Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo

Versión 2.0

Adoptado el 29 de enero de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historial de versiones

Versión 2.1	26 de febrero de 2020	Corrección de un error sustancial
Versión 2.0	29 de enero de 2020	Adopción de las directrices tras la consulta pública
Versión 1.0	10 de julio de 2019	Adopción de las directrices para consulta pública

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, «RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité conjunto del EEE n.º 154/2018, de 6 de julio de 2018,[1]

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO LAS SIGUIENTES DIRECTRICES

1 INTRODUCCIÓN

1. El uso intensivo de dispositivos de vídeo afecta al comportamiento de los ciudadanos. La aplicación significativa de estas herramientas en muchos aspectos de la vida de los ciudadanos presionará a estos aún más para evitar la detección de lo que pueda percibirse como anomalías. De hecho, estas tecnologías pueden limitar las posibilidades de movimientos y usos anónimos de los servicios y en general limitar la posibilidad de que pasen desapercibidos. Las repercusiones de cara a la protección de datos son enormes.

2. Aunque los ciudadanos puedan sentirse cómodos con la videovigilancia configurada por ejemplo con una finalidad de seguridad determinada, deben adoptarse medidas para evitar cualquier uso indebido con fines totalmente diferentes y, respecto al interesado, con fines imprevistos (p. ej., objetivos de mercadotecnia, supervisión del rendimiento de los empleados, etc.). Además, actualmente se están implementando numerosas herramientas para explotar las imágenes capturadas y convertir las cámaras tradicionales en cámaras inteligentes. La cantidad de datos generados por el vídeo, combinada con estas herramientas y técnicas aumentan los riesgos de usos secundarios (relacionados o no con la finalidad asignada en un principio al sistema) o incluso los riesgos de usos indebidos. Los principios generales del RGPD (artículo 5) se deben tener siempre muy en cuenta cuando se trata de videovigilancia.

3. Los sistemas de videovigilancia cambian en muchos aspectos la forma en que los profesionales del sector público y privado interactúan en lugares privados o públicos a efectos de aumentar la seguridad, obtener análisis de audiencia, prestar servicios de publicidad personalizados, etc. La videovigilancia ha resultado muy eficaz gracias a la creciente aplicación del análisis de vídeo inteligente. Estas técnicas pueden ser más intrusivas (p. ej., complejas tecnologías biométricas) o menos intrusivas (p. ej., simples algoritmos de recuento). Por lo general resulta cada vez más difícil permanecer en el anonimato y preservar la propia privacidad. Los problemas planteados respecto a la protección de datos en cada

[1] Las referencias a los «Estados miembros» realizadas en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».

situación pueden diferir, de la misma forma que el análisis jurídico, cuando se utilice una u otra de estas tecnologías.

4. Además de los problemas de privacidad, también existen los riesgos relativos a posibles averías de estos dispositivos y los prejuicios que pueden conllevar. Los investigadores han señalado que el software utilizado para la identificación, el reconocimiento o el análisis facial funciona de manera diferente en función de la edad, del sexo y del origen étnico de la persona a la que identifica. Los algoritmos funcionan según diferentes factores demográficos, por lo que el sesgo del reconocimiento facial amenaza con aumentar los prejuicios de la sociedad. Es este el motivo por el que los responsables del tratamiento de los datos deben también garantizar que el tratamiento de los datos biométricos derivado de la videovigilancia se someta a una evaluación periódica de la importancia y suficiencia de las garantías que proporciona.

5. La videovigilancia no constituye por defecto una necesidad cuando existen otros medios de conseguir la finalidad subyacente. De lo contrario se corre el riesgo de cambiar las normas culturales, lo que llevaría a aceptar la falta de privacidad como algo común.

6. Estas directrices tienen por objeto ofrecer una orientación sobre cómo aplicar el RGPD en relación con el tratamiento de datos personales a través de dispositivos de vídeo. Los ejemplos no son exhaustivos y el razonamiento general se puede aplicar a todos los posibles ámbitos de utilización.

2 ÁMBITO DE APLICACIÓN[2]

2.1 Datos personales

7. La supervisión automatizada y sistemática de un espacio concreto por medios ópticos o audiovisuales, principalmente a efectos de la protección de los bienes o de la vida y la salud de las personas, se ha convertido en un fenómeno significativo en nuestros días. Esta actividad propicia la obtención y conservación de información pictórica o audiovisual sobre todas las personas que entren en el espacio controlado a las que se pueda identificar por su aspecto u otros elementos específicos. La identidad de estas personas se puede determinar sobre la base de estos datos. También permite el tratamiento de datos personales en cuanto a la presencia y al comportamiento de las personas en ese espacio en concreto. El riesgo potencial de uso indebido de estos datos aumenta en relación con la dimensión del espacio controlado así como con la cantidad de personas que lo frecuentan. Este hecho se refleja en el Reglamento General de Protección de Datos en el artículo 35, apartado 3, letra c), que exige la realización de una evaluación de impacto de la protección de datos en caso de observación sistemática a gran escala de una zona de acceso público, así como en el artículo 37, apartado 1, letra b), que exige a los encargados del tratamiento designar a un delegado de protección de datos si la naturaleza del tratamiento conlleva una observación habitual y sistemática de los interesados.

8. No obstante, el Reglamento no se aplica al tratamiento de datos que no se refieran a una persona, esto es, si no se puede identificar a una persona, ni directa ni indirectamente.

> Ejemplo: El RGPD no es aplicable a las cámaras falsas (es decir, cualquier cámara que no funcione como tal y que por lo tanto no trate datos personales). *Sin embargo, en algunos Estados miembros, puede estar sujeto a otras normativas.*
>
> Ejemplo: Las grabaciones a gran altura únicamente están en el ámbito de aplicación del RGPD si en las circunstancias concretas los datos tratados están relacionados con una persona específica.
>
> Ejemplo: Una cámara de vídeo está integrada en un vehículo para ofrecer aparcamiento asistido. Si la cámara está fabricada o configurada de forma que no recopile información relativa a una persona física (como matrículas o información que pueda identificar a los transeúntes), el RGPD no es de aplicación.

9.

2.2 Aplicación de la Directiva sobre protección de datos [DPD, (UE) 2016/680]

10. Concretamente, el tratamiento de datos personales por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública, pertenece al ámbito de aplicación de la Directiva (UE) 2016/680.

[2] El Comité Europeo de Protección de Datos (CEPD) señala que, cuando el RGPD así lo permita, podrán aplicarse requisitos específicos en la legislación nacional.

2.3 Exención de las actividades de tratamiento de carácter doméstico

11. De conformidad con el artículo 2, apartado 2, letra c), el tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, que puede incluir también actividades en línea, queda fuera del ámbito de aplicación del RGPD.[3]

12. Esta disposición, denominada exención de las actividades de tratamiento de carácter doméstico, se debe interpretar en sentido estricto en el contexto de la videovigilancia. Por lo tanto, tal y como considera el Tribunal de Justicia Europeo, la denominada «exención de las actividades de tratamiento de carácter doméstico» debe «*interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es este el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por internet de modo que resulten accesibles a un grupo indeterminado de personas*»[4]. Asimismo, si un sistema de videovigilancia, en la medida en que implique la grabación constante y el almacenamiento de datos personales y se extienda *«aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente "personal o doméstica" a efectos del artículo 3, apartado 2, segundo guion, de la Directiva 95/46»*[5].

13. En lo que respecta a los dispositivos de vídeo operados en el interior de la vivienda de un particular, pueden estar comprendidos en la exención de las actividades de tratamiento de carácter doméstico. Dependerá de varios factores, todos los cuales deberán tenerse en cuenta a la hora de llegar a una conclusión. Además de los elementos antes mencionados identificados en las resoluciones del Tribunal de Justicia, el usuario de la videovigilancia en el entorno doméstico debe considerar si tiene algún tipo de relación personal con el interesado, si la envergadura o la frecuencia de la vigilancia sugiere algún tipo de actividad profesional por su parte y el posible impacto adverso de la vigilancia en los interesados. La presencia de uno solo de los elementos antes mencionados no sugiere necesariamente que el tratamiento esté fuera del ámbito de aplicación de la exención de las actividades de tratamiento de carácter doméstico, por lo que es necesaria una evaluación global para tal determinación.

[3] Véase asimismo el considerando 18.

[4] Tribunal de Justicia Europeo, asunto C-101/01, *Bodil Lindqvist*, 6 de noviembre de 2003, apartado 47.

[5] Tribunal de Justicia Europeo, asunto C-212/13, *František Ryneš/Úřad pro ochranu osobních údajů*, 11 de diciembre de 2014, apartado 33.

Ejemplo: Un turista está grabando vídeos tanto con su teléfono móvil como con una cámara de vídeo para documentar sus vacaciones. Muestra las imágenes a sus familiares y amigos pero no las hace accesibles a una cantidad indefinida de personas. Esto estaría comprendido en la exención de las actividades de tratamiento de carácter doméstico.

Ejemplo: Una ciclista de montaña desea grabar su descenso con una cámara de acción. Recorre un área remota y solo piensa usar las grabaciones para su entretenimiento personal en el hogar. Esto estaría comprendido en la exención de las actividades de tratamiento de carácter doméstico aunque en cierta medida se traten datos personales.

Ejemplo: Una persona está vigilando y grabando su propio jardín. La propiedad está vallada y únicamente el propio responsable y su familia entran en el jardín regularmente. Esto estaría comprendido en la exención de las actividades de tratamiento de carácter doméstico, siempre y cuando la videovigilancia no se extienda, aun parcialmente, a un espacio público o propiedad vecina.

14.

3 LICITUD DEL TRATAMIENTO DE DATOS

15. Antes de utilizarse, las finalidades del tratamiento deben especificarse de forma detallada [artículo 5, apartado 1, letra b)]. La videovigilancia puede tener varias finalidades, p. ej., ayudar a proteger la propiedad y otros activos, ayudar a proteger la vida y la integridad física de las personas u obtener pruebas para demandas civiles.[6] Estas finalidades de vigilancia se deben documentar por escrito (artículo 5, apartado 2) y deben especificarse para cada cámara de vigilancia que se utilice. Las cámaras que se usen con la misma finalidad por un solo responsable se pueden documentar conjuntamente. Asimismo, se debe informar a los interesados sobre la o las finalidades del tratamiento de conformidad con el artículo 13 (*véase el apartado 7, Obligaciones de transparencia e información*). La videovigilancia basada en la mera finalidad de «seguridad» o «por su seguridad» no es lo suficientemente específica [artículo 5, apartado 1, letra b)]. Además es contraria al principio según el cual los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado [véase el artículo 5, apartado 1, letra a)].

16. En principio, cada fundamento jurídico con arreglo al artículo 6, apartado 1, pueden proporcionar una base jurídica para el tratamiento de datos de videovigilancia. Por ejemplo, el artículo 6, apartado 1, letra c) se aplica cuando la legislación nacional estipule la obligación de llevar a cabo la videovigilancia.[7] No obstante, en la práctica, las disposiciones que con más probabilidad se van a utilizar son las siguientes:

- artículo 6, apartado 1, letra f) (interés legítimo);
- artículo 6, apartado 1, letra e) (necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos).

En casos más bien excepcionales, el artículo 6, apartado 1, letra a) (consentimiento) se puede utilizar como base jurídica por el responsable del tratamiento.

3.1 Interés legítimo [artículo 6, apartado 1, letra f)]

17. La evaluación jurídica del artículo 6, apartado 1, letra f) debe basarse en los siguientes criterios de conformidad con el considerando 47.

3.1.1 Existencia de un interés legítimo

18. La videovigilancia es legítima si es necesaria para cumplir la finalidad del interés legítimo perseguido por un responsable o un tercero, a menos que dicho interés no prevalezca sobre los intereses del interesado o sus derechos y libertades fundamentales [artículo 6, apartado 1, letra f)]. Los intereses legítimos perseguidos por un responsable del tratamiento o un tercero pueden ser de carácter jurídico[8], económico o moral.[9] No obstante, el responsable del tratamiento debe tener en cuenta que si el interesado se opone a la vigilancia de conformidad con el artículo 21, solo podrá proceder con la videovigilancia de ese interesado si tiene un interés legítimo *imperioso* que prevalece sobre los

[6] Las normas para reunir pruebas dirigidas a las demandas civiles varían entre los Estados miembros.

[7] Las presentes directrices no analizan ni detallan las legislaciones nacionales que pueden diferir de un Estado miembro a otro.

[8] Tribunal de Justicia Europeo, asunto C-13/16, *Rīgas satiksme*, 4 de mayo de 2017

[9] Véase WP217, Grupo de Trabajo del Artículo 29.

intereses, derechos y libertades del interesado o para establecer, ejercer o defender demandas judiciales.

19. En una situación real de peligro, la finalidad de proteger la propiedad frente a robos, hurtos o vandalismo puede constituir un interés legítimo para la videovigilancia.

20. El interés legítimo debe existir realmente y ser una cuestión actual (es decir, no debe ser ficticio ni especulativo)[10]. Debe existir una situación de peligro real, como daños o incidentes graves en el pasado, para poder iniciar la vigilancia. A la luz del principio de rendición de cuentas, a los responsables les convendría documentar los incidentes pertinentes (fecha, forma, pérdida económica) y los cargos penales relacionados. Estos incidentes documentados pueden ser una prueba sólida de la existencia de un interés legítimo. La existencia de un interés legítimo y la necesidad de vigilancia se deben evaluar a intervalos periódicos (por ejemplo, una vez al año, en función de las circunstancias).

> Ejemplo: El propietario de una tienda desea abrir una nueva tienda e instalar un sistema de videovigilancia para evitar el vandalismo. Puede demostrar, presentando estadísticas, que existe una elevada posibilidad de vandalismo en el vecindario. También resultaría útil la experiencia de las tiendas vecinas. No es necesario que se produzca un daño para el responsable del tratamiento en cuestión, siempre y cuando los daños en el vecindario sugieran un peligro o similar, y por tanto puedan ser un indicio de un interés legítimo. No obstante, no es suficiente con presentar estadísticas delictivas nacionales o generales sin analizar la zona en cuestión o los peligros para esta tienda en concreto.

21.

22. Las situaciones de peligro inminente pueden constituir un interés legítimo, como los bancos o las tiendas que venden artículos de valor (p. ej., joyerías), o las zonas que se conocen como escenarios delictivos típicos de delitos contra la propiedad (p. ej., gasolineras).

23. El RGPD también deja claro que los poderes públicos no pueden basar su tratamiento en motivos de interés legítimo cuando desempeñan sus funciones (artículo 6, apartado 1, segunda frase).

3.1.2 Necesidad del tratamiento

24. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); véase el artículo 5, apartado 1, letra c). Antes de instalar un sistema de videovigilancia, el responsable del tratamiento debe examinar siempre de forma crítica si dicha medida es en primer lugar adecuada para lograr el objetivo deseado y, en segundo lugar, si es adecuada y necesaria para su fin. Solo se debe optar por las medidas de videovigilancia si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios que sean menos intrusivos para los derechos y libertades fundamentales del interesado.

25. En una situación en la que el responsable del tratamiento desea evitar que se produzcan delitos relacionados con la propiedad, en lugar de instalar un sistema de videovigilancia, también podría adoptar medidas de seguridad alternativas como vallar la propiedad, establecer patrullas periódicas de personal de seguridad, emplear vigilantes de seguridad, ofrecer una mejor iluminación, instalar cerraduras de seguridad, ventanas y puertas estancas o selladas, o aplicar revestimientos o capas antigrafiti en las paredes. Estas medidas pueden ser tan efectivas como los sistemas de videovigilancia

[10] Véase WP217, Grupo de Trabajo del Artículo 29., p. 24 y ss. Véase también TJE, asunto C-708/18, p. 44.

contra los robos, los hurtos y el vandalismo. El responsable debe evaluar caso por caso si dichas medidas pueden ser una solución razonable.

26. Antes de utilizar un sistema de cámaras, el responsable está obligado a evaluar si las medidas de videovigilancia son estrictamente necesarias y cuándo lo son. Normalmente, un sistema de vigilancia que funcione por la noche y fuera del horario laboral normal cubrirá las necesidades del responsable de evitar peligros en su propiedad.

27. Por lo general, la necesidad de utilizar la videovigilancia para proteger las instalaciones de los responsables termina en los límites de la propiedad.[11] No obstante, hay casos en los que la vigilancia de la propiedad no es suficiente para lograr una protección efectiva. En algunos casos concretos, puede resultar necesario extender la videovigilancia a las inmediaciones de las instalaciones. En este contexto, el responsable debe tener en cuenta los medios físicos y técnicos, por ejemplo, bloquear o pixelar las zonas no pertinentes.

> Ejemplo: Una librería desea proteger sus instalaciones frente al vandalismo. En general, las cámaras solo deberían grabar las propias instalaciones, puesto que no es necesario observar las instalaciones vecinas o las zonas públicas de las proximidades de la librería para tal fin.

28.

29. Las cuestiones relativas a la necesidad del tratamiento también surgen respecto a la forma en que se conservan las pruebas. En algunos casos puede resultar necesario utilizar soluciones de tipo «caja negra» cuando las imágenes se eliminan automáticamente después de un determinado período de almacenamiento y utilizarse únicamente en caso de producirse incidentes. En otras situaciones, puede no ser necesario registrar el material de vídeo, sino utilizar vigilancia en tiempo real en su lugar. La decisión entre optar por soluciones de tipo caja negra o la vigilancia en tiempo real también se debe basar en el fin perseguido. Si, por ejemplo, la finalidad de la videovigilancia es conservar pruebas, normalmente los métodos en tiempo real no son adecuados. En algunas ocasiones la vigilancia en tiempo real puede también ser más intrusiva que conservar y suprimir automáticamente el material, transcurrido un intervalo de tiempo determinado (p. ej., si alguien está viendo continuamente el monitor, puede ser más intrusivo que si no hay ningún monitor y el material se conserva directamente en una caja negra). El principio de la minimización de datos debe tenerse en cuenta en este contexto ([artículo 5, apartado 1, letra c)]. También debe tenerse en cuenta que existe la posibilidad de que el responsable utilice personal de seguridad en lugar de videovigilancia que pueda reaccionar e intervenir inmediatamente.

3.1.3 Equilibrio de intereses

30. Suponiendo que la videovigilancia sea necesaria para proteger los intereses legítimos de un responsable, un sistema de videovigilancia solo podrá emplearse si los intereses legítimos del responsable o los de un tercero (p. ej., protección de la propiedad o de la integridad física) prevalecen sobre los intereses o los derechos y las libertades fundamentales del interesado. El responsable debe considerar: 1) hasta qué punto la vigilancia afecta a los intereses y los derechos y libertades fundamentales de las personas, y 2) si ello causa infracciones o tiene consecuencias negativas respecto a los derechos del interesado. En realidad, equilibrar los intereses es obligatorio. Los derechos y libertades fundamentales por un lado, y el interés legítimo del responsable por otro, deben evaluarse y equilibrarse minuciosamente.

[11] Esto también puede estar sujeto a la legislación nacional en algunos Estados miembros.

Ejemplo: Una empresa de aparcamiento privado ha documentado problemas recurrentes por robos en los vehículos aparcados. La zona de aparcamiento es un espacio abierto al que cualquier persona puede acceder fácilmente, pero está claramente señalizado y tiene bloqueadores de acceso alrededor de dicho espacio. La empresa de aparcamiento tiene un interés legítimo (evitar los robos en los vehículos de los clientes) para vigilar la zona durante las horas en las que tienen problemas. Los interesados están vigilados durante un período limitado, no se encuentran en la zona por motivos recreativos y también redunda en su propio interés evitar los robos. El interés de los interesados en no ser vigilados no prevalece en este caso sobre el interés legítimo del responsable.

Ejemplo: Un restaurante decide instalar cámaras de vídeo en los aseos para controlar la limpieza de las instalaciones sanitarias. En este caso, los derechos de los interesados prevalecen claramente sobre el interés del responsable, por lo que no se pueden instalar cámaras en ese lugar.

31.

3.1.3.1 Adoptar decisiones caso por caso

32. Dado que el equilibrio de intereses es obligatorio de conformidad con el Reglamento, la decisión debe adoptarse caso por caso [véase el artículo 6, apartado 1, letra f)]. Hacer referencia a situaciones abstractas o comparar casos similares entre sí no es suficiente. El responsable debe evaluar los riesgos de intrusión en los derechos del interesado; en este caso el criterio decisivo es la intensidad de la intervención para los derechos y libertades del particular.

33. La intensidad se puede definir entre otros aspectos por el tipo de información que se recopila (contenido de la información), el ámbito de aplicación (densidad de la información, dimensión espacial y geográfica), el número de interesados afectados, ya sea como un número específico o en proporción a la población pertinente, la situación en cuestión, los intereses reales del grupo de interesados, los medios alternativos o la naturaleza y alcance de la evaluación de datos.

34. Factores de equilibrio importantes pueden ser el tamaño de la zona objeto de vigilancia o la cantidad de interesados que se encuentran bajo vigilancia. La utilización de la videovigilancia en una zona remota (p. ej., para observar la fauna o proteger infraestructuras críticas como una antena de radio privada) debe evaluarse de forma diferente que la videovigilancia en una zona peatonal o un centro comercial.

Ejemplo: Si se instala una cámara de salpicadero (p. ej., para reunir pruebas en caso de accidente), es importante garantizar que la cámara no esté grabando el tráfico continuamente, como tampoco las personas que están cerca de una carretera. De lo contrario, el interés de contar con grabaciones de vídeo como prueba en el caso más teórico de un accidente vial no puede justificar esta grave injerencia en los derechos de los interesados.[11]

35.

3.1.3.2 Expectativas razonables de los interesados

36. De conformidad con el considerando 47, la existencia de un interés legítimo necesita una evaluación detenida. En este caso, deberán incluirse las expectativas razonables del interesado en el momento y en el contexto del tratamiento de sus datos personales. En relación con la vigilancia sistemática, la relación entre el interesado y el responsable puede variar significativamente y puede afectar a las expectativas razonables que pueda tener el interesado. La interpretación del concepto de expectativas razonables no solo debe basarse en las expectativas subjetivas en cuestión. En lugar de ello, el criterio

decisivo debe ser si un tercero objetivo podría razonablemente esperar y determinar que está sujeto a vigilancia en esta situación específica.

37. Por ejemplo, un empleado en su lugar de trabajo en la mayoría de los casos probablemente no espera ser vigilado por su empleador.[12] Tampoco se espera la vigilancia en el jardín privado, en áreas comunes ni en salas de examen o tratamiento. En la misma línea, no es razonable esperar la vigilancia en instalaciones sanitarias o saunas; la vigilancia en esas zonas representa una intrusión intensa en los derechos de los interesados. Las expectativas razonables de los interesados son que no haya videovigilancia en esas zonas. Por otro lado, el cliente de un banco puede esperar que sea vigilado en el interior de un banco o en el cajero.

38. Los interesados también pueden esperar no estar sujetos a vigilancia en áreas de acceso público, especialmente si las mismas se utilizan normalmente para actividades de recuperación, regeneración y ocio, como tampoco en lugares en los que las personas permanecen o se comunican, como áreas de descanso, mesas de restaurantes, parques, cines o gimnasios. En este caso, los intereses o derechos y libertades del interesado a menudo prevalecerán sobre los intereses legítimos del responsable.

> Ejemplo: Los interesados esperan que no se les vigile en los aseos. La videovigilancia para evitar accidentes, por ejemplo, no es proporcional.

39.

40. Las señales que informan al interesado acerca de la videovigilancia no tienen relevancia a la hora de determinar lo que puede esperar objetivamente un interesado. Esto significa, por ejemplo, que el propietario de una tienda no se puede basar en que los clientes tengan *objetivamente* expectativas razonables de ser vigilados simplemente porque una señal les informa en la entrada acerca de la vigilancia.

3.2 Necesidad de cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento [artículo 6, apartado 1, letra e)]

41. Los datos personales se pueden tratar con videovigilancia con arreglo al artículo 6, apartado 1, letra e) si resulta necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos.[13] Es posible que el ejercicio del poder público no permita dicho tratamiento, pero otras bases legislativas como la «salud y seguridad» para la protección de los visitantes y empleados puede ofrecer un alcance limitado para el tratamiento, al tiempo que respeta las obligaciones del RGPD y los derechos del interesado.

42. Los Estados miembros pueden mantener o incorporar leyes nacionales específicas para la videovigilancia con el fin de adaptar la aplicación de las normas del RGPD determinando requisitos específicos de forma más precisa para el tratamiento siempre que cumplan los principios establecidos en el RGPD (p. ej., limitación del almacenamiento, proporcionalidad).

---

[12] Véase también: Grupo de Trabajo del Artículo 29, Dictamen 2/2017 sobre el tratamiento de datos personales en el trabajo, WP 249, adoptado el 8 de junio de 2017.

[13] La base para el tratamiento mencionado debe establecerse por el Derecho de la Unión o el Derecho del Estado miembro y debe ser «necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento» (artículo 6, apartado 3).

3.3 Consentimiento [artículo 6, apartado 1, letra a)]

43. El consentimiento debe darse libremente y de forma específica, informada, e inequívoca como se describe en las directrices sobre el consentimiento.[14]

44. En relación con la vigilancia sistemática, el consentimiento del interesado solo puede servir de base jurídica de conformidad con el artículo 7 (véase el considerando 43) en casos excepcionales. El hecho de que esta tecnología vigila a una cantidad desconocida de personas a la vez reside en la propia naturaleza de la vigilancia. Difícilmente el responsable podrá demostrar que el interesado ha dado su consentimiento antes del tratamiento de sus datos personales (artículo 7, apartado 1). Suponiendo que el interesado retire su consentimiento será difícil para el responsable demostrar que los datos personales ya no se tratan (artículo 7, apartado 3).

> Ejemplo: Los atletas pueden solicitar la vigilancia durante los ejercicios individuales con el fin de analizar sus técnicas y su rendimiento. Por otro lado, cuando un club deportivo toma la iniciativa de vigilar a todo un equipo con la misma finalidad, el consentimiento a menudo no será válido, ya que cada atleta puede sentirse presionado para dar su consentimiento de forma que su negativa a darlo no tenga efectos desfavorables en sus compañeros de equipo.

45.

46. Si el responsable desea basarse en el consentimiento, es su obligación asegurarse de que cada interesado que entre en la zona objeto de videovigilancia haya dado su consentimiento. Dicho consentimiento debe cumplir las condiciones del artículo 7. El entrar en una zona vigilada señalizada (p. ej., cuando se invita a las personas a pasar por una entrada o puerta específicas para entrar en una zona vigilada), no constituye una declaración ni una clara acción afirmativa necesarias para el consentimiento, a menos que satisfaga los criterios de los artículos 4 y 7 tal y como se describe en las directrices sobre el consentimiento.[15]

47. Dado el desequilibrio de poder entre los empleados y los empleadores, en la mayoría de los casos estos últimos no deben basarse en el consentimiento al tratar datos personales, ya que difícilmente se dará libremente. Las directrices sobre el consentimiento deben tomarse en consideración en este contexto.

48. La legislación de los Estados miembros o los convenios colectivos, incluidos los «acuerdos de empresa», pueden estipular normas específicas sobre el tratamiento de los datos personales de los empleados en el contexto laboral (véase el artículo 88).

[14] Grupo de Trabajo del Artículo 29 (art. 29 WP) «Directrices sobre el consentimiento con arreglo al Reglamento 2016/679» (WP 259 rev. 01). - aprobado por el CEPD

[15] Grupo de Trabajo del Artículo 29 (art. 29 WP) «Directrices sobre el consentimiento con arreglo al Reglamento 2016/679» (WP 259), aprobado por el CEPD, que debe tenerse en cuenta.

4 DIVULGACIÓN DE IMÁGENES DE VÍDEO A TERCEROS

49. En principio, las normas generales del RGPD se aplican a la divulgación de grabaciones de vídeo a terceros.

4.1 Divulgación de imágenes de vídeo a terceros en general

50. La divulgación se define en el artículo 4, apartado 2, como la transmisión (p. ej., la comunicación individual), la difusión (p. ej., la publicación en línea) o la puesta a disposición de cualquier otra forma. Los terceros se definen en el artículo 4, apartado 10. Cuando la divulgación se realiza a terceros países o a organizaciones internacionales, también se aplican las disposiciones especiales del artículo 44 y ss.

51. Cualquier comunicación de datos personales es un tipo distinto de tratamiento de datos personales para el que el responsable debe tener una base jurídica en el artículo 6.

> Ejemplo: Un responsable que desea cargar una grabación en internet debe fundamentarse en una base jurídica para dicho tratamiento, por ejemplo, mediante la obtención del consentimiento del interesado con arreglo al artículo 6, apartado 1, letra a).

52.

53. La transmisión de imágenes de vídeo a terceros con fines distintos de aquellos para los que se han obtenido los datos es posible en virtud de las reglas del artículo 6, apartado 4.

> Ejemplo: La videovigilancia de una barrera (en un aparcamiento) se instala con la finalidad de resolver daños. Si se produce un daño, la grabación se transmite a un abogado para entablar una acción. En este caso, la finalidad de la grabación es la misma que la de la transmisión.
>
> Ejemplo: La videovigilancia de una barrera (en un aparcamiento) se instala con la finalidad de resolver daños. La grabación se publica en línea puramente por motivos de diversión. En este caso, la finalidad ha cambiado y no es compatible con la finalidad inicial. Además sería problemático identificar una base jurídica para dicho tratamiento (publicación).

54.

55. Un tercer destinatario tendría que realizar su propio análisis jurídico, en particular identificando su base jurídica con arreglo al artículo 6 para su tratamiento (p, ej., recibir el material).

4.2 Divulgación de imágenes de vídeo a las autoridades competentes

56. La divulgación de grabaciones de vídeo a las autoridades competentes es también un proceso independiente que exige una justificación distinta para el responsable.

57. De conformidad con el artículo 6, apartado 1, letra c), el tratamiento es lícito si es necesario para cumplir una obligación legal a la que está sujeto el responsable del tratamiento. Aunque la legislación policial aplicable es un asunto que corresponde exclusivamente a los Estados miembros, existen con toda probabilidad reglas generales que rigen la transferencia de pruebas a las autoridades competentes de cada Estado miembro. El tratamiento del responsable que entrega los datos está regulado por el RGPD. Si la legislación nacional exige que el responsable del tratamiento coopere con la aplicación de la ley (p. ej., una investigación), la base jurídica para transmitir los datos es la obligación legal con arreglo al artículo 6, apartado 1, letra c).

58. La limitación de la finalidad del artículo 6, apartado 4, normalmente no es problemática, puesto que la divulgación corresponde explícitamente a la legislación del Estado miembro. Por consiguiente, no es necesario tomar en consideración los requisitos especiales del cambio de finalidad en el sentido de las letras a) a e).

> Ejemplo: El propietario de una tienda graba imágenes en su entrada. Las imágenes muestran a una persona que roba la cartera a otra. La policía solicita al responsable del tratamiento que entregue el material para ayudar en la investigación. En ese caso, el propietario de la tienda utilizará la base jurídica del artículo 6, apartado 1, letra c) (obligación legal) en combinación con la legislación nacional pertinente para la transmisión del tratamiento.

59.

> Ejemplo: Una cámara se instala en una tienda por motivos de seguridad. El propietario de la tienda considera que ha grabado algo sospechoso y decide enviar el material a la policía (sin indicar que hay una investigación en curso de algún tipo). En este caso, el propietario de la tienda debe evaluar si se cumplen las condiciones, en la mayoría de los casos, del artículo 6, apartado 1, letra f). Esto se da normalmente cuando el propietario de la tienda sospecha razonablemente que se ha cometido un delito.

60.

61. El tratamiento de los datos personales por las propias autoridades competentes no cumple el RGPD [véase el artículo 2, apartado 2, letra d)], pero sí la Directiva sobre protección de datos (UE) 2016/680.

5 TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS

62. Los sistemas de videovigilancia normalmente recopilan cantidades masivas de datos personales que pueden revelar datos de naturaleza muy personal e incluso categorías especiales de datos. En efecto, los datos aparentemente no significativos recogidos en un principio mediante el vídeo se pueden usar para inferir otra información dirigida a lograr una finalidad diferente (p. ej., realizar un seguimiento de los hábitos de una persona). Sin embargo, la videovigilancia no se considera siempre como un tratamiento de categorías especiales de datos personales.

> Ejemplo: Las imágenes de vídeo que muestran a un interesado que lleva gafas o que utiliza una silla de ruedas no se consideran por sí mismas una categoría especial de datos personales.

63.

64. No obstante, si las imágenes de vídeo se tratan para inferir categorías especiales de datos, es de aplicación el artículo 9.

> Ejemplo: Se podrían deducir opiniones políticas, por ejemplo, de imágenes que mostraran a interesados identificables participando en un evento, iniciando una huelga, etc. Esto estaría dentro del ámbito de aplicación del artículo 9.
>
> Ejemplo: Un hospital que instala una cámara de vídeo con el fin de vigilar el estado de salud de un paciente podría considerarse como un tratamiento de categorías especiales de datos personales (artículo 9).

65.

66. En general, por principio, cuando se instala un sistema de videovigilancia debe prestarse especial atención al principio de minimización de datos. Por lo tanto, aun en los casos en los que no se aplica el artículo 9, apartado 1, el responsable del tratamiento debe procurar siempre minimizar el riesgo de capturar imágenes que revelen otros datos sensibles (además del artículo 9), independientemente del objetivo.

> Ejemplo: La videovigilancia que captura una iglesia no pertenece en sí al ámbito de aplicación del artículo 9. Sin embargo, el responsable del tratamiento debe realizar una evaluación especialmente cuidadosa con arreglo al artículo 6, apartado 1, letra f) y tener en cuenta la naturaleza de los datos, así como el riesgo de capturar otros datos sensibles (además del artículo 9) cuando evalúe los intereses del interesado.

67.

68. Si se utiliza un sistema de videovigilancia con el fin de tratar categorías especiales de datos, el responsable del tratamiento debe identificar tanto una excepción para el tratamiento de categorías especiales de datos en virtud del artículo 9 (esto es, una excepción a la regla general según la cual no se deben tratar categorías especiales de datos) como una base jurídica con arreglo al artículo 6.

69. Por ejemplo, el artículo 9, apartado 2, letra c) («[…] *el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física* […]») podría utilizarse, en teoría y de forma excepcional, pero el responsable del tratamiento tendría que justificarlo como una necesidad absoluta de proteger los intereses vitales de una persona y demostrar que «[…] el interesado *no esté capacitado, física o jurídicamente, para dar su consentimiento*». El responsable del tratamiento tampoco estará autorizado a usar el sistema con ningún otro motivo.

70. Es importante señalar que no es probable que cada excepción enumerada en el artículo 9 pueda utilizarse para justificar el tratamiento de categorías especiales de datos mediante la videovigilancia. De manera más específica, los responsables que traten esos datos en el contexto de la videovigilancia no se pueden basar en el artículo 9, apartado 2, letra e), que permite el tratamiento relativo a datos personales que el interesado ha hecho manifiestamente públicos. El mero hecho de entrar en el alcance de la cámara no implica que el interesado pretenda hacer públicas categorías especiales de datos relacionadas con su persona.

71. Además, el tratamiento de categorías especiales de datos exige una mayor y continua vigilancia de determinadas obligaciones, por ejemplo, un elevado nivel de seguridad y una evaluación de impacto de la protección de datos cuando sea necesario.

> Ejemplo: Un empleador no debe utilizar grabaciones de videovigilancia que muestren una manifestación para identificar a los huelguistas.

72.

5.1 Consideraciones generales para el tratamiento de datos biométricos

73. El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento.

74. Para considerarse datos biométricos en el sentido del RGPD, el tratamiento de datos sin procesar, como las características físicas, fisiológicas o conductuales de una persona física deben implicar una medición de dichas características. Dado que los datos biométricos son el resultado de tales mediciones, el RGPD indica en su artículo 4, apartado 14, que son datos personales «*[…] obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona […]».* Las imágenes de vídeo de una persona física no pueden sin embargo considerarse en sí mismas datos biométricos con arreglo al artículo 9, si no se han tratado técnicamente de forma específica para contribuir a la identificación de la persona. [16]

75. Con el fin de que pueda considerarse como tratamiento de categorías especiales de datos personales (artículo 9) exige que los datos biométricos se traten para «identificar de manera unívoca a una persona física».

76. En resumen, a la luz de los artículos 4, apartado 14, y 9, deben tenerse en cuenta tres criterios:

- **la naturaleza de los datos:** datos relativos a las características físicas, fisiológicas o conductuales de una persona física;

[16] El considerando 51 del RGPD respalda este análisis al declarar que «*[…] El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. […]*».

- **los medios y las formas de tratamiento**: datos «obtenidos a partir de un tratamiento técnico específico»;
- **la finalidad del tratamiento:** los datos se deben utilizar para la finalidad de identificar de manera unívoca a una persona física.

77. La utilización de la videovigilancia, incluida la función de reconocimiento biométrico instalada por entidades privadas para sus propios fines (p. ej., mercadotecnia, estadísticas o incluso seguridad), requerirá en la mayoría de los casos el consentimiento explícito de todos los interesados [artículo 9, apartado 2, letra a)]; no obstante, también podría aplicarse otra excepción adecuada del artículo 9.

> Ejemplo: Para mejorar su servicio, una empresa privada sustituye los puntos de control de identificación de los pasajeros en un aeropuerto (despacho de equipajes, embarque) por sistemas de videovigilancia que usan técnicas de reconocimiento facial para comprobar la identidad de los pasajeros que han optado por consentir dicho procedimiento. Puesto que el tratamiento pertenece al ámbito de aplicación del artículo 9, los pasajeros, quienes habrán dado previamente su consentimiento explícito e informado, tendrán que incluirse en una lista en un terminal automático, por ejemplo, para poder crear y registrar su plantilla facial asociada a su identidad y su tarjeta de embarque. Los puntos de control con reconocimiento facial deben estar claramente separados, es decir, el sistema se debe instalar en un pórtico para que no se capturen las plantillas biométricas de las personas que no han dado su consentimiento. Únicamente los pasajeros que hayan dado su consentimiento previamente y procedido a su registro usarán el pórtico equipado con el sistema biométrico.
>
> Ejemplo: Un responsable del tratamiento gestiona el acceso a su edificio mediante un método de reconocimiento facial. Las personas solo pueden utilizar esta forma de acceso si han dado su consentimiento informado explícitamente [de conformidad con el artículo 9, apartado 2, letra a)] de antemano. No obstante, con el fin de garantizar que no se capture a ninguna persona que no haya dado previamente su consentimiento, el método de reconocimiento facial debe activarse por el propio interesado, por ejemplo, pulsando un botón. Para garantizar la legitimidad del tratamiento, el responsable siempre debe ofrecer una forma alternativa de acceder al edificio, sin tratamiento biométrico, como insignias o llaves.

78.

79. En este tipo de casos, cuando se generan las plantillas biométricas, los responsables del tratamiento deben garantizar que, una vez se haya obtenido un resultado coincidente o no, todas las plantillas intermedias realizadas sobre la marcha (con el consentimiento explícito e informado del interesado) para poder compararse con las creadas por los interesados en el momento del registro, se eliminen de forma inmediata y segura. Las plantillas creadas para la inclusión en la lista deben conservarse únicamente para cumplir la finalidad del tratamiento y no deben conservarse ni archivarse.

80. No obstante, cuando la finalidad del tratamiento sea por ejemplo distinguir a una categoría de personas de otra pero no identificar de forma unívoca a una persona, el tratamiento no está incluido en el artículo 9.

Ejemplo: El propietario de una tienda desea personalizar su publicidad en función de las características de sexo y edad del cliente capturado por un sistema de videovigilancia. Si el sistema no genera plantillas biométricas para identificar a las personas de forma unívoca sino que tan solo detecta esas características físicas para clasificar a la persona, el tratamiento no pertenece al ámbito de aplicación del artículo 9 (siempre y cuando no se traten otros tipos de categorías especiales de datos).

81.

82. Sin embargo, el artículo 9 se aplica si el responsable del tratamiento conserva datos biométricos (normalmente a través de plantillas creadas mediante la extracción de características clave del formato sin procesar de los datos biométricos, p. ej., mediciones faciales de una imagen) con el fin de identificar de forma unívoca a una persona. Si un responsable del tratamiento desea detectar a un interesado que vuelve a entrar en la zona o que entra en otra (por ejemplo, para proyectar una publicidad personalizada continua), la finalidad en tal caso sería identificar de forma unívoca a una persona física, lo que significa que la operación estaría comprendida desde el principio en el artículo 9. Este sería el caso si un responsable del tratamiento conserva las plantillas generadas para proporcionar más publicidad adaptada en varios tablones de diferentes ubicaciones dentro de la tienda. Dado que el sistema utiliza características físicas para detectar a personas específicas que vuelven dentro del alcance de la cámara (como los visitantes de un centro comercial) y realizar un seguimiento de los mismos, constituiría un método de identificación biométrica, porque pretende el reconocimiento con el uso de un tratamiento técnico específico.

Ejemplo: El propietario de una tienda ha instalado un sistema de reconocimiento facial en su tienda para personalizar su publicidad a las personas. El responsable del tratamiento debe obtener el consentimiento explícito e informado de todos los interesados para poder utilizar este sistema biométrico y ofrecer una publicidad adaptada. El sistema sería ilícito si capturara a visitantes o transeúntes que no hubieran consentido la creación de su plantilla biométrica, aunque su plantilla se elimine en el período más corto posible. De hecho, estas plantillas temporales constituyen datos biométricos tratados con el fin de identificar de forma unívoca a una persona que no desea recibir publicidad personalizada.

83.

84. El CEPD señala que algunos sistemas biométricos están instalados en entornos no controlados[17], lo que significa que el sistema captura sobre la marcha los rostros de cualquier persona que entre dentro del alcance de la cámara, incluidas las personas que no han dado su consentimiento al dispositivo biométrico, con lo que se crean plantillas biométricas. Estas plantillas se comparan con las creadas de los interesados que han dado previamente su consentimiento durante un proceso de inclusión en lista (el usuario de un dispositivo biométrico) a fin de que el responsable del tratamiento reconozca si la persona es o no un usuario del dispositivo. En este caso, el sistema a menudo está diseñado para distinguir a las personas que desea reconocer de una base de datos de aquellas que no están en la lista. Dado que el objetivo es identificar de forma unívoca a las personas físicas, se sigue necesitando una excepción del artículo 9, apartado 2, del RGPD para cualquier persona capturada por la cámara.

[17] Significa que el dispositivo biométrico está situado en un espacio abierto al público y puede funcionar con cualquiera que pase, por oposición a los sistemas biométricos de entornos controlados que se pueden utilizar únicamente consintiendo la participación de la persona.

Ejemplo: Un hotel utiliza videovigilancia para avisar automáticamente al director del hotel de que ha llegado un VIP cuando reconoce el rostro del huésped. Estas personas VIP tienen prioridad dado su consentimiento explícito a la utilización del reconocimiento facial antes de ser registradas en una base de datos creada al efecto. Estos sistemas de procesamiento de datos biométricos serían ilícitos a menos que todos los demás huéspedes vigilados (para identificar a los VIP) hubieran dado su consentimiento al tratamiento de conformidad con el artículo 9, apartado 2, letra a), del RGPD.

Ejemplo: Un responsable del tratamiento instala un sistema de videovigilancia con reconocimiento facial en la entrada de la sala de conciertos que dirige. El responsable debe configurar entradas claramente separadas: una con un sistema biométrico y otra sin él (donde en su lugar por ejemplo se escanea un ticket). Las entradas equipadas con dispositivos biométricos deben instalarse y ser accesibles de forma que el sistema no pueda capturar plantillas biométricas de los espectadores que no han dado su consentimiento.

85.

86. Por último, cuando el artículo 9 del RGPD exige el consentimiento, el responsable del tratamiento no puede supeditar el acceso a sus servicios a la aceptación del tratamiento biométrico. En otras palabras, y especialmente cuando el tratamiento biométrico se utiliza con fines de autenticación, el responsable del tratamiento debe ofrecer una solución alternativa que no implique el tratamiento biométrico, sin restricciones ni coste adicional para el interesado. Esta solución alternativa también se necesita para las personas que no cumplen las limitaciones del dispositivo biométrico (imposibilidad de registro o lectura de los datos biométricos, situación de incapacidad que dificulta el uso, etc.) y como anticipación a la falta de disponibilidad del dispositivo biométrico (como una avería del dispositivo), se debe instalar una «solución de copia de seguridad» para garantizar la continuidad del servicio prestado, limitado no obstante al uso excepcional. En casos excepcionales, puede existir una situación en la que el tratamiento de los datos biométricos sea la actividad principal de un servicio ofrecido por contrato, por ejemplo, un museo que celebra una exposición para demostrar el uso de un dispositivo de reconocimiento facial, en cuyo caso el interesado no podrá rechazar el tratamiento de los datos biométricos en caso de que deseen participar en la exposición. En tal caso, el consentimiento exigido con arreglo al artículo 9 sigue siendo válido si se cumplen los requisitos del artículo 7.

5.2 Medidas sugeridas para minimizar los riesgos al tratar datos biométricos

87. De conformidad con el principio de minimización de datos, los responsables del tratamiento deben garantizar que los datos extraídos de una imagen digital para crear una plantilla no serán excesivos y solo contendrán la información necesaria para el fin específico, evitando así cualquier otro posible tratamiento. Se deben aplicar medidas para garantizar que las plantillas no se puedan transferir a través de los sistemas biométricos.

88. Es probable que la identificación y la autenticación/comprobación requieran el almacenamiento de la plantilla para su uso en una comparación posterior. El responsable del tratamiento debe tener en cuenta la ubicación más adecuada para el almacenamiento de los datos. En un entorno controlado (entradas o puntos de control delimitados), las plantillas se conservarán en un dispositivo individual guardado por el usuario y bajo el control exclusivo de este (en un smartphone o tarjeta identificativa) o bien, cuando sea necesario con fines específicos y en presencia de necesidades objetivas, se conservarán en una base de datos centralizada de forma cifrada con una clave/número secreto en posesión exclusivamente de la persona para evitar el acceso no autorizado a la plantilla o al lugar de almacenamiento. Si el responsable del tratamiento no puede evitar tener acceso a las plantillas, deberá

adoptar las medidas adecuadas para garantizar la seguridad de los datos almacenados. Esto puede incluir el cifrado de la plantilla mediante algoritmos criptográficos.

89. En cualquier caso, el responsable deberá tomar todas las precauciones necesarias para preservar la disponibilidad, integridad y confidencialidad de los datos tratados. Para ello, el responsable del tratamiento deberá en especial adoptar las siguientes medidas: separar los datos durante la transmisión y el almacenamiento, conservar las plantillas biométricas y los datos sin procesar o los datos identificativos en bases de datos distintas, cifrar los datos biométricos, concretamente las plantillas biométricas y definir una política para el cifrado y la gestión de claves, integrar una medida organizativa y técnica para la detección de fraudes, asociar un código de integridad a los datos (por ejemplo, mediante firma o huella digital) y prohibir cualquier acceso externo a los datos biométricos. Estas medidas deberán evolucionar con el progreso de las tecnologías.

90. Los responsables del tratamiento deberán además proceder a suprimir los datos sin procesar (imágenes faciales, señales de voz, la marcha, etc.) y garantizar la eficacia de dicha eliminación. Si ya no existe una base legítima para el tratamiento, los datos no procesados deberán suprimirse. De hecho, en la medida en que las plantillas biométricas se deriven de dichos datos, se puede considerar que la creación de bases de datos podría representar una amenaza similar si no mayor (pues es posible que no siempre se pueda leer una plantilla biométrica sin saber cómo se programó, mientras que los datos sin procesar serán los componentes fundamentales de cualquier plantilla). En caso de que el responsable del tratamiento necesite conservar los datos, se deberán analizar métodos de ruido aditivo (como el marcado con filigrana), que haría ineficaz la creación de la plantilla. El responsable debe también suprimir los datos y las plantillas biométricos en caso de acceso no autorizado al terminal de comparación de lectura o servidor de almacenamiento y eliminar cualquier dato que no sea útil para proseguir el tratamiento al final de la vida del dispositivo biométrico.

6 DERECHOS DEL INTERESADO

91. Debido al carácter del tratamiento de datos al usar la videovigilancia, algunos derechos del interesado con arreglo al RGPD sirven para mayor aclaración. El presente capítulo no es exhaustivo y todos los derechos con arreglo al RGPD se aplican al tratamiento de datos personales con videovigilancia.

6.1 Derecho de acceso

92. El interesado tiene derecho a obtener la confirmación del responsable del tratamiento respecto a si sus datos personales son o no objeto de tratamiento. Para la videovigilancia, esto significa que si no se conserva ni transfiere ningún dato de ninguna forma, una vez transcurrido el momento de la vigilancia en tiempo real, el responsable solo podría dar la información de que ya no se trata ningún dato personal (aparte de las obligaciones de información general estipuladas en el artículo 13; véase el apartado *7, Obligaciones de transparencia e información*). Si, no obstante, los datos se siguen tratando en el momento de la solicitud (esto es, si los datos se conservan o tratan continuamente de cualquier otra forma), el interesado debe obtener acceso e información de conformidad con el artículo 15.

93. Existen no obstante varias limitaciones que pueden aplicarse en algunos casos en relación con el derecho de acceso.

- Artículo 15, apartado 4 del RGPD: afectar negativamente a los derechos de otros

94. Dado que es posible grabar a cualquier número de interesados en la misma secuencia de videovigilancia, un filtrado causaría el tratamiento adicional de datos personales de otros interesados. Si el interesado desea recibir una copia del material (artículo 15, apartado 3), esto afectaría negativamente a los derechos y libertades de otros interesados sobre el material. Para evitar este efecto, el responsable del tratamiento debe por tanto tener en cuenta que debido a la naturaleza intrusiva de las imágenes de vídeo, no debe en determinados casos entregar las imágenes de vídeo cuando se pueda identificar a otros interesados. No obstante, la protección de los derechos de terceros no se puede utilizar como excusa para evitar las reivindicaciones legítimas de acceso de las personas; el responsable del tratamiento debe en estos casos aplicar medidas técnicas para cumplir la solicitud de acceso (por ejemplo, editando las imágenes con enmascaramiento o codificación). Sin embargo, los responsables no están obligados a aplicar tales medidas técnicas si pueden garantizar de otro modo que pueden responder a una solicitud con arreglo al artículo 15 en el plazo estipulado en el artículo 12, apartado 3.

- Artículo 11, apartado 2 del RGPD: el responsable del tratamiento no puede identificar al interesado

95. Si no es posible buscar datos personales en las imágenes de vídeo (esto es, el responsable probablemente tendría que revisar una gran cantidad de material conservado para encontrar al interesado en cuestión), es posible que el responsable no pueda identificar al interesado.

96. Por estos motivos, el interesado debería especificar (además de identificarse a sí mismo, incluido el documento de identidad o personalmente) en su solicitud al responsable cuándo entró en la zona vigilada (en un plazo razonable en proporción a la cantidad de interesados grabados). El responsable del tratamiento debe notificar al interesado previamente qué información necesita para dar respuesta a la solicitud. Si el responsable del tratamiento puede demostrar que no está en condiciones de identificar al interesado, deberá informar de ello al interesado en consecuencia, si fuera posible. En tal situación, en su respuesta al interesado, el responsable debe informar sobre

la zona exacta de vigilancia, la comprobación de las cámaras que se estaban usando, etc. para que el interesado entienda perfectamente qué datos personales suyos se pueden haber tratado.

Ejemplo: Si un interesado solicita una copia de sus datos personales tratados con videovigilancia en la entrada de un centro comercial con 30 000 visitantes al día, debe especificar cuándo pasó por la zona vigilada en un plazo de aproximadamente una hora. Si el responsable sigue tratando el material, debe facilitar una copia de las imágenes de vídeo. Si se puede identificar a otros interesados en el mismo material, esa parte del material debe permanecer en el anonimato (por ejemplo, difuminando la copia o partes de la misma) antes de entregar la copia al interesado que presentó la solicitud.

Ejemplo: Si el responsable del tratamiento suprime automáticamente todas las imágenes por ejemplo en un plazo de dos días, no puede facilitar las imágenes al interesado transcurridos esos dos días. Si el responsable recibe una solicitud después de esos dos días, se debe informar al interesado en consecuencia.

97.

- Artículo 12 del RGPD: solicitudes excesivas

98. Cuando las solicitudes de un interesado sean manifiestamente infundadas o excesivas, el responsable del tratamiento podrá cobrar un canon razonable de conformidad con el artículo 12, apartado 5, letra a) del RGPD o bien negarse a actuar respecto de la solicitud [artículo 12, apartado 5, letra b) del RGPD]. El responsable del tratamiento debe poder demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6.2 Derecho de supresión y de oposición

6.2.1 Derecho de supresión (derecho al olvido)

99. Si el responsable del tratamiento continúa tratando datos personales más allá de la vigilancia en tiempo real (p. ej., almacenamiento) el interesado puede solicitar que se supriman los datos personales con arreglo al artículo 17 del RGPD.

100. Cuando así se le solicite, el responsable estará obligado a suprimir los datos personales sin dilación indebida si se aplica cualquiera de las circunstancias enumeradas en el artículo 17, apartado 1, del RGPD (y ninguna de las excepciones enumeradas en el artículo 17, apartado 3, del RGPD). Esto incluye la obligación de suprimir los datos personales cuando ya no se necesiten para la finalidad para la que se conservaron inicialmente o cuando el tratamiento sea ilícito (véase también el apartado 8, *Plazo de conservación y obligación de supresión*). Asimismo, en función de la base jurídica del tratamiento, los datos personales deberán suprimirse:

- *por el consentimiento* cuando este se retire (y no exista ninguna otra base jurídica para el tratamiento)
- por *interés legítimo*
    - cuando el interesado ejerza el derecho de oposición (véase el apartado 6.2.2) y no existan motivos legítimos imperiosos que prevalezcan para el tratamiento, o
    - en caso de mercadotecnia directa (incluida la elaboración de perfiles) cuando el interesado se oponga al tratamiento.

101. Si el responsable del tratamiento ha hecho públicas las imágenes de vídeo (p. ej., por difusión o en línea), deben adoptarse medidas razonables para informar a otros responsables del tratamiento (que ahora tratan los datos personales en cuestión) de la solicitud de conformidad con el artículo 17, apartado 2, del RGPD. Las medidas razonables deberán incluir medidas técnicas y tener en cuenta la tecnología disponible y el coste de la aplicación. En la medida de lo posible, el responsable del tratamiento deberá notificarlo, en el momento de la supresión de los datos personales, a cualquier persona a la que se hayan comunicado previamente los datos personales, de conformidad con el artículo 19 del RGPD.

102. Además de la obligación del responsable del tratamiento de suprimir los datos personales previa solicitud del interesado, el responsable estará obligado con arreglo a los principios generales del RGPD a limitar los datos personales conservados (véase el apartado 8).

103. Respecto a la videovigilancia merece la pena observar que, por ejemplo, al difuminar la imagen sin la posibilidad retroactiva de recuperar los datos personales que contenía la imagen previamente, los datos personales se considerarán suprimidos de conformidad con el RGPD.

> Ejemplo: Una tienda tiene problemas con el vandalismo, en particular en su exterior y, por tanto, utiliza videovigilancia fuera de su entrada, en conexión directa con las paredes. Un transeúnte solicita que se supriman sus datos personales a partir de ese momento. El responsable del tratamiento está obligado a responder a la solicitud sin dilación indebida y como máximo en el plazo de un mes. Puesto que las imágenes en cuestión ya no cumplen la finalidad para la que se conservaron inicialmente (no se ha producido vandalismo durante el período en el que pasaba el interesado), en el momento de la solicitud no existe interés legítimo para conservar los datos que prevalezca sobre los intereses de los interesados. El responsable del tratamiento debe suprimir los datos personales.

104.

6.2.2 Derecho de oposición

105. Respecto a la videovigilancia basada en un *interés legítimo* [artículo 6, apartado 1, letra f) del RGPD] o a la necesidad cuando se realiza una tarea en *interés público* [artículo 6, apartado 1, letra e) del RGPD] el interesado tiene derecho en cualquier momento a oponerse, por motivos relacionados con su situación particular, al tratamiento de conformidad con el artículo 21 del RGPD. A menos que el responsable del tratamiento acredite motivos legítimos imperiosos que prevalezcan sobre los derechos e intereses del interesado, deberá detenerse el tratamiento de los datos de la persona que se opuso. El responsable del tratamiento estará obligado a responder al interesado sin dilación indebida y como máximo en el plazo de un mes.

106. En el contexto de la videovigilancia, esta oposición se puede realizar al entrar en la zona vigilada, durante el tiempo en la misma o después de salir de ella. En la práctica esto significa que a menos que el responsable del tratamiento tenga motivos legítimos imperiosos, la vigilancia en una zona en la que se pueda identificar a las personas físicas solo es legítima si

(1) el responsable del tratamiento puede detener inmediatamente el tratamiento de datos personales de la cámara cuando se solicite, o

(2) la zona vigilada está tan restringida que el responsable puede garantizar la aprobación del interesado antes de entrar en la zona y no es una zona a la que el interesado tiene derecho a acceder como ciudadano.

107. Estas directrices no pretenden identificar lo que se considera un interés legítimo *imperioso* (artículo 21 del RGPD).

108. Cuando se utilice la videovigilancia con fines de mercadotecnia directa, el interesado tendrá derecho a oponerse al tratamiento de forma discrecional, ya que el derecho de oposición es absoluto en ese contexto (artículo 21, apartados 2 y 3 del RGPD).

> Ejemplo: Una empresa tiene dificultades con las infracciones de seguridad en su entrada pública y utiliza la videovigilancia por motivos de interés legítimo, con la finalidad de capturar a los que entran ilícitamente. Un visitante se opone al tratamiento de sus datos personales con el sistema de videovigilancia por motivos relacionados con su situación particular. No obstante, la empresa en este caso rechaza la solicitud explicando que las imágenes conservadas se necesitan debido a una investigación interna en curso, con lo que tiene motivos legítimos imperiosos para seguir tratando los datos personales.

109.

7 OBLIGACIONES DE TRANSPARENCIA E INFORMACIÓN[18]

110. Desde hace mucho tiempo es inherente a la legislación europea sobre protección de datos que los interesados deben ser conscientes del hecho de que la videovigilancia está en funcionamiento. Se les debe informar de forma detallada sobre los lugares vigilados.[19] Con arreglo al RGPD, las obligaciones generales de transparencia e información se recogen en el artículo 12 y siguientes del RGPD. Las «Directrices sobre transparencia con arreglo al Reglamento 2016/679 (WP260)» del Grupo de Trabajo del Artículo 29 que aprobó el CEPD el 25 de mayo de 2018 ofrecen más información. En línea con el WP260, apartado 26, es el artículo 13 del RGPD el que es de aplicación si se recogen datos personales «[…] de un interesado por observación (p. ej., empleando dispositivos de captura de datos automatizados o software de captura de datos como las cámaras […]».

111. Debido al volumen de información que es preciso facilitar al interesado, es posible que los responsables del tratamiento adopten un enfoque de varios niveles y opten por utilizar una combinación de métodos para garantizar la transparencia (WP260, apartado 35; WP89, apartado 22). Respecto a la videovigilancia, la información más importante debe mostrarse en la propia señal de advertencia (primer nivel) mientras que los demás datos obligatorios pueden facilitarse por otros medios (segundo nivel).

7.1 Información de primer nivel (señal de advertencia)

112. El primer nivel afecta a la forma principal en que el responsable del tratamiento interactúa en primer lugar con el interesado. En esta fase, los responsables pueden utilizar una señal de advertencia que muestre la información pertinente. La información mostrada puede proporcionarse en combinación con un icono que ofrezca, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto (artículo 12, apartado 7 del RGPD). El formato de la información deberá ajustarse a cada ubicación (WP89 apartado 22).

7.1.1 Colocación de la señal de advertencia

113. La información debe colocarse de forma que el interesado pueda reconocer fácilmente las circunstancias de la vigilancia antes de entrar en la zona vigilada (aproximadamente a la altura de los ojos). No es necesario revelar la posición de la cámara siempre y cuando no haya dudas respecto a las zonas sujetas a vigilancia y el contexto de esta quede claro de forma inequívoca (WP 89, apartado 22). El interesado debe poder estimar qué zona se captura por una cámara de forma que pueda evitar la vigilancia o adaptar su comportamiento si fuera necesario.

7.1.2 Contenido del primer nivel

114. La información de primer nivel (señal de advertencia) debe por lo general transmitir la información más importante, p. ej., los datos de la finalidad del tratamiento, la identidad del responsable del tratamiento y la existencia de los derechos del interesado, junto con información sobre los mayores efectos del tratamiento.[20] Esto puede incluir por ejemplo los intereses legítimos perseguidos por el responsable del tratamiento (o por un tercero) y los datos de contacto del delegado de protección de

[18] Pueden aplicarse requisitos específicos en la legislación nacional.

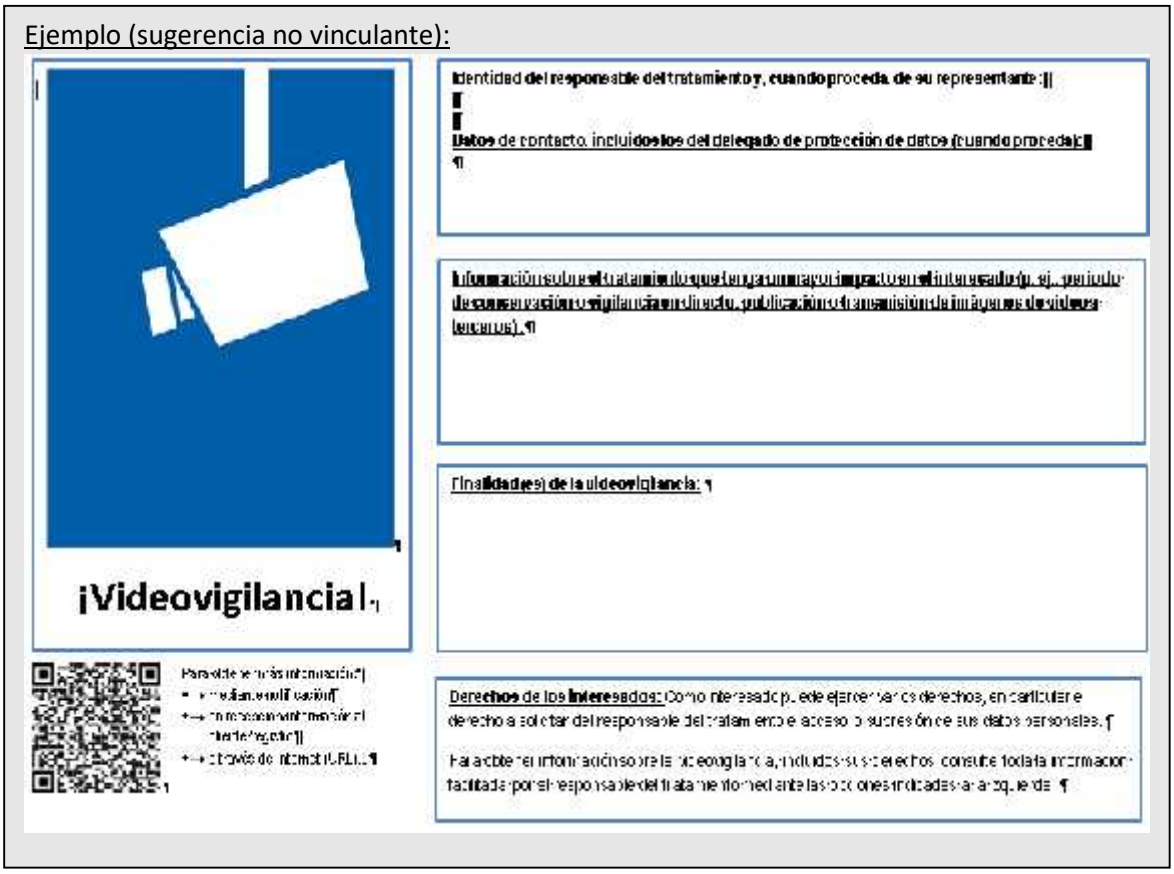
[19] Véase el WP89, dictamen 4/2004, relativo al tratamiento de datos personales mediante el sistema de vigilancia por videocámara del Grupo de Trabajo del Artículo 29.

[20] Véase WP260, apartado 38.

datos (en su caso). También debe hacer referencia al segundo nivel más detallado de información así como a dónde y cómo encontrarla.

115. La señal debe además contener cualquier información que pueda sorprender al interesado (WP260, apartado 38). Podrían ser, por ejemplo, transmisiones a terceros, especialmente si se encuentran fuera de la UE, y el período de conservación. Si no se indica esta información, el interesado debe poder confiar en que solo hay una vigilancia en directo (sin grabación de datos ni transmisión a terceros).

116. Ejemplo (sugerencia no vinculante):



7.2 Información de segundo nivel

117. La información de segundo nivel también debe facilitarse en un lugar al que el interesado pueda acceder fácilmente, por ejemplo, una hoja informativa completa disponible en una ubicación central (p. ej., mostrador de información, recepción o caja) o mostrarse en un cartel de fácil acceso. Como ya se ha indicado, la señal de advertencia de primer nivel debe referirse claramente a la información de segundo nivel. Asimismo, es mejor si la información de primer nivel hace referencia a una fuente digital (p. ej., código QR o dirección de un sitio web) del segundo nivel. No obstante, la información también debe estar disponible fácilmente en formato no digital. Debe ser posible acceder a la información de segundo nivel sin entrar en la zona vigilada, especialmente si la información se facilita digitalmente (esto puede conseguirse por ejemplo mediante un enlace). Otros medios adecuados podrían ser un número de teléfono al que se pueda llamar. Aunque se facilite la información, esta debe contener todos los elementos obligatorios con arreglo al artículo 13 del RGPD.

118. Además de estas opciones, y para que sean aún más eficaces, el CEPD fomenta el uso de medios tecnológicos para facilitar información a los interesados. Esto puede incluir, por ejemplo, cámaras de localización geográfica e información en aplicaciones o sitios web de cartografía de forma que las personas puedan fácilmente, por un lado, identificar y especificar las fuentes de vídeo relativas al ejercicio de sus derechos y, por otro lado, obtener información más detallada sobre el funcionamiento del tratamiento.

> Ejemplo: El propietario de una tienda vigila su tienda. Para cumplir con el artículo 13, basta con colocar una señal de advertencia en un punto fácilmente visible de la entrada de la tienda, que contenga la información de primer nivel. Además, debe facilitar una hoja informativa que incluya la información de segundo nivel en la caja o en cualquier otro lugar central y de fácil acceso en la tienda.

119.

8 PERÍODOS DE CONSERVACIÓN Y OBLIGACIÓN DE SUPRESIÓN

120. Los datos personales no podrán conservarse durante más tiempo del necesario para la finalidad para la que se tratan [artículo 5, apartado 1, letras c) y e) del RGPD]. En algunos Estados miembros, puede haber disposiciones específicas para los períodos de conservación respecto a la videovigilancia de conformidad con el artículo 6, apartado 2, del RGPD.

121. El hecho de si es necesario conservar o no los datos personales debe controlarse en un corto espacio de tiempo. Por lo general, los fines legítimos de la videovigilancia son normalmente la protección de la propiedad o la conservación de pruebas. Normalmente los daños producidos se pueden reconocer un uno o dos días. Para facilitar la demostración del cumplimiento del marco de protección de datos, va en interés del responsable del tratamiento celebrar acuerdos organizativos por adelantado (p. ej., nombrar, si fuera necesario, a un representante para examinar y asegurar el material de vídeo). Teniendo en cuenta los principios del artículo 5, apartado 1, letras c) y e) del RGPD, concretamente la minimización de datos y la limitación del plazo de conservación, los datos personales deberán suprimirse en la mayoría de los casos (p. ej., a efectos de detectar vandalismo), preferentemente de forma automática, transcurridos unos días. Cuanto más tiempo dure el período de conservación (especialmente cuando supere las 72 horas), más argumentos deberán facilitarse para la legitimidad de la finalidad y la necesidad de conservación. Si el responsable del tratamiento utiliza la videovigilancia no solo para controlar sus instalaciones sino también para conservar los datos, deberá garantizar que la conservación es efectivamente necesaria para lograr la finalidad. Si es así, el plazo de conservación deberá definirse claramente y fijarse individualmente para cada fin particular. Es responsabilidad del responsable del tratamiento definir el período de conservación de conformidad con los principios de necesidad y proporcionalidad y acreditar el cumplimiento de las disposiciones del RGPD.

> Ejemplo: El propietario de una tienda pequeña normalmente se daría cuenta de cualquier signo de vandalismo el mismo día. En consecuencia, bastaría con un período normal de conservación de 24 horas. Los fines de semana que está cerrada o las vacaciones más prolongadas pueden no obstante ser motivos para un período de conservación más largo. Si se detecta un daño también puede ser necesario conservar las imágenes de vídeo durante un período más prolongado con el fin de interponer demandas contra el infractor.

122.

9 MEDIDAS TÉCNICAS Y ORGANIZATIVAS

123. Tal y como se estipula en el artículo 32, apartado 1, del RGPD, el tratamiento de datos personales durante la videovigilancia no solo debe estar legalmente autorizado sino que los responsables y los encargados del tratamiento también deben garantizar la seguridad debidamente. Las **medidas técnicas y organizativas** aplicadas deben ser **proporcionales a los riesgos para los derechos y libertades de las personas físicas**, como resultado de la destrucción accidental o ilícita, la pérdida, alteración, divulgación no autorizada o acceso a los datos de videovigilancia. De conformidad con los artículos 24 y 25 del RGPD, los responsables del tratamiento también deben aplicar medidas técnicas y organizativas para proteger todos los principios de la protección de datos durante el tratamiento y establecer medios para que los interesados puedan ejercer sus derechos como se define en los artículos 15 a 22 del RGPD. Los responsables del tratamiento de datos deben adoptar marcos y políticas internos que garanticen esta aplicación tanto en el momento de determinar los medios para el

tratamiento como en el momento del propio tratamiento, incluidos los resultados de las evaluaciones de impacto de la protección de datos cuando sea necesario.

9.1 Descripción general del sistema de videovigilancia

124. Un sistema de videovigilancia (VSS, por sus siglas en inglés)[21] consiste en dispositivos analógicos y digitales y en software con el fin de capturar imágenes de un escenario, tratar las imágenes y mostrarlas a un operador. Sus componentes se agrupan en las siguientes categorías:

- Entorno de vídeo: captura de imagen, interconexiones y gestión de imágenes:
  - el objetivo de la captura de imágenes es generar una imagen del mundo real en un formato que pueda utilizar el resto del sistema,
  - las interconexiones describen todas las transmisiones de datos en el entorno de vídeo, como las conexiones y las comunicaciones. Ejemplos de conexiones son los cables, las redes digitales y las transmisiones inalámbricas. Las comunicaciones describen todas las señales de datos de vídeo y control, que pueden ser digitales o analógicas,
  - la gestión de imágenes incluye el análisis, conservación y presentación de una imagen o una serie de imágenes.
- Desde el punto de vista de la gestión del sistema, un VSS presenta las siguientes funciones lógicas:
  - gestión de datos y gestión de actividad, que incluye comandos de operador de tratamiento y actividades generadas por el sistema (procedimientos de alarma, alerta a los operadores),
  - las interfaces a otros sistemas pueden incluir la conexión a otros sistemas de seguridad (control de acceso, alarma contra incendios) y no de seguridad (sistemas de gestión de edificios, reconocimiento automático de matrículas).
- La seguridad de un VSS consiste en la confidencialidad, la integridad y la disponibilidad del sistema y los datos:
  - la seguridad del sistema incluye la seguridad física de todos los componentes del sistema y el control de acceso al VSS,
  - la seguridad de los datos incluye la prevención de pérdidas o manipulaciones de los datos.

[21] El RGPD no ofrece una definición para ello; se puede por ejemplo encontrar una descripción técnica en EN 62676-1-1:2014 Sistemas de videovigilancia para utilización en aplicaciones de seguridad – Parte 1-1: Requisitos del sistema.

125.

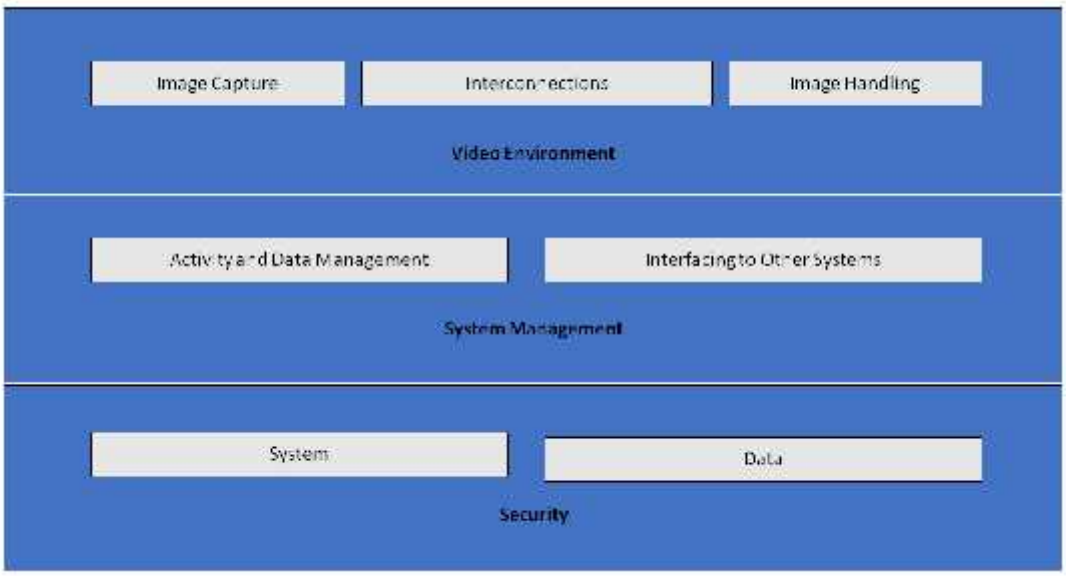


Image Capture	Captura de imágenes
Interconnections	Interconexiones
Image Handling	Gestión de imágenes
Video Environment	Entorno de vídeo
Activity and Data Management	Gestión de la actividad y los datos
Interfacing to Other Systems	Interfaces con otros sistemas
System Management	Gestión del sistema
System	Sistema
Data	Datos
Security	Seguridad

Figura 1: sistema de videovigilancia

9.2 Protección de los datos desde el diseño y por defecto

126. Tal y como se establece en el artículo 25 del RGPD, los responsables del tratamiento deben aplicar medidas técnicas y organizativas adecuadas de protección de datos tan pronto como prevean la videovigilancia y antes de empezar a recoger y tratar las imágenes de vídeo. Estos principios destacan la necesidad de contar con tecnologías integradas de mejora de la privacidad, ajustes por defecto que minimicen el tratamiento de los datos y el suministro de las herramientas necesarias para permitir el mayor grado de protección posible de los datos personales[22].

127. Los responsables del tratamiento deben integrar la protección de datos y de la privacidad no solo en las especificaciones de diseño de la tecnología sino también en las prácticas organizativas. En lo que respecta a las prácticas organizativas, el responsable del tratamiento debe adoptar un marco de gestión adecuado, y establecer y aplicar políticas y procedimientos relativos a la videovigilancia. Desde el punto de vista técnico, las especificaciones del sistema y el diseño deben incluir requisitos para el tratamiento de los datos personales de conformidad con los principios establecidos en el artículo 5 del

[22] WP 168, Dictamen sobre «El futuro de la vida privada», contribución conjunta del Grupo de trabajo sobre protección de datos del artículo 29 y del Grupo «Policía y Justicia» a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental de protección de datos personales (adoptado el 1 de diciembre de 2009).

RGPD (licitud del tratamiento, finalidad y limitación de los datos, minimización de datos por defecto en el sentido del artículo 25, apartado 2, del RGPD, integridad y confidencialidad, responsabilidad, etc.). En caso de que un responsable del tratamiento tenga previsto adquirir un sistema de videovigilancia comercial, deberá incluir estos requisitos en las especificaciones de compra. El responsable del tratamiento debe garantizar el cumplimiento de estos requisitos y aplicarlos a todos los componentes del sistema y a todos los datos que trate, durante todo el ciclo de vida.

9.3 Ejemplos concretos de medidas pertinentes

128. La mayor parte de las medidas que se pueden utilizar para asegurar la videovigilancia, especialmente cuando se usan equipos digitales y software, no difieren de las utilizadas en otros sistemas informáticos. No obstante, independientemente de la solución seleccionada, el responsable del tratamiento debe proteger adecuadamente todos los componentes de un sistema de videovigilancia y los datos en todas las fases, es decir, durante la conservación (datos en reposo), la transmisión (datos en tránsito) y el tratamiento (datos en uso). Para ello, es necesario que los responsables y los encargados del tratamiento combinen medidas técnicas y organizativas.

129. Al seleccionar las soluciones técnicas, el responsable del tratamiento debe tener en cuenta también las tecnologías que protegen la privacidad porque aumentan la seguridad. Ejemplos de estas tecnologías son los sistemas que permiten el enmascaramiento o la codificación de zonas que no son relevantes para la vigilancia, o la edición de imágenes de terceros, al proporcionar imágenes de vídeo a los interesados.[23] Por otro lado, las soluciones seleccionadas no deben ofrecer funciones que no sean necesarias (p. ej., movimiento ilimitado de las cámaras, capacidad de zoom, transmisión por radio, análisis y grabaciones de audio). Las funciones proporcionadas que no sean necesarias se deben desactivar.

130. Hay mucha documentación disponible sobre este tema, incluidas especificaciones técnicas y normas internacionales sobre la seguridad física de los sistemas multimedia[24] y la seguridad de los sistemas informáticos en general[25]. Por lo tanto, este apartado ofrece únicamente un resumen de alto nivel de este tema.

9.3.1 Medidas organizativas

131. Además de la posible necesidad de una evaluación del impacto sobre la protección de datos (EIPD) (véase el apartado 10), los responsables del tratamiento deben tener en cuenta los siguientes aspectos al crear sus propios procedimientos y políticas de videovigilancia:

- Persona responsable de la gestión y el funcionamiento del sistema de videovigilancia.
- Objetivo y ámbito de aplicación del proyecto de videovigilancia.
- Uso adecuado y prohibido (dónde y cuándo está permitida la videovigilancia y dónde y cuándo no lo está; p. ej., utilización de cámaras y audio ocultos además de la grabación con vídeo)[26].

[23] La utilización de estas tecnologías puede incluso ser obligatoria en algunos casos con el fin de cumplir el artículo 5, apartado 1, letra c). En cualquier caso, pueden servir de ejemplos de buenas prácticas.

[24] IEC TS 62045 — Seguridad multimedia - Guía para la protección de la privacidad de equipos y sistemas de entrada y salidas de uso.

[25] ISO/IEC 27000 — Serie de sistemas de gestión de seguridad de la información.

[26] Esto dependerá de la legislación nacional y la normativa del sector.

- Las medidas de transparencia a las que se refiere el apartado 7 *(Obligaciones de transparencia e información).*
- Cómo se graba el vídeo y durante cuánto tiempo, incluido el almacenamiento de las grabaciones de vídeo relativas a incidencias de seguridad.
- Quién debe recibir la formación pertinente y cuándo.
- Quién tiene acceso a las grabaciones de vídeo y con qué finalidades.
- Procedimientos operativos (p. ej., por quién y desde dónde se supervisa la videovigilancia, qué hacer en caso de violación de la seguridad de los datos).
- Qué procedimientos deben seguir los terceros externos para solicitar grabaciones de vídeo y procedimientos para denegar u otorgar tales solicitudes.
- Procedimientos para el suministro, instalación y mantenimiento de VSS.
- Procedimientos de recuperación y gestión de incidentes.

9.3.2 Medidas técnicas

132. **Seguridad del sistema** significa **seguridad física** de todos los componentes del sistema y la integridad del sistema, esto es, **la protección y resiliencia en condiciones de injerencia intencionada e involuntaria en sus operaciones normales** y el **control de acceso**. Seguridad de los datos significa **confidencialidad** (solo pueden acceder a los datos las personas a las que se haya concedido acceso), **integridad** (prevención frente a la pérdida de datos o la manipulación) y **disponibilidad** (se puede acceder a los datos cuando sea necesario).

133. La **seguridad física** es una parte vital de la protección de datos y la primera línea de defensa, dado que protege a los equipos de VSS frente al robo, el vandalismo, los desastres naturales, las catástrofes ocasionadas por el hombre y los daños accidentales (p. ej., por sobrecargas eléctricas, temperaturas extremas o café vertido). En el caso de los sistemas analógicos, la seguridad física desempeña un papel principal en su protección.

134. **La seguridad de los datos y sistemas**, es decir, la protección frente a las injerencias intencionadas e involuntarias en sus operaciones normales, puede incluir:

- Protección de toda la infraestructura del VSS (incluidas cámaras remotas, cableado y fuente de alimentación) frente al robo y la manipulación física.
- Protección de la transmisión de imágenes con canales de comunicación contra las intercepciones.
- Cifrado de datos.
- La utilización de soluciones basadas en hardware y software como cortafuegos, antivirus o sistemas de detección de intrusos contra ciberataques.
- Detección de fallos de componentes, software e interconexiones.
- Medios para restaurar la disponibilidad y el acceso al sistema en caso de incidente físico o técnico.

135. El **control de acceso** garantiza que solo las personas autorizadas puedan acceder al sistema y los datos, mientras que otras no puedan hacerlo. Las medidas que respaldan el control de acceso físico y lógico son las siguientes:

- Garantizar que todas las instalaciones en las que exista videovigilancia y en las que se conserven imágenes de vídeo estén protegidas frente al acceso no supervisado de terceros.
- Colocar los monitores (especialmente cuando estén en espacios abiertos, como una recepción) de forma que solo los operadores autorizados puedan verlos.
- Definir y aplicar procedimientos para conceder, cambiar y revocar el acceso físico y lógico.

- Aplicar métodos y medios de autenticación y autorización, incluidos por ejemplo la longitud y la frecuencia de cambio de las contraseñas.
- Registrar y revisar periódicamente las acciones realizadas por el usuario (tanto en el sistema como en los datos).
- Realizar continuamente la vigilancia y detección de fallos de acceso y tratar lo antes posible las deficiencias identificadas.

10 EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

136. De conformidad con el artículo 35, apartado 1, del RGPD, los responsables del tratamiento deben realizar evaluaciones de impacto relativas a la protección de datos (EIPD) cuando un tipo de tratamiento de datos pueda tener como resultado un elevado riesgo para los derechos y libertades de las personas físicas. El artículo 35, apartado 3, letra c), del RGPD estipula que los responsables del tratamiento deberán llevar a cabo evaluaciones de impacto de la protección de datos si el tratamiento constituye una observación sistemática a gran escala de una zona de acceso público. Asimismo, con arreglo al artículo 35, apartado 3, letra b), del RGPD, también se requerirá la evaluación de impacto relativa a la protección de datos cuando el responsable del tratamiento pretenda tratar categorías especiales de datos a gran escala.

137. Las Directrices sobre la evaluación de impacto relativa a la protección de datos[27] ofrecen asesoramiento adicional y ejemplos más detallados relativos a la videovigilancia (p. ej., en relación con el «uso de un sistema de cámaras para supervisar el comportamiento de conducción en las carreteras»). El artículo 35, apartado 4, del RGPD exige que cada autoridad de control publique una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto en su país. Estas listas se pueden encontrar normalmente en los sitios web de las autoridades. Dadas las finalidades típicas de la videovigilancia (protección de las personas y los bienes, detección, prevención y control de delitos, obtención de pruebas e identificación biométrica de sospechosos), es razonable suponer que muchos casos de videovigilancia requerirán una EIPD. Por consiguiente, los responsables del tratamiento de datos deben consultar detenidamente estos documentos para determinar si se requiere dicha evaluación y llevarla a cabo si fuera necesario. El resultado de la EIPD realizada deberá determinar la elección del responsable del tratamiento de las medidas de protección de datos aplicadas.

138. También es importante observar que si los resultados de la EIPD indican que del tratamiento se derivaría un alto riesgo a pesar de las medidas de seguridad previstas por el responsable del tratamiento, será necesario consultar a la autoridad de control pertinente antes de llevar a cabo el tratamiento. Se puede encontrar más información sobre las consultas previas en el artículo 36.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)

[27] WP248 rev.01, Directrices sobre la evaluación de impacto relativa a la protección de datos y determinación de si el tratamiento «puede dar lugar a un alto riesgo» a efectos del Reglamento 2016/679. - aprobado por el CEPD