidencia de la República, Agesic, URCDP. Recurso en línea. Recuperado de: ‹https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/dictamen-n-22021›.

— (2021*b*). Resolución 58/021 del Consejo Ejecutivo de la URCDP, de 21 de diciembre de 2021. Montevideo: Presidencia de la República, Agesic, URCDP. Montevideo: Presidencia de la República, Agesic, URCDP. Recurso en línea. Recuperado de: ‹https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-n-58021›.

Otra bibliografía consultada

Agencia Española de Protección de Datos (AEPD) (2006). Instrucción 1/2006 de la AEPD, de 8 de noviembre de 2006. En *Boletín Oficial del Estado*, n.º 296 (dic.). Madrid: Agencia Estatal (España), AEPD. Recurso en línea. Recuperado de: ‹https://www.boe.es/eli/es/ins/2006/11/08/1/con›.

— (2023). *Guía sobre el uso de videocámaras para seguridad y otras finalidades*. Madrid: Agencia Estatal (España), AEPD. Recurso en línea. Recuperado de: ‹https://www.aepd.es/documento/guia-videovigilancia.pdf›.

Bernasconi, Mariella (coord.) (2022). «Protección de datos personales: Clearing de Informes, derecho al olvido y cámaras de videovigilancia». Trabajos realizados por estudiantes de Actividad Integrativa de Extensión e Investigación (curso 2022). En *Revista de Técnica Forense*, n.º 26, pp. 191-207. Montevideo: Udelar, Facultad de Derecho, Instituto de Técnica Forense.

Brian Nougrères, Ana (2017). «Los sistemas de videovigilancia y la protección de datos personales». En *Tribuna del Abogado*, n.º 204 (oct.-dic.), pp. 16-19. Montevideo: Colegio de Abogados del Uruguay.

Gil Membrado, Cristina (2019). *Videovigilancia y protección de datos. Especial referencia a la grabación de la vía pública desde el espacio privado*. Madrid: Wolters Kluwer.

Hormaizteguy, Gabriela (2013). «El uso de las nuevas tecnologías y la protección de datos personales en Uruguay. Videovigilancia: ¿derechos fundamentales vulnerados?». Trabajo presentado al XVII Congreso Iberoamericano de Derecho e Informática (FIADI).