

## ASPECTOS REGULATORIO/LEGALES DE LA VISIÓN ARTIFICIAL

La VA permite realizar automáticamente numerosos casos de uso de interés para el negocio a través de:

- **Reconocimiento facial:** localizar caras en una imagen y reconocerlas (identificando o no a la persona). Sin averiguar la identidad de una persona, se puede saber que la persona de la imagen está en otra imagen. En todo caso, únicamente si la persona resulta identificada o identificable se activará el régimen jurídico relativo a la protección de datos personales, con independencia del grado o nivel de sensibilidad de la información personal recabada, puesto que esta no tiene por qué ser catalogada necesariamente como información de carácter biométrico y, por ende, como una categoría especial de datos por relación al artículo 9 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 adelante, Reglamento general de protección de datos o RGPD).
- **Reconocimiento del movimiento y acciones:** localizar personas, animales o cosas en una imagen, reconocer qué movimientos simples realizan (saltar, levantar un brazo) y reconocer qué acciones complejas realizan (abrir una llave de paso, saltar la verja de un jardín). En particular, se pueden detectar comportamientos considerados anómalos: una persona en un lugar prohibido, una persona quieta o tumbada mucho tiempo, etc. Resulta de interés hacer seguimiento de los posibles perfiles o patrones comportamentales que puedan inferirse con apoyo de la VA cuando estos se refieren a personas físicas, debido al especial componente en términos de protección legal a diferente nivel (privacidad, intimidad, discriminación o posibles sesgos asociados, etc.).
- **Identificación de personas:** descubrir la identidad de una persona de diversas formas, como sus rasgos faciales, su forma de caminar, sus huellas dactilares, la ropa que lleva en un momento determinado, etc. Atender a la normativa protectora de datos personales protección resulta relevante en estos casos. En este punto, se deben considerar de forma particular, por ejemplo, las Directrices europeas sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, entre otros documentos y resoluciones de interés a nivel europeo y comparado.
- **Análisis de sentimiento:** inferir el estado de una persona (atenta, enfadada, alegre, despistada) según su mirada y rasgos faciales. A este respecto, la tecnología emocional asociada, por lo general, a técnicas de reconocimiento facial, -aunque no necesariamente-, supone uno de los grandes retos y desafíos jurídicos y éticos en la actualidad, asociándose de forma directa a la nueva corriente a nivel global que aboga por la protección de los neuroderechos, entre otros, la

libertad cognitiva y la privacidad mental. En España, la Carta de Derechos Digitales ya esboza los mismos<sup>1</sup>.

- **Conteo de personas y objetos:** detectar aglomeraciones, contar el número de personas u objetos, contar cuántas veces ha pasado una persona por un punto o área, controlar flujos de personas y objetos, gestionar colas, gestionar zonas de exclusión o puntos calientes, etc. Cuando este tipo de tratamientos sobre imágenes se realiza sin identificación personal, en tiempo real y sin registro alguno de estos datos personales, podría entenderse que no se está produciendo tratamiento de estos.
- **Reconstrucción de escenas,** a partir de imágenes parciales o secuencias de vídeo incompletas, lo que podría llegar a plantear situaciones que pudieran afectar jurídicamente o de forma significativa a las personas (imaginemos la reconstrucción de escenas que pudieran servir de prueba válida en sede judicial).

La Inteligencia Artificial no opera en un mundo sin leyes, como toda solución tecnológica está sujeta a los tratados de la Unión Europea y su Carta de Derechos Fundamentales, así como al Reglamento General de Protección de Datos, pero también a los Tratados de Derechos Humanos de la ONU y los Convenios del Consejo de Europa y regulaciones de los estados miembros.

Tras la publicación el día 2 de diciembre por parte del Gobierno de España de la Estrategia Nacional de Inteligencia Artificial se marca un punto de inflexión en nuestro país que viene precedido de diferentes publicaciones y anuncios por parte de las autoridades europeas y nacionales que a continuación se enumeran en orden cronológico:

- [Estrategia Europea de Inteligencia Artificial](#) (25 abril 2018), además de la [declaración conjunta de cooperación sobre Inteligencia Artificial](#)
- [Plan Coordinado sobre Inteligencia Artificial](#) (diciembre 2018)
- [Estrategia Española de I+D+i en Inteligencia Artificial](#) (marzo 2019)
- [Directrices Éticas para una IA Fiable](#) (abril 2019) y la [guía de definición](#) de las disciplinas asociadas a la Inteligencia Artificial, así como el [mapa de entidades](#) dedicadas a tecnologías relacionadas con la IA.
- Propuesta regulatorias dispuestas por el Parlamento Europeo en torno a la regulación de la IA:
  - <https://www.europarl.europa.eu/news/es/headlines/society/20201015STO89417/regulacion-de-la-inteligencia-artificial-en-la-ue-la-propuesta-del-parlamento>, y

---

<sup>1</sup> Para más información se pueda consultar el siguiente enlace informativo: <https://www.mptfp.gob.es/portal/funcionpublica/secretaria-general-de-funcion-publica/Actualidad/2020/11/2020-11-19.html>

- <https://www.europarl.europa.eu/news/es/press-room/20201016IPR89544/el-parlamento-muestra-el-camino-para-la-normativa-sobre-inteligencia-artificial> (octubre 2020).
- Se crea la **SEDIA** (Secretaría de estado de Digitalización e Inteligencia Artificial) que coordina la estrategia de IA para España.
  - En febrero se publica el **Libro Blanco de IA** y la **Estrategia Europea de Datos**
  - En junio se lanza el proyecto **GAIA-X** y las grandes organizaciones tanto del sector público como privado se suman a él.
  - El Gobierno de España publica la **Carta de Derechos Digitales**, que, sin ser una ley, define las líneas generales de derechos que todos deberíamos tener.
- En respuesta a la Estrategia europea de datos de la Comisión, el Parlamento pidió, en un informe aprobado en la sesión plenaria el 24 de marzo de 2021, una legislación centrada en las personas y basada en los valores europeos sobre privacidad y transparencia. Esta tiene que permitir a las empresas y a la ciudadanía europea beneficiarse del potencial de los datos públicos y a gran escala en la UE.: <https://www.europarl.europa.eu/news/es/headlines/priorities/inteligencia-artificial-en-la-ue/20210218STO98124/estrategia-europea-de-datos-que-quieren-los-eurodiputados>

Por otro lado, el reglamento general de protección de datos se aplica a las imágenes cuando éstas permiten identificar a las personas que aparecen en ellas, incluyendo las que se toman en instalaciones y actividades deportivas. Este reglamento presta especial atención a la protección de los menores y personas vulnerables, así como a la protección de la intimidad, proporcionando a cualquier persona el derecho a la privacidad de sus datos, a disponer de ellos, a conocer quién los posee y con qué finalidad, siendo necesario el consentimiento informado del sujeto afectado o de sus tutores legales para su tratamiento. Todo esto sin perjuicio del derecho a la propia imagen, recogido como un derecho fundamental en el artículo 18.1 de la Constitución Española y desarrollado en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

De lo anterior podemos inferir que este tipo de soluciones pueden conllevar el tratamiento o no de datos personales. Además, es posible que tales soluciones tengan por fin el tratamiento de información personal o que, sin tener como fin principal tal tratamiento, este se produzca si bien de forma colateral o indirecta.

Cuando no se traten datos de carácter personales en el marco de soluciones de VA la normativa de protección de datos personales no será aplicable. Por el contrario, cuando tengan por fin y efecto el tratamiento de estos datos la misma sería aplicable.

En tal sentido, cuando los proyectos o soluciones de VA conlleven el tratamiento de datos personales, es importante considerar, como mínimo, los siguientes extremos, a saber:

- 1. Privacidad y Seguridad desde el diseño y por defecto:** Las soluciones de VA deben diseñarse y desarrollarse siempre bajo parámetros de privacidad y seguridad desde el diseño y por defecto

atendiendo las diversas indicaciones, directrices y recomendaciones emitidas por las autoridades competentes. No atender estos parámetros puede suponer infringir de forma grave la normativa vigente de acuerdo con el artículo 73 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, la LOPDGDD).

El enfoque de privacidad, seguridad y riesgo debe plantearse, además, no sólo en el momento de la génesis o desarrollo inicial del producto o servicio de VA, sino también durante los procesos de mejora o desarrollo evolutivo de tales soluciones. Es interesante atender y adecuarse a certificaciones o estándares internacionalmente reconocidos en este ámbito y, asimismo, acreditar, si quiera mediante etiquetas o sellos privados, en caso de existir, el grado de cumplimiento de dichas soluciones. También es interesante hacerlo desde una perspectiva de negocio y competitividad (privacidad/seguridad competitiva).

Y es que, el Considerando 81 del RGPD dispone de forma clara que para garantizar el cumplimiento de las disposiciones de este Reglamento, el responsable al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. Ofrecer estas garantías de forma proactiva y anticipada a los clientes de soluciones de VA brinda claras ventajas competitivas en el mercado al permitir una mayor confiabilidad y confort legal a los clientes y, en general, a los destinatarios y usuarios finales de estas soluciones.

Por su parte, el Considerando 83 del mismo Reglamento indica que a fin de mantener la seguridad y evitar que el tratamiento infrinja la normativa aplicable, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

Por tanto, tales análisis de riesgo no recaen de forma exclusiva sobre el responsable del tratamiento (por lo general, clientes de soluciones de VA), sino también sobre los prestadores de servicios de VA (de forma habitual, titulares de las soluciones o productos de VA) quienes actúan, por lo general, como meros encargados del tratamiento.

- 2. Proporcionalidad de la solución de VA respecto a los derechos de las personas:** Desde el punto de vista de proyectos específicos, la aplicación de soluciones de VA debe ser acorde y proporcionada a

los fines perseguidos, de forma que si existiera cualquier otra tecnología, medio o solución menos intrusiva para los derechos e intereses de los afectados se deberá priorizar por los clientes estas últimas. Es por ello que, con carácter inicial, es importante valorar o ponderar de forma trazable el grado de proporcionalidad desde la perspectiva de la menor afección posible a tales derechos e intereses. Si como prestadores colaboramos con el cliente en la realización de este análisis según el tipo de proyecto de que se trate ello coadyuvará a que las garantías que ofrezcamos a los clientes sean acordes con lo requerido con la ley, impulsando un mejor cumplimiento de la norma.

- 3. Bases legítimas:** Con carácter adicional a lo anterior, se deben analizar las bases legales que, en cada caso, permiten a una entidad, en su calidad de responsable del tratamiento, aplicar soluciones de VA. Los desarrolladores de estas soluciones no tendrán, con carácter general, esta posición ostentando, en la mayor parte de los casos, el carácter de encargados del tratamiento. Ello no es óbice para informar y recordar proactivamente al cliente, a través de los respectivos contratos que se suscriban, acerca de esta obligación legal de determinación por su parte de las mejores bases legítimas en cada caso.
- 4. VA y reconocimiento facial:** Si la solución supone aplicar técnicas de reconocimiento facial, atender a las diferencias entre los conceptos de identificación y verificación biométrica, aplicando medidas reforzadas en la protección de los derechos de las personas cuando se estén tratando categorías especiales de datos (datos biométricos). Considerar asimismo que, cuando se trata de la imagen de personas, no sólo hay que considerar la protección protectora de datos personales, sino también la normativa protectora del derecho de imagen en tanto derecho fundamental independiente.
- 5. Elementos a considerar en los contratos o condiciones de servicios asociadas a las soluciones de VA:** Se deberá prever de forma transparente y clara:
  - Las funcionalidades y fines que atiende la solución de VA y, por consiguiente, las categorías o tipologías de tratamientos, así como de datos personales que pueden estar afectos en los distintos supuestos, quedando reflejado este aspecto en el sentido dispuesto por el artículo 28 del RGPD.
  - El resto de los elementos o contenidos obligatorios de acuerdo con el artículo 28 del RGPD y la normativa local aplicable concordante.
  - Especial atención a las medidas de seguridad y protección para los derechos e intereses de las personas físicas que pudieran resultar las destinatarias finales de este tipo de tecnologías. Todo ello bajo un enfoque de riesgo y un criterio de mejora continua.
  - Mención específica a certificaciones aplicables o códigos tipo a los que pueda estar adherido la empresa o prestador de soluciones de VA, sobre todo, en el sentido dispuesto por el artículo 32 del RGPD (seguridad e la información personal y poder demostrar cumplimiento en este sentido).
  - Posible reutilización o compartición segura de la información recabada sobre bases legales claras, informando de forma transparente al cliente de soluciones de VA, en su caso. Todo

ello en consonancia con posibles estrategias de Data Sharing al calor de la nueva Estrategia europea de Datos y las posibilidades que esta conlleva para innovar sobre la base de datos. En este punto, será muy importante activar procesos de anonimización de la información personal implicada, mitigando al máximo posibles riesgos legales o éticos en torno al uso indebido de esta información.

Es posible, además, que puedan darse de forma colateral o indirecta tratamientos de datos personales a través de soluciones de VA que no tengan como fin primordial estos. Es decir, aunque no sea el objetivo principal o perseguido de la solución de VA, existe el riesgo de que se produzca la captura de imágenes de forma inintencionada o inadvertida. Esto puede ocurrir bien porque sea inevitable capturar en segundo plano determinadas imágenes de personas, o bien por la captura de otro tipo de información (viviendas próximas, zonas de recreo, vehículos, etc.).

En estos casos, y por analogía con las recomendaciones dispuestas por la Agencia Española de Protección de Datos (AEPD) en el caso de los Drones<sup>2</sup>, muchas de ellas relativas a aspectos de privacidad desde el diseño y por defecto, y otras para atender a los principios esenciales del tratamiento, sería conveniente observar las siguientes recomendaciones:

- Minimizar la presencia de personas y objetos que permitan su identificación (bañistas, matrículas de vehículos, transeúntes, etc.) en el lugar de la operación. Realizando la captación de imágenes en horarios en los que no exista gran afluencia de público o controlando el acceso a la zona de captación de imágenes si fuera posible. En conclusión, minimizar la captura de imágenes a lo absolutamente necesario, reduciendo las posibilidades de que puedan aparecer personas inadvertidamente en las imágenes.
- Promover y aplicar características de privacidad desde el diseño, como, por ejemplo, ajustar la resolución de la imagen al mínimo necesario para ejecutar el propósito del tratamiento, reducir la granularidad de la geolocalización con el mismo propósito; aplicar técnicas para anonimizar imágenes (automáticamente durante la captura o procedimientos para hacerlo inmediatamente después) o mecanismos para iniciar y detener la captura de datos en cualquier momento durante la operación de captación o tratamiento de la imagen de que se trate; implantar protocolos de comunicaciones seguros que impidan a terceros el acceso a las transmisiones de los datos capturados o incluso al control del propio dispositivo o sistema de tratamiento de imágenes, o incluir mecanismos que permitan el cifrado de los datos capturados y almacenados.
- Para lugares en los que inevitablemente habrá personas realizar la captura de imágenes de forma que las personas no puedan ser identificadas, por ejemplo, realizando capturas únicamente a distancia suficiente para que la identificación de estas no sea posible. Cuando

---

<sup>2</sup> Se puede consultar este informe a partir del siguiente enlace web: <https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf>

captas imágenes de personas físicas, pero estas no resultan identificables tampoco sería aplicable la normativa protectora de datos personales.

- Evitar el tratamiento de otro tipo de datos personales como, por ejemplo, la captura indiscriminada de identificadores de dispositivos móviles. No almacenar información innecesaria relativa a personas.

Sin perjuicio de los anteriores problemas, y sin ánimo exhaustivo, asimismo se deben considerar los siguientes aspectos con impacto legal/ético:

- Cómo evitar o reducir al máximo posible el sesgo algorítmico que pueda derivarse de las imágenes tratadas, con el consiguiente riesgo inherente para los derechos básicos de las personas.
- Cómo garantizar la protección de la propiedad intelectual e industrial asociada a las soluciones de VA. También los secretos comerciales vinculados en los términos de la legislación europea y española sobre secretos empresariales.
- Cómo atender la responsabilidad civil derivada de las soluciones de VA.