- **Procedimiento Nº: PS/00120/2021**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

Del procedimiento instruido por la Agencia Española de Protección de Datos y con base en los siguientes

ANTECEDENTES

PRIMERO: Con fecha 5 de mayo de 2021 la directora acordó iniciar procedimiento sancionador a MERCADONA, S.A. (en adelante la parte reclamada). Notificado el acuerdo de inicio y tras analizar las alegaciones presentadas, con fecha 29 de junio de 2021 se emitió la propuesta de resolución que a continuación se transcribe:

<< Procedimiento nº: PS/00120/2021

Del procedimiento instruido por la Agencia Española de Protección de Datos y con base en los siguientes:

ANTECEDENTES

PRIMERO: Con fecha de 6 de julio de 2020 la Directora de la Agencia Española de Protección de Datos (en adelante, AEPD) acuerda iniciar actuaciones de investigación a la vista de las noticias publicadas en medios de comunicación acerca de la implantación que Mercadona, S.A. (en adelante, Mercadona o reclamado) estaría realizando en sus establecimientos de un sistema de detección de aquellas personas con sentencias firmes y órdenes de alejamiento en vigor contra Mercadona o contra alguno de sus trabajadores.

Con posterioridad se registran en la AEPD dos reclamaciones en relación con los mismos hechos:

El día 15 de julio de 2020, número de registro 025103/2020, procedente de la ASOCIACION DE CONSUMIDORES Y USUARIOS EN ACCION-FACUA (NIF G91344986).

El día 27 de julio de 2020, número de registro 026511/2020, procedente de APEDANICA (NIF G80593254).

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante / de los hechos y documentos de los que ha tenido conocimiento esta Agencia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en

adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

Como resultado de las actuaciones de investigación practicadas, se constata que el responsable del tratamiento es el reclamado.

Asimismo, se constatan los siguientes extremos:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han realizado investigaciones a las siguientes entidades:

- Mercadona, S.A., con NIF A46103834 y con domicilio en Paseo de la Castellana n.º 259 C, 28046 Madrid.

La reclamada tiene una cifra de negocios en 2019 de más de 25.000 millones de euros de facturación y más de 94.000 empleados, según consta en el último informe de auditoría emitido por la entidad, por lo que constituye una gran empresa.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

La redacción de estos resultados se apoya en la información facilitada por Mercadona (números de registro de entrada 026455/2020, 026457/2020, 026459/2020, 026460/2020, 026461/2020, 026462/2020, 026463/2020, 026464/2020, y 027549/2020) y en los siguientes documentos incorporados al presente expediente a través de la correspondiente diligencia:

- Referencia número 1: Boletín Oficial del Registro Mercantil (en adelante BORME) de ***FECHA.1, (…).

- Referencia número 2: BORME de ***FECHA.2, (…).

- Referencia número 3: consulta realizada el 5 de noviembre de 2020 de la entidad ***EMPRESA.1** en el servicio de información empresarial Axesor.

- Referencia número 4: informe del gabinete jurídico de la AEPD de número de referencia 010308/2019.

- Referencia número 5: directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 del Grupo de Trabajo sobre protección de datos personales del artículo 29.

- Referencia número 6: extracto de la Ley 5/2014, de 4 de abril, de Seguridad Privada.

- Referencia número 7: extracto de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- Referencia número 8: extracto del Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil.

- Referencia número 9: extracto de la Constitución Española.

- Referencia número 10: informe del gabinete jurídico de la AEPD de número de referencia 36/2020.

- Referencia número 11: dictamen del ICO (*Information Commissioner´s Office*) titulado *"The use of live facial recognition technology by law enforcement in public places",* publicado el 31 de octubre de 2019.

- Referencia número 12: política de privacidad publicada en el sitio de internet de Mercadona cuya última actualización, según cita el propio documento, se produjo con fecha de 5 de octubre de 2020.

Se hace constar que allí donde este informe alude a manifestaciones, descripciones, o exposiciones realizadas por Mercadona *"en su escrito"* esta expresión hace referencia al escrito de entrada registrado el día 25 de julio de 2020 con el número 026455/2020.

Al efecto de conseguir la mayor claridad expositiva posible se ordenan los resultados de la investigación en los siguientes apartados:

1. Contexto y despliegue

2. Intervinientes, destinatarios, y transferencias internacionales de datos

3. Aportación de la imagen al procedimiento judicial e inclusión en el Sistema de Detección Anticipada (en adelante SDA)

4. Activación del SDA, detección, y alerta

5. Recepción y validación de la alerta, y comunicación a las Fuerzas y Cuerpos de Seguridad del Estado (en adelante FCSE)

6. Plazos de conservación de los datos personales

7. Arquitectura del sistema, evaluación de impacto, y medidas de seguridad

8. Finalidad, licitud, y proporcionalidad

9. Cumplimiento del deber de información

1. Contexto y despliegue

Mercadona, según define en su propio escrito, es una *"compañía global que se dedica, entre otras actividades propias de su objeto social, a la explotación de una cadena de supermercados de alimentación"*. Así, según los datos que facilita, dispone de *"1.636 tiendas y aproximadamente 95.000 trabajadores en territorio español".* Añade además que, *"a nivel genérico, podría determinarse que un [sic] el número aproximado de personas que acceden cada día a una tienda MERCADONA es de* ******NÚM.1"***.

Expone igualmente que *"cada año, la Compañía cuenta aproximadamente con* ******NÚM.2*** *procesos judiciales que pueden terminar en más de* ******NÚM.3*** *resoluciones judiciales a su favor en las que se condena en firme al denunciado con órdenes de alejamiento sobre las instalaciones de MERCADONA".* Al respecto cita que son objeto de denuncia y por tanto *"susceptibles de que se solicite una orden de prohibición de acceso a una tienda de la Compañía"* las personas que:

- *"Sean reincidentes en el delito de robo o hurto contra MERCADONA.*

- *Hayan robado una gran cantidad de productos susceptibles de venta*

- *Hayan sido denunciadas y condenadas por delitos relacionados con las instalaciones, bienes o trabajadores de MERCADONA*

- *Amenacen o agredan a los trabajadores propios o vigilantes de seguridad que prestan servicio en las tiendas MERCADONA*

- *Cometan ilícitos sobre los clientes de MERCADONA".*

Al hilo de lo anterior, manifiesta que *"se planteó la implementación de un sistema de detección anticipada utilizando la tecnología de reconocimiento facial en sus tiendas […] motivada por el riesgo derivado de la comisión de hechos delictivos, con su correspondiente riesgo para los clientes y empleados de MERCADONA debido a la gran cantidad de delitos que se comenten en sus más de 1.600 centros distribuidos en toda la geografía española, contra sus empleados o bienes".*

Explica Mercadona que *"un proceso de reconocimiento facial consiste en comparar una muestra biométrica dubitada, obtenida a través de una o varias imágenes de una persona, frente a una base de datos de muestras biométricas ya asociadas de forma indubitada a la identidad de una persona, que han sido*

registradas previamente a través de una o varias fotografías". Para ello, añade, *"las muestras biométricas dubitadas son transformadas en patrones. Posteriormente, a través del reconocimiento facial, las muestras biométricas son comparadas con la plantilla indubitada guardada previamente, a través de cálculos algorítmicos que se evalúan con base en umbrales de coincidencia previamente establecidos".*

Describe Mercadona que el procedimiento consta de las siguientes fases (el documento número 1 del escrito 026457/2020 lista, además de estas fases, las acciones que incluye cada una de ellas):

- Aportación de la imagen al procedimiento judicial.

- Inclusión de la imagen en el SDA.

- Activación del SDA.

- Fase de detección.

- Fase de alerta.

- Recepción y validación de la alerta.

- Comunicación con FCSE.

La información condensada del tratamiento puede consultarse en el extracto del registro de actividades de tratamiento aportado por Mercadona como parte del documento número 29 del escrito 026463/2020 que incluye las actividades de tratamiento de datos que tienen relación con el SDA. Se anticipa la siguiente información del mismo, cuyo detalle se amplía en los siguientes apartados:

- Tratamiento de datos: gestión del sistema de detección anticipada

- Categoría de datos tratados: datos identificativos; imagen; perfil biométrico.

- Categoría de interesados: sujetos que acceden a los centros de Mercadona; sujetos con condena firme.

- Origen del dato:

o Imagen indubitada: a través de la imagen aportada en sentencia firme en la que Mercadona es parte.

o Imagen en tiempo real: captación de los datos a través de las cámaras con sistema de reconocimiento facial de los centros en los que está activo dicho sistema.

- Legitimación:

o Interés público

o Datos sensibles: tratamiento necesario para la formulación, el ejercicio, o la defensa de reclamaciones

- Destinatarios: FCSE; juzgados y tribunales

En cuanto al despliegue del sistema, expone Mercadona *"que el 1 de julio de 2020 se inició el Proyecto piloto del Sistema de Detección Anticipada en* ******NÚM.4*** tiendas*".* Añade, no obstante, que *"el sistema única y exclusivamente se encuentra activo en* ******NÚM.5*** tiendas de ******LOCALIDAD.1****, es decir, en las tiendas que actualmente se ven afectadas por una resolución judicial firme, en la que se decrete como medida una orden de alejamiento, habiendo aportado MERCADONA las correspondientes imágenes en el procedimiento y estableciéndose la posibilidad por el Juzgado, para hacer efectiva la misma, la utilización de medios tecnológicos."*

En relación con el despliegue futuro, Mercadona explica que la finalidad del sistema es proteger la seguridad de los clientes y empleados, *"por lo que el criterio a seguir en el despliegue obedecerá se evaluará [sic] atendiendo a las zonas más vulnerables, en las que pueda existir un mayor riesgo para los clientes o trabajadores de MERCADONA, atendiendo al número de procedimientos judiciales en curso".* Con respecto al número de interesados a incluir en el SDA expone que *"dentro de esas* ******NÚM.3*** *órdenes de alejamiento sobre las instalaciones de MERCADONA se podría estimar el número máximo de interesados incluidos anuales [sic] en el Sistema*". No obstante, matiza que *"estos números son una aproximación y podrán aumentarse o reducirse en función del propio conocimiento de la tecnología por parte de los juzgados o por peticiones que pudiera realizar directamente los FCS"*.

2. Intervinientes, destinatarios y transferencias internacionales de datos

En su escrito Mercadona lista los siguientes intervinientes en el proyecto:

- El Departamento de Seguridad de Mercadona.

En concreto se mencionan los siguientes perfiles:

o ***(…)***

Mercadona informa de que el personal de Mercadona ha suscrito un compromiso de confidencialidad específico relativo a este proyecto (además de los compromisos que firma cualquier trabajador de Mercadona). Así, facilita como documento número 8 del escrito 026464/2020, una copia ejemplo de este compromiso de confidencialidad.

o ***(…)***

o La prestación del servicio implica la realización por ******EMPRESA.2*** de los tratamientos de registro, conservación y supresión de datos personales, en la medida en que resulte necesario para su ejecución.

o Mercadona garantiza y declara que cuenta con una base de legitimación suficiente para el tratamiento de los datos de los interesados objeto de este Acuerdo, de conformidad con lo dispuesto en la normativa de protección de datos.

o Con carácter general, queda prohibida la subcontratación con terceros de los servicios que impliquen el acceso y/o tratamiento, parcial o total, de datos personales, salvo que ******EMPRESA.2*** cuente con la autorización previa, expresa y por escrito de Mercadona.

o Los datos personales de Mercadona serán tratados por ******EMPRESA.2*** únicamente para llevar a cabo la prestación del servicio. Si ******EMPRESA.2*** considerase necesario llevar a cabo un tratamiento de los datos con una finalidad distinta, deberá solicitar previamente la autorización por escrito de Mercadona. A falta de dicha autorización, ******EMPRESA.2*** no podrá efectuar dicho tratamiento.

o Las categorías de interesados cuyos datos serán tratados por el ******EMPRESA.2*** en virtud de este acuerdo son: clientes de Mercadona, personas con una orden de alejamiento o medida judicial análoga a las instalaciones de Mercadona, personas captadas por el sistema de reconocimiento facial.

o ******EMPRESA.2*** tratará únicamente datos identificativos (nombre, apellidos e imagen) y los datos personales asociados al patrón biométrico en virtud de este Acuerdo.

o ******EMPRESA.2*** se compromete a garantizar, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto, y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, la aplicación de medidas técnicas y organizativas apropiadas para garantizar un

nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: la seudonimización y el cifrado de datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

o ******EMPRESA.2*** se compromete a notificar a Mercadona, sin dilación indebida y en un plazo máximo de 72 horas, las violaciones de la seguridad de los datos personales de las que tenga conocimiento, dando apoyo en la notificación a la AEPD u otra Autoridad de Control competente y, en su caso, a los interesados, de las violaciones de seguridad que se produzcan, así como a dar apoyo, cuando sea necesario, en la realización de evaluaciones de impacto de privacidad y en la consulta previa a la AEPD u otra Autoridad de Control competente, cuando proceda.

o ******EMPRESA.2*** se compromete a llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de Mercadona.

o ******EMPRESA.2*** se compromete a poner a disposición de Mercadona toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en este Acuerdo y para permitir y contribuir a la realización de auditorías, incluidas las inspecciones, por parte de Mercadona o un tercero autorizado por Mercadona.

o La estipulación séptima del acuerdo detalla las obligaciones de secreto y confidencialidad (así como de establecimiento de medidas para su protección) a las que están sometidas ambas partes incluso después de finalizada la relación contractual en relación con la información y datos personales a los que tengan acceso.

o ***(…)***

o ******EMPRESA.2*** garantiza que, en relación con la ejecución del Acuerdo, no se llevará a cabo un tratamiento de datos personales fuera de la Unión Europea o en un país que no cuente con un nivel adecuado de protección.

El acuerdo anterior contiene, además, un anexo dedicado a medidas de seguridad en relación con: ***(…)***

- ******EMPRESA.3,*** como proveedor de seguridad privada y mantenimiento de sistemas de reconocimiento facial. Refiere el perfil de Responsable de Producción, con exclusividad para Mercadona según manifiesta, como

encargado de dirigir y coordinar los técnicos exclusivos para el servicio en Mercadona.

Se adjunta como documento número 10 del escrito 026459/2020, el Acuerdo de confidencialidad y tratamiento de Datos Personales por cuenta de tercero suscrito con fecha de 29 de diciembre de 2011 entre Mercadona y ******EMPRESA.4.***

Según publicación del BORME (referencia número 1) ******EMPRESA.4*** fue absorbida (…) por ******EMPRESA.6*** Con posterioridad, el día ***FECHA.2, se publicó en el BORME (referencia número 2) la entrada como socio único de ******EMPRESA.5 en ***EMPRESA.6***. Asimismo, se hace constar (referencia número 3) la relación de coincidencia por órgano social y domicilio entre ******EMPRESA.5 y ***EMPRESA.3.***

El objeto del acuerdo es regular el tratamiento que se va a dar a toda la información confidencial y datos de carácter personal a los que se tenga acceso en el contexto de los servicios prestados. Se refiere en el documento, dada la fecha de firma, la normativa de protección de datos personales conformada por la Ley Orgánica 15/1999 y su reglamento de desarrollo. Se destaca el siguiente contenido:

o *(…)*

o El encargado de tratamiento se obliga a:

(…)

"Adoptar todas las medidas de índole técnicas y organizativas exigidos por la normativa de protección de datos que resulten necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal, evitando la alteración, pérdida, tratamiento, acceso o cesión no autorizados."

"Una vez finalizada la prestación de servicios, los datos personales deberán ser destruidos o devueltos a la parte emisora (a elección de ésta última), el igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto de tratamiento."

"Todos los datos personales suministrados tienen el carácter de confidencial, y bajo ningún concepto podrán ser revelados."

"El Encargado de Tratamiento deberá comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente Acuerdo y, en concreto, las relativas al deber de secreto y medidas de seguridad."

Por otro lado, en relación con los destinatarios de la información, aclara Mercadona en su escrito que las únicas comunicaciones de datos previstas son las derivadas de la puesta en conocimiento de los quebrantamientos de órdenes de alejamiento de las FCSE, y de los juzgados y tribunales competentes en los procedimientos. Igualmente, el documento número 29 del escrito 026463/2020 que incluye la definición de la actividad de tratamiento relativa a la gestión del SDA, señala que estas cesiones se harían en el marco de una *"obligación legal"* del responsable.

Por último, Mercadona señala que en el marco de este proyecto no se llevan a cabo transferencias internacionales de datos personales.

3. Aportación de la imagen al procedimiento judicial e inclusión en el SDA

En relación con las imágenes "indubitadas" contra las que se efectúa la comparación, señala Mercadona que *"ha tenido en cuenta que, sin unas imágenes fiables y nítidas, que cumplan determinadas exigencias técnicas explicadas más adelante, no sería posible llevar a cabo la actividad pretendida".* Señala que, *"por ello con carácter previo a la implementación del Sistema se han hecho numerosas pruebas (…) verificando que el sistema funciona de forma correcta".* Añade que, *"todo ello, tendente a evitar errores en los sistemas biométricos que, en su caso, pudieran derivar en graves consecuencias para la persona y, en particular, la denegación errónea a personas autorizadas y la aceptación errónea de personas no autorizadas que podrían llegar a ocasionar serios problemas a muy diferentes niveles, tal y como ha puesto de manifiesto la Agencia en su Informe 010308/2019"* (referencia número 4).

Sobre este particular Mercadona adjunta un documento (documento número 3 del escrito 026457/2020) que detalla *"los requisitos técnicos para las imágenes del Sistema".* De este documento, redactado en inglés y titulado *"Face Enrollment Best Practices",* se subraya el siguiente contenido:

- ***(…)***

Sobre la fuente de la que se obtendrían estas imágenes, primeramente manifiesta Mercadona que *"respecto a las condenas firmes que son resultado de procedimientos penales en los que MERCADONA es parte del procedimiento, las imágenes se obtienen de las cámaras de videovigilancia con las que cuenta en sus instalaciones y que fueron aportadas en el procedimiento como prueba, siendo válidamente obtenidas y admitidas por el Juzgado o Tribunal competente".*

En concreto, indica Mercadona que cuando se produce una denuncia por hechos que guardan relación con las instalaciones, bienes o trabajadores de Mercadona, los abogados responsables de las tiendas solicitan vía correo electrónico al CAS las imágenes de los hechos y del autor o autores. A continuación, ***"(…)"***. Apunta Mercadona que las personas encargadas de localizar y extraer las imágenes *"tienen la clasificación de "Gerente" de visionado de imágenes, posición que requiere de una formación específica en materia de seguridad y videovigilancia, así como un entrenamiento específico sobre el funcionamiento de este sistema".* A continuación, expresa que las imágenes ***"(…)***".

Indica Mercadona en este punto que dispone de un registro, que denomina *"Petición imágenes DAM",* que consiste en *"un listado propio de trabajo interno y exclusivo del CAS con los siguientes campos:*

- *Zona: número de la zona de tiendas a la que pertenece el centro*

- *Centro: número de la tienda.*

- *Denominación: nombre del centro.*

- *Población: municipio donde está ubicada.*

- *Provincia: en la que se ubica.*

- *Fecha solicitud imágenes: fecha en la que el abogado solicita las imágenes al CAS.*

- *Observaciones: anotaciones que se quieran registrar.*

- *Entregado: a FCSE, Juzgado o en blanco si no se ha hecho.*

- *Fecha juicio.*

- *Sentencia: prohibición de acceso, orden de alejamiento o en blanco si no se ha dictado.*

- *Liquidación de condena: al recibirla se rellena con un sí, en caso contrario se indica pendiente.*

- *Fecha inicio: en la liquidación de condena aparece desde que día la persona condenada no pueda entrar.*

- *Fecha fin: fecha de finalización de la condena de prohibición de acceso u orden de alejamiento.*

- ****EXPEDIENTE.1: identificador único que coincide con el del procedimiento del Juzgado.*

- *Fecha de identificación: día y hora en el que se ha identificado 100% a la persona condenada a no poder entrar a esa tienda.*

- *Tienda de identificación: centro donde se ha identificado 100% a esa persona.*

- *Gerentes CAS: nombres de los Gerentes de visionado presentes en la confirmación de identificación de esa persona."*

Según explica, en este momento se registra la petición en el listado y los distintos campos se van completando según corresponde a lo largo de las diferentes fases.

Mercadona adjunta (documento número 2 del escrito 026457/2020) el documento *"Petición imágenes DAM"*.

Añade que *"en el supuesto de que la resolución judicial determine la orden de alejamiento, las imágenes aportadas al procedimiento se convertirían en muestra biométrica indubitada y, consecuentemente, serían transformadas en plantilla".* En cuanto al alcance territorial, expresa que *"vendrá definido por la resolución judicial firme, pudiendo limitarse a una tienda, a varias o al territorio determinado por el Juzgado pertinente"*.

En segundo lugar, *"en relación con aquellas condenas en las que MERCADONA no es parte en el procedimiento (en caso de órdenes de alejamiento por delitos cometidos contra empleados de MERCADONA -supuestos de violencia de género, por ejemplo-) y los Juzgados y Tribunales soliciten directamente la colaboración a MERCADONA, en relación con el alcance de la orden de alejamiento al centro de trabajo de la víctima, para hacer efectivas las órdenes de alejamiento, serán los propios Juzgados y Tribunales quienes comunicarán, a través de la oportuna resolución judicial, a MERCADONA la necesidad de su colaboración para garantizar dicha efectividad, así como los términos de dicha medida, en relación con aspectos tales como la duración de la misma y tiendas sobre las que sería aplicable"*. Según expone, *"en estos casos, estas imágenes habrán sido aportadas en el procedimiento del que la resolución judicial trae causa y la justificación para su uso vendrá determinada por el requerimiento de utilización de medios tecnológicos para la orden de alejamiento concreta".* Y añade que en estos supuestos necesitaría que "*los Juzgados y Tribunales directamente, o a través de la FCSE, le entregasen imágenes válidas, que cumplan con los requisitos expuestos que el sistema de reconocimiento facial necesita para establecer una muestra indubitada previa*".

Expone además el caso en que *"el requerimiento provenga directamente de FCSE o* ******ORGANISMO.1****, con base en una investigación que se encuentren llevando a cabo o cuestiones relacionas con* ******ASUNTO.1****".* Al respecto,

expresa que *"para poder emplear el sistema analizado, deberá proveerse, igualmente, de las garantías expuestas (concretamente, cuando procedan, las establecidas por la normativa en materia de protección de datos), a saber, orden judicial fundamentada en Derecho, fotografía sobre la que pueda obtenerse el patrón biométrico, delimitación temporal de la medida y tiendas sobre las que sería aplicable".*

En relación con la inclusión de las imágenes en el SDA, señala Mercadona que, *"una vez que MERCADONA cuenta con una resolución judicial firme que determine la imposición de una orden de alejamiento o medida judicial análoga respecto a una o varias tiendas MERCADONA, el abogado responsable del expediente, envía un correo electrónico al CAS"* en el que se indica el número de sentencia, los centros a los que afecta, y el período de vigencia, y se adjunta el *"documento pdf. con liquidación de condena/medida cautelar"*. Así, detalla Mercadona que *"la imagen se incorpora al sistema con la limitación territorial del área o tiendas determinadas en la resolución judicial, indicando la limitación temporal del plazo o caducidad de la orden de alejamiento, el cual viene determinado en la resolución judicial".*

Según señala Mercadona, este proceso implica completar la información correspondiente del registro *"Petición imágenes DAM"*. Tras ello el Departamento de Seguridad, al objeto de realizar una nueva alta en el sistema, utiliza una *"ficha"* con la siguiente información:

- Número de procedimiento judicial.

- Descripción, incluyendo teléfonos de las FCSE a los que llamar y del servicio de vigilancia en caso de disponer de él en el centro, fecha de inicio y fecha de fin de detección, y una breve descripción de la medida judicial.

El documento número 4 del escrito 026457/2020 contiene el listado de teléfonos asociados a los distintos centros de Mercadona.

- Grupo: *(…)*.

En caso de que la resolución judicial fuese absolutoria o se denegase la medida cautelar, señala Mercadona que *"el abogado responsable del caso enviaría un correo electrónico al CAS, para la eliminación de las imágenes bloqueadas".* Ello provocaría la supresión de las imágenes y la actualización del listado *"Petición imágenes DAM"*.

4. Activación del SDA, detección y alerta

Según describe Mercadona, ***(…).***

Para hacer el seguimiento de las fechas de finalización de la medida judicial, se utiliza la aplicación *"*****APLICACION.1**". **(…).** Añade que el acceso al sistema requiere de usuario y contraseña individuales que son facilitados por el Departamento de Informática.

Una vez activado el sistema, "*a través de las cámaras de reconocimiento facial, se realizará la comprobación de las imágenes captadas a tiempo real con la imagen o imágenes indubitadas que se hayan incluido. Este proceso de comprobación dura décimas de segundo (0.3 segundos en la actualidad) entre que una imagen es captada y se realiza la verificación frente a la imagen indubitada incluida en el Sistema".*

En relación con las cámaras instaladas en cada centro, se subraya la siguiente información contenida en el escrito:

- ***(…)***

- Mercadona *"ha procedido y procederá a cumplir con el deber de información (…) en aquellos centros en los que se haya procedido a la instalación de dichas cámaras, incluso aunque las mismas no estén activadas para cumplir con la expectativa de privacidad de los clientes y empleados"*.

En relación con la captación de la imagen por la cámara, Mercadona aporta los siguientes documentos:

- Documento número 5 del escrito 026457/2020, ***(…)***, calificado como confidencial. Este documento redactado por **"***EMPRESA.2"** en inglés y titulado "******TITULO.1***" presenta los resultados obtenidos tras analizar el potencial sesgo de género y color de piel en el sistema de reconocimiento facial ***"***APLICACION.2" de ***EMPRESA.2.*** El documento concluye que el sistema no se encuentra sesgado en base a estos atributos.

- Documento número 6 del escrito 026459/2020, *"descripción del sistema utilizado por *****APLICACION.2,** en la extracción del patrón biométrico y su comparación en relación con el proceso de anonimización empleado"*. El documento, redactado en inglés por ******EMPRESA.2***, se titula *"*****TITULO.2**".* Algunas de las características del sistema descritas en el documento son:

o ***(…)***

- Documento número 7 del escrito 026459/2020, ***"***DOCUMENTO.1"***. El documento, redactado en inglés por ******EMPRESA.2,*** se titula ***"***TITULO.3"*** e incluye una explicación del proceso de reconocimiento facial, que sigue las siguientes fases: detección, extracción de características, ajuste, y reconocimiento. Define resultado como la distancia entre el patrón analizado y el

patrón de comparación inscrito. Añade que las probabilidades de que esta distancia sean mayores entre sujetos diferentes aumentan si se mejora la calidad de las imágenes.

Asimismo, Mercadona describe en su escrito (págs 24-33) la evaluación que ha realizado al objeto de valorar la eficacia del sistema de detección. Según explica, las pruebas se han realizado con un umbral de detección de ***X,XX*** ya que sería el recomendado por el fabricante ******EMPRESA.2.*** para optimizar la relación entre detecciones y falsos positivos. Así, expresa que *"una persona detectada con score **X,XX** significa que tiene una semejanza como mínimo en un **YY%** a la imagen de referencia del sistema."*

Añade además que las pruebas se han realizado utilizando la solución ***"***APLICACION.2*** versión 2.2 del fabricante ******EMPRESA.2"*** sobre distintos tipos de cámaras, configuraciones, imágenes de referencia ***(…)*** y escenarios (***…)*** que le han permitido seleccionar la combinación que ofrece mejores resultados. Según manifiesta en el escrito, en las pruebas realizadas no se habría producido ningún falso positivo.

Además, señala en relación con el proceso de detección de una persona con mascarilla que:

"el proveedor de la solución informática ha desarrollado una mejora con el fin de identificar personas con la cara semi-oculta por estas mascarillas, tal y como se puede visualizar en las imágenes aportadas a lo largo del escrito.

*En este sentido, es importante señalar que los sistemas de reconocimiento facial basan la identificación recogiendo la información de la zona periocular de la cara **(…).***

El sistema pierde información ya que parte de esta zona está oculta, por lo que se ha optimizado la lectura de la parte visible sin bajar el umbral (treshold [sic]) de identificación."

Hechas estas precisiones respecto a las pruebas de eficacia del sistema, se describe el proceso de generación de la alerta:

*"Una vez activado el Sistema de Detección Anticipada en la/las tienda/s objeto de la sentencia firme y en el caso de que alguna de las cámaras de reconocimiento facial instaladas en las tiendas detectase el acceso de una persona cuya imagen está incluida en el sistema *****APLICACION.2**, se generaría una alerta que iniciaría el proceso de confirmación y aviso a las FCSE.*

Esta alerta que detecta la coincidencia en las cámaras de la tienda se envía por correo electrónico a una dirección específica elaborada a tal efecto […]

A esta cuenta de correo tienen acceso las [sic] únicamente los siguientes perfiles:

- *El Responsable de Proyecto.*
- *Coordinador del CAS.*
- *Gerentes, responsables de turno en el CAS.*
- *Gerentes de visionado de imágenes.*

[…] Si alguna otra persona necesitara acceder a esta cuenta tendría que solicitar expresamente al responsable del Proyecto, la necesidad de este nuevo acceso.

Este correo de alarma indicando la coincidencia de las imágenes en una tienda concreta, es generado por cada uno de los equipos de las tiendas"

Mercadona facilita en su escrito (pg. 21) un ejemplo de correo enviado. Según se indica, en el correo se envía la siguiente información:

- *"Título:* ***(…)***
- *Nombre:* ***(…)***
- *Grupo:* ***(…)***
- *Centro:* ***(…)***
- *Cámara:* ***(…)***
- *Fecha y hora de la detección.*
- *Coincidencia:* ***(…)***
- *Descripción:* ***(…)***
- *Imagen de referencia:* ***(…)***
- *Imagen de detección:* ***(…)***

5. Recepción y validación de la alerta, y comunicación a las FCSE

Tal y como describe Mercadona, el proceso involucra *"un doble factor de verificación de los positivos para evitar los riesgos derivados de un tratamiento*

exclusivamente automatizado". Así, incide en que *"una vez recibida la alerta, la misma será contrastada por los Gerentes de visionado del Centro de Atención a la Seguridad presentes en ese momento, siendo confirmada (sólo en el caso de que todos los Gerentes de visionado confirmen que se trata de la misma persona) o no confirmada (si alguno de ellos presenta dudas a la hora de confirmar que se trata de la misma persona). En el caso de que no sea confirmada, la imagen se destruirá, estudiando las razones técnicas de la alarma y se terminará el proceso".* Según señala, *"los Gerentes de visionado del CAS tienen la experiencia y formación suficientes para realizar esta comprobación".*

Mercadona incide en su escrito en que *"esta comprobación por parte de los responsables del Departamento de Seguridad es totalmente obligatoria en el proceso".* Así, entiende que *"debido al proceso de comprobación posterior, no existiría en ningún caso un tratamiento a través de una decisión automatizada".* Para realizar esta afirmación se apoya en la *"Guía del Grupo de Trabajo del Artículo 29 sobre las decisiones automatizadas publicada el 3 de octubre de 2017"* (referencia número 5).

Tras la confirmación de la alarma, según describe Mercadona, un Gerente de visionado se encargará de:

(…)

Una vez cerrado este proceso, se procederá a la extracción de la imagen objeto de detección, para evitar tratamientos no necesarios sobre la misma más allá de su aportación a las autoridades competentes."

6. Plazos de conservación de los datos personales

Manifiesta Mercadona en su escrito que *"**(…)**"*

Seguidamente, Mercadona diferencia dos supuestos. Así, en primer lugar, describe el comportamiento del sistema durante la fase de detección en relación con las personas cuya imagen no coincide con ninguna de las imágenes almacenadas en el sistema:

"se han adoptado todas las medidas técnicas y organizativas necesarias al objeto de minimizar al máximo cualquier potencial tratamiento de datos y limitarlo a meros almacenamientos residuales técnicos (estrictamente necesarios para el propio funcionamiento del sistema)."

*"el sistema de reconocimiento facial detectará (de manera automática y durante un lapso no apreciable) y analizará las imágenes individualmente que reciba de cada centro. **(…)***

Con respecto al supuesto de detección de un positivo (coincidencia con una imagen de la base de datos), Mercadona expresa lo siguiente:

(…)

Todo lo anterior figura consignado, de manera resumida, en la evaluación de impacto de la privacidad (documento 30 del escrito 026463/2020). Así, ésta expresa que:

"Los datos se conservarán:

(…)

Por último, se hace constar que, según se observa en el registro de actividades de tratamiento (extracto adjunto como documento número 29 del escrito 026463/2020), la gestión del SDA y la videovigilancia son actividades de tratamiento independientes. En el caso del tratamiento de datos personales relativo a la actividad de videovigilancia el plazo de conservación consignado es de treinta días.

7. Arquitectura del sistema, evaluación de impacto, y medidas de seguridad

El documento número 29 del escrito 026463/2020 incluye el análisis de riesgos relativo a la gestión del SDA. Éste, otorga a esta actividad de tratamiento un riesgo inherente medio y un riesgo residual bajo tras la implantación de medidas mitigadoras. Entre otras cuestiones, el análisis señala que la actividad implica: ***"(…)".*** Esto le lleva a determinar la necesidad de ejecutar una *"PIA"*.

El documento número 30 del escrito 026463/2020 se corresponde con la evaluación de impacto de la privacidad del proyecto. Ésta incluye la evaluación del riesgo inherente al tratamiento a través del análisis de ******NÚM.6*** amenazas. El resultado que obtiene es que el nivel de riesgo es *"tolerable"*. Se subraya el contenido relativo a las siguientes amenazas:

- **(…)**

Asimismo, se señala en la evaluación de impacto que *"se ha procedido a examinar el Proyecto, una vez operativo, para verificar que los riesgos detectados se han abordado correctamente y que no se han detectado otros nuevos".*

La evaluación de impacto de la privacidad incluye, asimismo, el contenido siguiente en el apartado quinto dedicado a las conclusiones:

"(…)"

Por otro lado, Mercadona describe en su escrito (págs. 35-49) la arquitectura del SDA y las medidas de seguridad implantadas. Según dispone, los elementos que componen la arquitectura son:

- Equipos de las tiendas.

(…)

- Cámaras de las tiendas.

(…)

- Equipos del CAS.

(…)

- Sistema ******APLICACION.2*** versión 2.2.0. de ******EMPRESA.2*.**

(…)

- Sobre las tiendas:

o ***(…)***

- Sobre el CAS:

o ***(…)*** de la División de Seguridad de Mercadona o tener una autorización de ésta.

- Sobre el programa de reconocimiento facial:

(…)

- Sobre los sistemas propios de Mercadona en que se apoya el SDA:

o ***(…)***

7. Finalidad, licitud y proporcionalidad

Señala Mercadona que *"puede concluirse que la finalidad a la que atiende la instalación del Sistema de Detección Anticipada es la de dar cumplimiento a las resoluciones judiciales en las que se haya condenado al denunciado con una orden de alejamiento, como consecuencia de hechos que tengan relación con*

las instalaciones, bienes o trabajadores de MERCADONA, en determinadas circunstancias especiales y siempre que así lo establezca una resolución judicial firme".

Con respecto a la base de legitimación manifiesta Mercadona que *"el tratamiento de datos llevado a cabo por parte de MERCADONA al objeto de preservar la seguridad de las personas y bienes, así como de sus instalaciones encuentra cabida en el interés público."* Así, cita igualmente en su escrito Mercadona el siguiente contenido del Informe 010308/2019 de la AEPD (referencia número 4):

"En el presente caso, ya hemos citado cómo el artículo 22 de la LPDGDD regula los tratamientos con fines de videovigilancia cuya legitimación se encuentra, tal y como señaló en su Dictamen el Consejo de Estado y ha recogido la Ley en su Exposición de Motivos, en la existencia de una finalidad de interés público incardinable en el artículo 6.1.e) del Reglamento general, al tener por finalidad "preservar la seguridad de las personas y bienes, así como de sus instalaciones".

A tal efecto expone Mercadona que *"el tratamiento realizado para preservar la seguridad de las personas y bienes, así como de sus instalaciones (el mencionado por la AEPD en el Informe mencionado, como ejemplo de tratamiento amparado en interés público) es el fin principal del tratamiento de datos llevado a cabo por MERCADONA".*

Por otra parte, trae a colación Mercadona que *"el artículo 8 de la Ley Orgánica 3/2018 […] recoge lo siguiente: "El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley". En base a lo expuesto, es interés de esta parte mencionar que la norma con rango de ley que habilita a MERCADONA para la adopción de mecanismos que detecten y mitiguen la comisión de conductas fraudulentas respecto al tratamiento realizado para preservar la seguridad de las personas y bienes, así como sus instalaciones, es la Ley 5/2014, de 4 de abril, de Seguridad Privada (como por ejemplo el artículo 4 sobre los fines de la norma o el artículo 8 sobre sus principios rectores)."*

Se incluye en el expediente, referencia número 6, un extracto de la citada Ley 5/2014 en el que figura la redacción de los artículos 4 y 8.

Por otra parte, manifiesta Mercadona que *"no cabe duda de que el tratamiento de datos llevado a cabo por un sistema de reconocimiento facial entraría dentro de la categoría de dato especial".* Sobre esto, expone que *"solamente va a utilizar el Sistema en el supuesto de que sea parte dentro de un procedimiento*

judicial en el que mediante resolución firme se determine el uso de reconocimiento facial para hacer efectivas órdenes de alejamiento. Por ello, mi representada considera que tratamiento analizado tiene cabida en el artículo 9.2.f) en virtud del cual podrían tratarse datos sensibles cuando "el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones". En relación con lo anterior, añade lo siguiente:

***"(…)"**.*

Este argumento, es el defendido por los Juzgados y Tribunales, cuando se posicionan a favor de la opción defendida MERCADONA, autorizando a que dicha condena se controle a través de medios electrónicos, en orden al reconocimiento facial, en virtud de lo previsto en el artículo 48.4 del CP."

Se ha incorporado al expediente (referencia número 7) un extracto de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal que contiene la redacción del artículo 48.

Al hilo de lo anterior añade además que:

"cabe traer a colación el artículo 1 del CC en el que se recoge lo siguiente:

"1. Las fuentes del ordenamiento jurídico español son la ley, la costumbre y los principios generales del derecho.

2. Carecerán de validez las disposiciones que contradigan otra de rango superior.

(…)

6. La jurisprudencia complementará el ordenamiento jurídico con la doctrina que, de modo reiterado, establezca el Tribunal Supremo al interpretar y aplicar la ley, la costumbre y los principios generales del derecho.

7. Los Jueces y Tribunales tienen el deber inexcusable de resolver en todo caso los asuntos de que conozcan, ateniéndose al sistema de fuentes establecido."

Por tanto, cabría concluir que, puesto que los Jueces y Tribunales tienen el deber inexcusable de resolver en todo caso los asuntos que conozcan, atendiéndose al sistema de fuentes establecido, el que un Juez haya considerado adecuado utilizar un sistema de reconocimiento facial para garantizar el cumplimiento de órdenes de alejamiento en las instalaciones de MERCADONA, tendría suficiente peso para legitimar el tratamiento.

Es más, cabe traer a colación el artículo 24 de la CE, que se eleva a la categoría de derecho fundamental y que regula el derecho de defensa dentro del cual se incardina el derecho a la tutela judicial efectiva, según el cual todas las personas tienen derecho de acceso a la jurisdicción, es decir, han de tener la posibilidad de acudir a los órganos jurisdiccionales y de formular ante ellos peticiones de tutela. Asimismo, el derecho a la tutela judicial efectiva también comprende el derecho a que los órganos jurisdiccionales se pronuncien sobre la pretensión formulada y dicten así una resolución sobre el fondo del asunto, motivada y fundada en Derecho.

Además, el Tribunal Constitucional viene entendiendo que dentro del derecho a la tutela judicial efectiva se encuentra, como una manifestación necesaria, el derecho que los justiciables tienen a que las sentencias que los tribunales ordinarios hayan dictado para la tutela de sus derechos e intereses legítimos se hagan cumplir forzosamente. Este derecho a la ejecución forzosa enlaza así con la potestad jurisdiccional que la CE reconoce a los tribunales en su artículo 117.

[…] Y, además, todos los sujetos jurídicos (de carácter público o privada) tiene la obligación de cumplir las resoluciones judiciales firmes y debe colaborar con los juzgados y tribunales en la ejecución de lo resuelto, tal y como dispone el artículo 118 de la CE.

En cualquier caso, el beneficiado por una resolución judicial dispone de un auténtico derecho subjetivo, que tiene carácter de derecho fundamental, al entroncar directamente con el derecho a la tutela judicial efectiva del artículo 24.1 de la CE, y es calificable de derecho subjetivo público, pues se exige respecto de los órganos jurisdiccionales del Estado."

Se ha incorporado al expediente (referencia número 8) un extracto del Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil que contiene la redacción de los artículos 1 y 3. Asimismo, también se ha incluido (referencia número 9) un extracto de la Constitución Española que incluye los artículos 24, 117 y 118.

Con respecto a la licitud del tratamiento concluye Mercadona que *"da cumplimiento a lo establecido por la AEPD en sus Informes 36/2020 y 010308/2019, en base a que "la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el artículo 6 RGPD, en sus apartados 2 y 3 […]. Y en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a que se refiere el artículo 9.1 RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter*

general en su apartado 1", en tanto en cuanto el tratamiento quedaría legitimado por el artículo 6.1.e) RGPD en base al interés público derivado de la necesidad de preservar la seguridad de los clientes, personal e instalaciones y por el artículo 9.2.f) para poder responder a los procesos en los que es parte y en los que se ha determinado como medida el uso de dicha tecnología para reconocer a los sujetos objetos de una orden de alejamiento."

Se ha incorporado al expediente (referencia número 10) el informe 36/2020 emitido por el gabinete jurídico de la AEPD.

Por otro lado, manifiesta Mercadona que la finalidad del sistema implica el tratamiento de datos relativos a condenas e infracciones penales. Explica, no obstante, que este tipo de datos ya se trataban con anterioridad a la implantación del sistema ya que se trata de una práctica habitual del sector identificar aquellas personas que puedan suponer un riesgo para garantizar la seguridad de los trabajadores y clientes. Consecuentemente expone que *"el sistema estudiado en este escrito viene a realizar este mismo tratamiento, no suponiendo una actividad diferente en lo referido al tratamiento de datos personales relativos a sanciones o condenas penales".*

Para apoyar la legitimidad del tratamiento de esta tipología de datos, en su escrito Mercadona (referenciando los artículos diez del RGPD y de la LOPDGDD) manifiesta que *"trata datos relativos a condenas e infracciones penales bajo la supervisión de las autoridades públicas, puesto que el tratamiento llevado a cabo por MERCADONA se encuentra plenamente legitimado, debido a que solo se lleva a cabo respaldado por la Administración de Justicia o las FCSE.[…] el tratamiento se efectuará solamente sobre aquellas resoluciones judiciales en las que MERCADONA sea parte, por lo que no se generaría una base de datos de condenas penales, siendo la utilización de datos biométricos una especialización dentro del tratamiento ya existente y necesario, al ser MERCADONA parte del procedimiento o haya sido requerida por los propios Juzgados y Tribunales".*

En relación con la idoneidad, necesidad y proporcionalidad de implantación del sistema, manifiesta Mercadona que:

- *"el cumplimiento de una orden de alejamiento en una tienda sólo puede garantizarse de forma eficaz a través de medios electrónicos, dado que MERCADONA tiene 1.636 tiendas y aproximadamente 95.000 trabajadores en territorio español y cada año, la Compañía cuenta aproximadamente con* ******NÚM.2*** *procesos judiciales que pueden terminar en más de* ******NÚM.3*** *resoluciones judiciales a su favor en las que se condena en firme al denunciado con órdenes de alejamiento sobre las instalaciones de MERCADONA".*

- *"gran parte de dichas resoluciones judiciales son contra personas que actúan en el seno de bandas organizadas o resultan de especial peligrosidad para los jefes y los trabajadores, sobre las que resulta inviable dar cumplimiento a las resoluciones judiciales y hacer efectivas las condenas sin la utilización de mecanismos tecnológicos, puesto que los condenados se dirigen a las tiendas MERCADONA con un aspecto físico muy diferente (disfraces, pelucas, etc.), lo que dificulta el reconocimiento de forma visual por parte del personal de seguridad a aquellas personas que cuentan con una prohibición de acceso, más aun teniendo en cuenta que, aproximadamente, entran* ******NÚM.1*** *personas al día en una tienda MERCADONA"*.

- *"si bien el fin perseguido podría ser alcanzado por otros medios (mediante vigilantes de seguridad que controlen los accesos a las tiendas, por ejemplo) estos no garantizan la fiabilidad de las soluciones tecnológicas basadas en biometría, las cuales permiten alcanzar el fin perseguido por MERCADONA con mayores garantías y fiabilidad y, por tanto, mayor seguridad jurídica".*

- *"el requerimiento de que el tratamiento de datos sea "estrictamente" necesario, igualmente, se ve justificado en tanto en cuanto la medida de intervención inmediata sea necesaria en casos de flagrante delito, como es el incumplimiento de una pena que precisamente trata de prevenir la reincidencia y, sobre todo, la seguridad de los clientes y trabajadores de MERCADONA"*.

Sobre este punto añade Mercadona que *"esta argumentación se ve reforzada por la Autoridad de Protección de Datos Británica, Information Commissioner's Office, en el documento "The use of live facial recognition technology by law enforcement in public places 31"[sic] de Octubre de 2019, al indicar que "el propósito para el que se despliega el sistema de reconocimiento facial es de gran importancia puesto que hay una diferencia considerable entre el uso del reconocimiento facial para mitigar determinados delitos graves o violentos y los despliegues generalizados de la tecnología de reconocimiento facial para identificar a los ladrones conocidos"."*

Se ha incorporado al expediente (referencia número 11) el documento titulado *"The use of live facial recognition technology by law enforcement in public places"* publicado por el ICO (*Information Commissioner´s Office*)

- *"el tratamiento en cuestión solo genera beneficios y ventajas para el interés general, tanto como para los clientes y trabajadores de MERCADONA, como para los propios Juzgados y Tribunales, puesto que es la única manera eficaz de hacer efectivas las medidas decretadas por los mismos y; para las FCSE, al garantizar el Sistema una colaboración con las mismas, facilitándoles el desempeño de sus funciones".*

Concluye que el sistema *"cumple los requisitos de proporcionalidad y es estrictamente necesario para cumplir con la finalidad perseguida, puesto que no existen unos medios menos intrusivos para la privacidad del usuario que permitan obtener el objetivo perseguido, al resultar técnicamente imposible controlar de forma eficaz la entrada de personas condenadas con una prohibición de acceso a las instalaciones sin la utilización de un mecanismo tecnológico"*. Así, expresa que *"optar por un mecanismo alternativo, implicaría, sin duda alguna, una alteración de la finalidad del tratamiento perseguida".*

De esta forma, añade que *"debido al interés de MERCADONA en la implementación del sistema de reconocimiento facial, desde marzo de 2019, en los procedimientos judiciales en los que ésta ha sido parte, se ha solicitado a la Administración de Justicia el establecimiento de medidas frente a los denunciados en relación con el acceso a los establecimientos de MERCADONA de una determinada área territorial, de acuerdo con los hechos denunciados, durante un período de tiempo determinado, haciendo efectivo el control de dicha medida a través de medios electrónicos en orden al reconocimiento facial"* obteniendo como resultado que *"todos y cada uno de los Juzgados a los que se ha hecho la petición, han considerado el sistema de reconocimiento facial un medio adecuado para garantizar el cumplimiento de las órdenes de alejamiento (…) en virtud de lo previsto en el artículo 48.4 del Código Penal".*

8. Cumplimiento del deber de información

En su escrito Mercadona lista los siguientes mecanismos utilizados para cumplir con el deber de información:

- Carteles informativos sobre el sistema de reconocimiento facial colocados de forma visible en los accesos a cada una de las tiendas.

Adjunta, documento número 18 del escrito 026461/2020 y documento 18 del escrito 026463/2020, copia de la cartelería que se ha instalado en *"los accesos a sala de ventas"* en los que se ha implantado el SDA. El cartel incluye, bajo el título *"ZONA DETECCIÓN ANTICIPADA",* información sobre el responsable del tratamiento, el funcionamiento del sistema, el destinatario de la información (FCSE), la base jurídica del tratamiento, y la posibilidad de ejercer los derechos de protección de datos y de presentar una reclamación ante la AEPD. Además, se facilitan diversas vías para consultar información adicional sobre el tratamiento (interior de la tienda, teléfono, página de internet).

Expresa al respecto además que *"los distintivos informativos tienen un tamaño suficiente como para que cualquier usuario pueda leer su contenido y están ubicados en lugar suficientemente visible, en la entrada de la tienda, teniendo en*

cuenta que, el deber de información debe ser previo al tratamiento de los datos, en aras del riguroso respeto de esta parte con el principio de transparencia y el propio deber de información."

- La Política de Privacidad de la web de Mercadona

Adjunta, documento número 19 del escrito 026461/2020, copia de la política de privacidad de Mercadona publicada internet cuya última actualización, según se hace constar en el propio documento, se produjo el 1 de julio de 2020.

En el apartado de categorías de datos tratados se mencionan los *"datos biométricos (en aquellas tiendas de España donde esté implandtado [sic] el sistema de detección anticipada)".*

En el apartado correspondiente a las finalidades cita: *"llevar a cabo las actuaciones precisas para proteger los intereses vitales de los clientes cuando así sea necesario, o el cumplimiento de las resoluciones judiciales y las medidas en ellas acordadas."*

En el epígrafe dedicado a los plazos de conservación expresa lo siguiente:

"En relación con la protección del interés vital de las personas y la ejecución de las sentencias o resoluciones que conlleven órdenes de alejamiento sobre los centros de trabajo y/o personas, los datos serán tratados y custodiados el tiempo imprescindible para dar cumplimiento a las medidas judicialmente [sic] de aquellas personas condenadas a dicha orden de alejamiento (en aquellas tiendas de España donde está implantado el sistema de detección anticipada).

No obstante, los datos recogidos accesoriamente para cumplir con dicha finalidad permanecerán en el servidor únicamente en el proceso de comprobación (esta comprobación dura décimas de segundo). Una vez realizada esta comprobación procederá a ser destruida definitivamente (en aquellas tiendas de España donde está implantado el sistema de detección anticipada)."

En cuanto a la legitimación, la política de privacidad consigna que *"en el caso del tratamiento de los datos de carácter sensible serán tratados por razones de interés público con las consiguientes consideraciones previstas por la normativa de protección de datos, que debe ser proporcional al objetivo perseguido, que es hacer cumplir la ley, respetando los restantes principios de la normativa de protección de datos y estableciendo las medidas adecuadas y específicas para proteger los intereses y derechos de los interesados, sobre la base del Derecho de la Unión o de los Estados miembros (en aquellas tiendas de España donde está implantado el sistema de detección anticipada)."*

Asimismo, el apartado titulado *"Otros datos que tratamos en Mercadona"* contiene los siguientes párrafos:

"De igual modo te informamos que, con el fin de mejorar la seguridad de clientes y empleados, MERCADONA, en base al interés público puede tratar su imagen o su perfil facial biométrico para identificar a sujetos con una orden de alejamiento (o medida judicial análoga) en vigor contra MERCADONA o contra cualquiera de sus trabajadores (en aquellas tiendas de España donde está implantado el sistema de detección anticipada).

Dicha imagen únicamente se utilizará con esta finalidad y permanecerá en el servidor central únicamente en el proceso de comprobación (esta comprobación dura décimas de segundo). Una vez realizada esta comprobación procederá a ser destruida definitivamente (en aquellas tiendas de España donde está implantado el sistema de detección anticipada).

Estas imágenes únicamente se tratarán internamente por MERCADONA, siendo exclusivamente comunicadas a las Fuerzas y Cuerpos de Seguridad para proteger la seguridad de los clientes y trabajadores de MERCADONA y el cumplimiento de las medidas decretadas judicialmente (en aquellas tiendas de España donde está implantado el sistema de detección anticipada)".

Se ha incorporado (referencia número 12) la política de privacidad publicada en el sitio de internet de Mercadona cuya última actualización, según se consigna en la misma, se produjo el 5 de octubre de 2020.

- El teléfono de atención al cliente.

Adjunta, documento número 20 del escrito 026461/2020, copia del argumentario telefónico utilizado en relación con el SDA en el que se describe el funcionamiento del sistema.

- Impresos informativos puestos a disposición de los interesados en las tiendas para entregárselos en caso de que lo soliciten.

Adjunta, documento número 21 del escrito 026461/2020, copia del impreso en el que se describe el funcionamiento del sistema, expone la base jurídica del tratamiento, informa de la posibilidad de ejercer los derechos de protección de datos personales y de interponer reclamaciones ante la AEPD, y refiere la política de privacidad al efecto de obtener más información.

Igualmente, adjunta Mercadona (documento número 28 del escrito 026464/2020), la copia del correo electrónico que, según manifiesta, dirige en *"Responsable de Seguridad"* a los *"Responsables de Tienda".* En éste se informa sobre los documentos que habría que imprimir y facilitar a los clientes y trabajadores que soliciten más información sobre el SDA.

- El plan de comunicación de Mercadona.

Adjunta, documento número 22 del escrito 026462/2020, un extracto del documento *"Plan de Comunicación Detección Anticipada"* cuya fecha de creación, según figura en el mismo, es 1 de junio de 2020.

Además de lo anterior, Mercadona manifiesta en su escrito que, con carácter previo a la puesta en marcha del proyecto piloto, dirigió una nota de prensa (adjunta copia como documento número 23 del escrito 026462/2020) a las agencias de noticias de las ciudades afectadas al objeto de que fuera publicada en los medios de comunicación y así dar a conocer el proyecto a los residentes de estas zonas. Asimismo, señala que el día 3 de julio de 2020 envío a estas mismas agencias *"unas FAQs sobre el proyecto"* (aporta copia como documento número 24 del escrito 026462/2020). Entre otras cuestiones, se incide en esta lista de preguntas y respuestas en que *"en las tiendas conviven dos sistemas independientes uno del otro. Por un lado, videovigilancia convencional, y por el otro, detección anticipada"*. Esta cuestión se observa igualmente plasmada en el registro de actividades de tratamiento (extracto adjunto como documento número 29 del escrito 026463/2020), en el que la gestión del SDA y la videovigilancia figuran como actividades de tratamiento independientes.

Igualmente, Mercadona señala que ha informado a sus trabajadores acerca del tratamiento realizado por el SDA a través de diversas acciones. Así, facilita como documento número 25 del escrito 026462/2020, el texto que, según expone, estaría disponible a través *"portal del empleado".* Este texto incluye información sobre el responsable, la finalidad, la base jurídica, y la posibilidad de ejercer los derechos de protección de datos personales así como de interponer una reclamación ante la AEPD. El documento número 26 del escrito 026462/2020 se corresponde con la información dirigida al *"Comité Intercentros".* En este escrito, fechado el 30 de junio de 2020, se informa de la puesta en marcha con fecha de 1 de julio de 2020 del sistema en varias tiendas. Por último, expresa que el Departamento de Comunicación habría elaborado un video *"para que sus trabajadores comprendiesen el Proyecto a la perfección".* Aporta (documento número 27 del escrito 026463/2020) el argumentario del mismo.

Para concluir, Mercadona menciona que *"desde que se ha instalado el Sistema, MERCADONA, únicamente, ha recibido* ***una*** *solicitud de ejercicio de derechos que ha sido atendida correspondientemente."* Y a continuación expresa que *"este hecho permite concluir que los interesados consideran que la información que MERCADONA les proporciona a través de los canales mencionados da estrictamente cumplimiento a las disposiciones de la normativa de protección de datos y que el propósito seguido por MERCADONA al objeto del Proyecto es proporcional y adecuado."*

El día 28 de mayo de 2020 la AEPD publicó una nota de prensa titulada: "*La AEPD analiza en un informe el uso de sistemas de reconocimiento facial por parte de las empresas de seguridad privada*".

Este comunicado ha sido asimismo incorporado al presente expediente a través de la correspondiente diligencia.

TERCERO: Con fecha 5 de mayo de 2021**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 5.1.c) del RGPD, Artículo 6 del RGPD, Artículo 9 del RGPD, Artículo 12 del RGPD, Artículo 35 del RGPD, Artículo 13 del RGPD, Artículo 25 del RGPD, tipificada en el Artículo 83.5 del RGPD, y la medida cautelar consistente en la suspensión de todo el tratamiento de datos personales relativo al reconocimiento facial en sus establecimientos.

CUARTO: Notificado el acuerdo de inicio, el reclamado solicitó copia del expediente y ampliación de plazo para presentar alegaciones, lo que se concedió en los términos legalmente establecidos. Posteriormente, el reclamado presentó en plazo y forma escrito de alegaciones en el que manifiesta, en resumen, lo siguiente respecto a aspectos sustantivos:

1. Que su legitimación se residencia en el interés público (art. 6.1.e) del RGPD) para asegurar el cumplimiento de resoluciones judiciales.

2. Que el RGPD permite la utilización de datos biométricos siempre que se adopten las medidas de seguridad adecuadas, focalizando no tanto en la legitimación, que da por hecho, sino en que lo importante son las medidas de seguridad. Añade que, con medidas de seguridad adecuadas, el tratamiento puede llevarse a cabo, aunque se trate de categorías especiales de datos personales.

3. Alega y afirma que el tratamiento ahora analizado es la única medida capaz de solucionar este problema e indica que es necesaria, idónea, eficaz y proporcional.

4. Alega y afirma que no se lesionan los derechos de otros sujetos que entren en el supermercado puesto que no hay tratamiento de datos porque se produce en 0.3 segundos. Así, considera que sólo se tratarían los datos biométricos identificables de los condenados por resolución judicial firme, siendo imposible que pueda identificar a aquellas personas que no están en la base de datos indubitada.

5. El tratamiento ahora analizado ha sido previamente validado por diversas sentencias judiciales.

6. La AEPD no ha realizado un análisis pormenorizado del sistema implantado, y ha incluido innumerables remisiones a "*guías, artículos y directrices*" que no resultan vinculantes. En consecuencia, existe una vulneración a los principios de tipicidad y legalidad vulnerando el principio de interdicción de la arbitrariedad de los poderes públicos (art 9.3 de la C.E.).

7. Se ha informado de manera diligente, suficiente y adecuada de la puesta en funcionamiento del Sistema e implicaciones de éste, así como el medio para ejercitar los derechos reconocidos a los afectados.

8. El sistema implantado ahora analizado tuvo en consideración desde el diseño la potencial afectación a la privacidad de las personas.

En cuanto a aspectos no sustantivos o formales, realiza las siguientes alegaciones:

A. Desconocimiento de las dos reclamaciones (Facua y Apedanica), lo que es contrario a la práctica habitual de la AEPD.

B. El patrón de una persona no constituye un dato de carácter personal, por lo que no se necesita base legal para su tratamiento.

C. El sistema implantado no recoge información adicional a la condición de condenado incluido en su base de datos.

D. La propuesta de Reglamento sobre inteligencia artificial (COM (2021) 206. Anexos 1 a 9) publicada el 21/04/2021, considera que el sistema sería posible y conforme a las medidas que se proponen en dicha propuesta.

E. Alega la inexistencia de elemento subjetivo de culpabilidad.

F. La actividad principal de MERCADONA no está vinculada al tratamiento de datos sino al a la gestión de una cadena de supermercados.

G. Alega que tanto la AEPD y MERCADONA han ido adoptando el Sistema y ajustándolo a los requisitos de la Agencia.

Por lo anterior, MERCADONA solicita que se archive el expediente sancionador.

QUINTO: No consta por la reclamada solicitud de práctica de pruebas por lo que se tienen por incorporadas las actuaciones previas de investigación, así como los documentos aportados por el reclamado y la inspección de esta AEPD. Tampoco consta aportación del *"dictamen pericial sobre reconocimiento facial"* anunciado en el Segundo Otrosí del escrito de alegaciones.

HECHOS PROBADOS

PRIMERO: El tratamiento de datos de carácter personal implantado en fecha 1/06/2020 y continuado hasta el 6/05/2021 por MERCADONA en cuarenta establecimientos de la mercantil relativo a reconocimiento facial de aquellas personas que acceden a sus centros comerciales, constituye un tratamiento de datos de categoría especial de los regulados en el art. 9 del RGPD y art 9 de la LOPDGDD.

SEGUNDO: En el tratamiento de datos personales biométricos ahora analizado (datos de categoría especial) no consta acreditado la concurrencia de las circunstancias expuestas en el art 9.2 del RGPD, por lo que según lo dispuesto en el art. 9.1 del RGPD el tratamiento se encuentra prohibido. Consta acreditado la improcedencia de aplicar las excepciones del art. 9.2.f), g) y h) del RGPD al levantamiento de la prohibición general indicada en el art 9.1 de dicha norma.

TERCERO: Además, sin perjuicio de lo señalado en los Hechos probado Primero y Segundo, en el tratamiento de datos personales biométricos ahora analizado (datos de categoría especial) no consta base legítima conforme señala el art. 6 del RGPD, ni normativa legal que lo permita según dispone el art. 8 de la LOPDGDD.

CUARTO: En el tratamiento de datos personales biométricos ahora analizado (datos de categoría especial), sin perjuicio de lo señalado en los Hechos probado Primero y Segundo, no consta acreditada la información requerida en el art. 13 en relación con la obligatoriedad general que impone el art. 12 del RGPD y, en especial, lo dispuesto en el 12.1 respecto a “niños”. Tampoco consta acreditado el cumplimiento de los requisitos establecidos en el art 7 de la LOPDGDD respecto a los menores de edad.

QUINTO: En el tratamiento de datos personales biométricos ahora analizado, sin perjuicio de lo señalado en los Hechos probado Primero y Segundo, no consta acreditado el cumplimiento del principio de minimización expuesto en el art. 5.1.c) toda vez que el sistema de reconocimiento implantado por MERCADONA podría tratar de forma altamente plausible datos de diversa índole al margen de los estrictamente necesarios, como son los indicados y calificados de categoría especial en el art. 9.1 del RGPD y 9 de la LOPDGDD.

SEXTO: En el tratamiento de datos personales biométricos ahora analizado, sin perjuicio de lo señalado en los Hechos probado Primero y Segundo, no consta acreditado que desde el diseño se hayan establecido las salvaguardas en orden a garantizar las libertades y derechos de todos los afectados, conforme señala el art. 25.1 del RGPD.

SÉPTIMO: En el tratamiento de datos personales biométricos ahora analizado, sin perjuicio de lo señalado en los Hechos probado Primero y Segundo, no consta acreditado el correcto análisis de riesgos y la preceptiva evaluación de impacto, toda vez que no contempla, ni en uno ni en la otra, todos los sujetos afectados (FD V), como es el caso de trabajadores y menores.

OCTAVO: Siendo, por consiguiente, un tratamiento prohibido, dicha prohibición no puede obviarse mediante la aplicación de medidas de seguridad proactiva, ya que la prohibición del tratamiento determina que las mismas sean irrelevantes.

NOVENO: De conformidad con lo señalado en los Hechos probado Primero, Segundo y Octavo, se confirma la medida cautelar impuesta en el acuerdo de inicio.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

En relación con el escrito de alegaciones al acuerdo de inicio presentado por la mercantil, se debe significar, en síntesis, lo siguiente:

Respecto de las alegaciones recogidas en el antecedente CUARTO de tipo sustancial y numeradas del 1 al 8, se debe señalar que todas ellas ya se encuentran desvirtuadas y motivada -a través de un análisis pormenorizado resultado de la exhaustiva investigación previa llevada a cabo por esta Agencia- su improcedencia en los Fundamentos de Derecho (FD) del propio acuerdo de Inicio del presente procedimiento sancionador y de los señalados en la presente Propuesta de Resolución. No obstante, se contestan ahora de forma sucinta, sin perjuicio de ampliación en posteriores Fundamentos de Derecho:

Contestando a las alegaciones presentadas por MERCADONA, se significa lo siguiente:

- Sobre la legitimación: Mercadona no aduce en sus alegaciones al presente procedimiento ninguna excepción entre las contempladas en el art. 9.2 del RGPD que legitime el tratamiento de los datos biométricos del condenado; se limita a citar la legitimidad del tratamiento so pretexto de que "*no se lesiona en ningún momento la protección de datos de los sujetos".*

Lo anterior confirma lo indicado en el Acuerdo de Inicio: Mercadona no ostenta legitimación para llevar a cabo el tratamiento de datos personales consistente en el reconocimiento facial.

Asimismo, a través de las alegaciones formuladas por Mercadona, se corroboran las evidencias iniciales apreciadas por esta Agencia, esto es, que la mercantil estaba preconstituyendo la excepción del art. 9.2 del RGPD a los efectos de

poder tratar los datos biométricos regulados en el art. 9 del RGPD. Pues una vez obtenida la resolución judicial que permite de forma genérica la implantación de la medida de seguridad, la cadena de supermercados interpreta de forma unilateral el alcance de la resolución judicial y la utiliza a los efectos de justificar que ostenta legitimación en el sentido del art. 9.2.f) del RGPD no sólo para el condenado, sino también para el resto de los ciudadanos afectados por el sistema cuando acceden a los supermercados - que la mercantil engloba bajo el nombre de “no condenados”-.

En el acuerdo de inicio ya se incidía sobre la falta de legitimación para llevar a cabo el tratamiento consistente en el reconocimiento facial: se señalaba que donde no haya concurrencia de una de las excepciones que señala el artículo 9.2 del RGPD, no hay legitimación para tratar datos biométricos de nadie, con independencia de las causas de licitud señaladas en el art. 6 del RGPD, toda vez que el art. 9.1 lo prohíbe; si bien, entendíamos que existía legitimación respecto del tratamiento de los datos biométricos del condenado porque contaba, en el supuesto examinado y planteado por Mercadona, con la correspondiente medida de seguridad adoptada en una resolución judicial. La AEPD respeta las resoluciones judiciales, no pudiendo oponerse a lo consignado en las mismas. Sin embargo, la interpretación extensiva y unilateral de los términos expuestos en la resolución judicial por parte de Mercadona es contraria a los principios de necesidad, proporcionalidad y minimización que señala el RGPD (arts. 5.1.c), 25, 35.7.a) y considerandos 4, 156 y 170, por todos).

En este momento hemos de traer a colación el Auto de la Audiencia Provincial de Barcelona de 115/02/2021, Nº de Recurso 840/2020, y Nº de Resolución 72/2021. En el citado Auto se examina la adopción de la medida de seguridad consistente en el reconocimiento facial solicitada por Mercadona para el condenado. Concluye que las previsiones del artículo 48 del Código Penal han de complementarse con el consentimiento del condenado para que tal tratamiento de datos personales de reconocimiento facial pueda ser efectuado con legitimación suficiente: “*Si bien el artículo 48 del Código Penal establece "la privación del derecho a residir en determinados lugares o acudir a ellos impide al penado residir o acudir al lugar en que haya cometido el delito" y que "el juez o tribunal podrá acordar que el control de estas medidas se realice a través de aquellos medios electrónicos que lo permitan"; esto se produciría asegurando los derechos fundamentales del condenado, es decir, siempre que este hubiera dado su consentimiento. Debemos recordar que los condenados gozan de todos los derechos fundamentales reconocidos en la Constitución, a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria”.*

Además, el Auto considera que con el tratamiento no se está protegiendo el interés público sino más bien, los intereses privados o particulares de la mercantil.

- Necesidad de la medida: También significar que la mercantil se centra en la utilidad de la medida porque es eficaz, confundiendo “utilidad” con la “necesidad” objetiva de la medida. La medida implantada podrá ser eficaz, pero de ninguna manera necesaria.

De lo anterior, y de los fundamentos de derecho siguientes, decae todo el soporte jurídico esgrimido por MERCADONA para llevar a cabo el tratamiento de datos que pretende, al resultar prohibido conforme señala el art. 9.1 del RGPD, y no existir excepción que levante la prohibición.

En cuanto a al resto de alegaciones presentadas por MERCADONA (reseñadas de la A a la G), se debe señalar lo siguiente:

En cuanto a aspectos no sustantivos o formales, realiza las siguientes alegaciones:

A) <<Desconocimiento de las dos reclamaciones (Facua y Apedanica), lo que es contrario a la práctica habitual de la AEPD.>>

En este sentido, significar que la AEPD procedió a iniciar investigaciones previas al objeto de comprobar las supuestas infracciones al RGPD conforme señala el Título VIII de la LOPDGDD, llegando con posterioridad una serie de reclamaciones motivadas por aspectos generales de procedimiento y no reclamaciones singulares de afectados concretos, la AEPD. Hay que añadir que, tras el Acuerdo de Inicio, la reclamada ha dispuesto de la totalidad de la documentación que obra en el expediente administrativo.

En atención a las alegaciones de la mercantil, recordar que el traslado es un trámite potestativo y no obligatorio, derivado de la presentación de una reclamación. El traslado es un trámite ajeno al procedimiento sancionador.

A mayor abundamiento la parte reclamada no concreta en qué se le conculca su derecho de defensa, que ha de ser material y no formal.

B) <<El patrón de una persona no constituye un dato de carácter personal, por lo que no se necesita base legal para su tratamiento>>.

La génesis del Patrón biométrico parte de la recogida de características físicas del sujeto (la fotografía, que por sí misma es un dato de carácter personal al ser posteriormente objeto de tratamiento y, en consecuencia, identificable) de forma tal que le caracterice de forma inequívoca, por lo que, por la propia definición de dato personal, al resultar identificable, tanto la fotografía como el Patrón biométrico constituyen dato personal y su tratamiento está sujeto al RGPD.

Que Mercadona trate la imagen de cualquier persona que entre en sus establecimientos, la capte, obtenga de la misma un patrón, la coteje con la de la persona condenada y la supriman es un tratamiento de datos de carácter personal (reconocimiento facial). El patrón así obtenido de la imagen personal

constituye en sí mismo, un dato de carácter personal. No hay dos patrones iguales (Doc 6 del escrito de nre: 026459/2020).

A mayor abundamiento, y en atención a las alegaciones formuladas por la mercantil, hemos de recordar que la imagen de una persona es un dato de carácter personal y así lo reitera continuamente la AEPD; la imagen de la cara de una persona, de la que se extrae el patrón biométrico, identifica plenamente a ésta sin ulteriores actuaciones. En el marco del tratamiento de datos consistente en el reconocimiento facial, que la mercantil no posea el nombre de las personas cuyos datos biométricos tratan, como sí poseen el del condenado, no implica que no se trate de datos de carácter personal. Que no tengan previamente almacenada la imagen de una persona distinta de la condenada, para cotejarla con una base de datos a través de un patrón, tampoco significa que no nos encontremos ante un tratamiento de datos de carácter personal.

C) <<El sistema implantado no recoge información adicional a la condición de condenado incluido en su base de datos.>>

Al respecto, de debe señalar que la información que se recoge del condenado a partir de la base de datos indubitada de la que dispone y trata MERCADONA, es contrastada con información adicional de terceros al objeto de “emparejar“ características biométricas de ambos y, posteriormente, con base en algoritmos y en criterios de calidad, se admite la identidad por emparejamiento o bien se inadmite. En ambos casos siempre se recoge información adicional basada en características y datos personales que enriquece el sistema y que carece de base legal para su tratamiento.

D) <<La propuesta de Reglamento sobre inteligencia artificial (COM (2021) 206. Anexos 1 a 9) publicada el 21/04/2021, considera que el sistema sería posible y conforme a las medidas que se proponen en dicha propuesta>>.

En el Acuerdo de Inicio ya se hizo mención a los aspectos que ahora se alegan respecto al borrador de reglamento sobre inteligencia artificial aludido. En este sentido, el artículo 5 del citado Reglamento alegado señala:

“*Quedan prohibidas las siguientes prácticas de inteligencia artificial:*

(…)

(a) *el uso de sistemas de identificación biométrica a distancia «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, a menos que y en la medida en que tal uso sea estrictamente necesario para uno de los objetivos siguientes:*

(i) *la búsqueda específica de posibles víctimas de delitos, incluidos los niños desaparecidos;*

(ii) *la prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de las personas físicas o de un ataque terrorista;*

(iii) *La detección, localización, identificación o enjuiciamiento de un autor o sospechoso de una infracción penal contemplada en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI del Consejo y sancionada en el Estado miembro de que se trate con una pena privativa de libertad o una orden de detención por un período máximo de tres años, tal como determine la legislación de dicho Estado miembro."*

En el presente caso, no consta que se cumplan las excepciones (i) a (iii).

A mayor abundamiento, amén de que el citado reglamento se encuentra en tramitación, la normativa de protección de datos requiere siempre un análisis pormenorizado del caso concreto de que se trate a los efectos de verificar si se ostenta legitimación para un específico tratamiento de datos personales, alejado siempre tal análisis del automatismo.

E) <<Alega la inexistencia de elemento subjetivo de culpabilidad.>>

Si bien no es posible imputar una infracción en ausencia del elemento volitivo de responsabilidad (responsabilidad objetiva), en el presente caso la mercantil responsable era conocedora de la actividad que iba a iniciar contratando a entidades especializadas para su puesta en marcha. El hecho de haber procedido a realizar un análisis de riesgos deficiente al omitir no solo todos los sujetos afectados sino no evaluar como riesgo la prohibición del tratamiento que se contempla en el artículo 9.1 del RGPD, ya configura el elemento volitivo de culpabilidad. De haber evaluado el riesgo del tratamiento previsto, el resultado hubiera sido que nos encontramos ante un tratamiento prohibido y, en consecuencia, inaceptable, lo que en su caso hubiera llevado a aplicación de lo dispuesto en el artículo 36 de RGPD (consulta previa), que en ningún momento se ha tenido en cuenta y hubiera dado lugar al pronunciamiento de esta AEPD sobre el tratamiento de datos personales ahora analizado.

A mayor abundamiento, a la deficiencia inaceptable cometida en la elaboración el análisis de riesgos previo al tratamiento hay que añadir la también deficiente evaluación de impacto posterior, al no implicar a los todos los sujetos afectados, lo que constituye también una grave deficiencia al no determinar las graves consecuencias para los derechos y libertades de los interesados. Todos los ciudadanos que acceden a un centro comercial de Mercadona con sistema de reconocimiento facial implantado son tratados como condenados.

Lo anterior, configura la presencia del elemento volitivo de culpabilidad exigido por el art. 28 de la Ley 40/2015, de 1/10, de RJSP.

F) <<La actividad principal de MERCADONA no está vinculada al tratamiento de datos sino al a la gestión de una cadena de supermercados>>.

Si bien la actividad principal de MERCADONA sea la gestión de supermercados, también es cierto que dicha gestión implica como actividad paralela cotidiana y continua el tratamiento de datos personales tanto de sus clientes online como presenciales y sus trabajadores, que estos últimos ascienden a más de cien mil.

G. <<Alega que tanto la AEPD y MERCADONA han ido adoptando el Sistema y ajustándolo a los requisitos de la Agencia>>.

Esta alegación debe ser rechazada toda vez que en ningún momento esta AEPD haya adoptado posición alguna con el establecimiento del tratamiento ahora analizado y, tal y como ya se ha comentado, Mercadona no ha utilizado el mecanismo normativo establecido a tal efecto en el RGPD (art. 36 RGPD).

H. <<Alega desproporcionalidad en la cuantía de la sanción>>.

En este sentido, consta motivado en el acuerdo de inicio la cuantía de la sanción. A este respecto, señalar que el propio RGPD, art 83.1, señala que: *"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias".*

En el presente caso, la efectividad, proporcionalidad y el carácter disuasorio queda garantizados. La cuantía de la multa administrativa se ajusta a niveles muy inferiores a los máximos permitidos (por cada una, 10 o 20 millones de euros, o el 2% o 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

En consecuencia, las alegaciones deben ser desestimadas en su totalidad.

III

A los efectos de sistematizar la lectura y comprensión desde su inicio de la presente Propuesta de Resolución, se expone a continuación la doctrina de esta AEPD respecto del tratamiento ahora objeto de análisis, a la que se hará referencia, entre otras, a lo largo de la Propuesta de Resolución.

El 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 (Reglamento general de protección de datos, RGPD) define en su artículo 4.14 los datos biométricos como *"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, como imágenes faciales o datos dactiloscópicos".*

El artículo 9 de dicha norma regula el tratamiento de categorías especiales de datos, entre los que se encuentran los datos biométricos, estableciendo una prohibición general de su tratamiento en los siguientes términos:

"Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física."

En relación con el tratamiento de datos de reconocimiento facial, en nuestro Informe 36/2020, analizando el artículo 9.1 en relación con el Considerando 51 del RGPD, así como el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) señalábamos que:

"Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas

se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno)."

En el presente caso se realiza un tratamiento de datos biométricos con fines de identificación, es decir, de aislar un individuo entre varios, por lo que es un tratamiento de categorías especiales de datos sujeto a la regla general de prohibición de los mismos (art. 9.1. RGPD).

No obstante, el artículo 9.2 del RGPD regula excepciones a dicha prohibición general al establecer que:

"el apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.

(…)

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;"

(…)

En relación con el apartado g), destaca que cuando el tratamiento sea necesario por razones de interés público, que debe ser esencial sobre la base del derecho de los Estados miembros, proporcional al objetivo perseguido, respetar en lo

esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Por tanto, procederá analizar si, en el presente caso, concurren los presupuestos establecidos en el artículo 9.2. para levantar la prohibición de tratamiento de datos biométricos.

Esta Agencia ha tenido ocasión de pronunciarse, en diversas ocasiones sobre los requisitos necesarios para levantar la prohibición establecida en el art. 9.1 del RGPD, en especial respecto de los requisitos establecidos por el artículo 9.2.g) del RGPD, para poder amparar los tratamientos de datos personales basados en el reconocimiento facial, dada la proliferación de propuestas recibidas en relación con los mismos desde ámbitos diferentes, lo que pone de manifiesto el interés creciente en utilizar estos sistemas y la constante preocupación de esta autoridad de control, al tratarse de sistemas de identificación muy intrusivos para los derechos y libertades fundamentales de las personas físicas. Preocupación que es compartida por el resto de autoridades de control desde hace años, como ponen de manifiesto el Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003 por el Grupo del 29, o el posterior Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, y que ha llevado a que el propio legislador comunitario incluya estos datos entre las categorías especiales de datos en el RGPD. De este modo, estando prohibido su tratamiento con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva.

A este respecto, cabe destacar, además del citado informe 36/2020, referido al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online que posteriormente se comenta, el informe 31/2019 sobre la incorporación de sistemas de reconocimiento facial en los servicios de videovigilancia al amparo del artículo 42 de la Ley de Seguridad Privada o el Informe 97/2020 relativo al Proyecto de Orden de la Ministra de Asuntos Económicos y Transformación Digital sobre los métodos de identificación no presencial para la expedición de certificados electrónicos cualificados. En todos estos casos se concluía que no existía norma legal en el ordenamiento jurídico español que reuniera los requisitos del artículo 9.2.g) del RGPD, por lo que el tratamiento únicamente podría ampararse en el consentimiento de los afectados siempre que quedara garantizado que el mismo es libre.

Analizando y desarrollando los requisitos del artículo 9.2.g) en nuestro Informe 36/2020 señalábamos -FD V-, lo siguiente:

<< La siguiente cuestión que se plantea en la consulta es si el tratamiento de los datos biométricos por los sistemas de reconocimiento facial en los procesos de evaluación online podría ampararse en la existencia de un interés público esencial conforme al artículo 9.2.g) del RGPD:

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Tal y como señalábamos anteriormente, el tratamiento de datos personales necesarios para la prestación del servicio público de educación superior se legitima, con carácter general, en la existencia de un interés público al amparo de lo previsto en el artículo 6.1.e) del RGPD. Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea "esencial", adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Dicho precepto encuentra su precedente en el artículo 8.4 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos: "4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control". No obstante, de su lectura resulta un mayor rigor en la nueva regulación por el RGPD, ya que se sustituye el adjetivo "importantes" por "esencial" y no se permite que la excepción pueda establecerse por las autoridades de control.

En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo (D.L. contra Bulgaria, nº 7472/14, 19 de mayo de 2016, Dragojević contra Croacia, nº 68955/11, 15 de enero de 2015, Peck contra Reino Unido, nº 44647/98, 28 de enero de 2003, Leander contra Suecia, n.o 9248/81, 26 de marzo de 1987, entre otras). Como señala en la última sentencia citada, «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional respecto a las restricciones al derecho fundamental a la protección de datos, que sintetiza en su sentencia 292/2000, de 30 de noviembre, en la que después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en lo siguiente:

Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos

fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional […]". (Fundamento Jurídico 11)

"De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar

una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica […]". (FJ 15).

"Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. […] (FJ 16)".

Asimismo, nuestro Tribunal Constitucional ha tenido ya la ocasión de pronunciarse específicamente sobre el artículo 9.2.g) del RGPD, como consecuencia de la impugnación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido por la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, relativo a la legitimación de la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales, precepto que fue declarado inconstitucional por la Sentencia num. 76/2019 de 22 mayo.

Dicha sentencia analiza, en primer término, el régimen jurídico al que se encuentra sometido el tratamiento de las categorías especiales de datos en el RGPD:

De acuerdo con el apartado 1 del art. 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, del mismo modo que lo está el tratamiento de datos personales que revelen el origen étnico o racial, las convicciones religiosas o filosóficas o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento de todos esos datos cuando concurra alguna de las diez circunstancias allí previstas [letras a) a j)]. Algunas de esas circunstancias tienen un ámbito de aplicación acotado (laboral, social, asociativo, sanitario, judicial, etc.) o responden a una finalidad determinada, por lo que, en sí mismas, delimitan los tratamientos específicos que autorizan como excepción a la regla general. Además, la eficacia habilitante de varios de los supuestos allí previstos está condicionada a que el Derecho de la Unión o el de los Estados miembros las circunstancias recogidas en las letras a), b), g), h), i) y j).

El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de manera expresa el Reglamento General de Protección de Datos ha reconocido a los Estados miembros "margen de maniobra" a la hora de "especificar sus normas", tal como lo califica su considerando 10. Este margen de configuración legislativa se extiende tanto a la determinación de las causas habilitantes para el tratamiento de datos personales especialmente protegidos -es decir, a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, respetando en lo esencial el derecho a la protección de datos- como al establecimiento de "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD]. El Reglamento contiene, por tanto, una obligación concreta de los Estados miembros de establecer tales garantías, en el caso de que habiliten para tratar los datos personales especialmente protegidos.

En relación con el primero de los requisitos exigidos por el artículo 9.2.g), la invocación de un interés público esencial y la necesaria especificación del mismo, el Alto Tribunal recuerda lo señalado en su sentencia 292/2000 en la que se rechazaba que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas, considerando que la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público" :

En la ya citada STC 292/2000 (RTC 2000, 292), en la que también se enjuició una injerencia legislativa en el derecho a la protección de datos personales, rechazamos que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas:

"16. [...] De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.

17. En el caso presente, el empleo por la LOPD (RCL 2018, 1629) en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya

consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE."

Esta argumentación es plenamente trasladable al presente enjuiciamiento. De igual modo, por tanto, debemos concluir que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público". Pues en otro caso el legislador habría trasladado a los partidos políticos -a quienes la disposición impugnada habilita para recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales- el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación.

Tampoco puede aceptarse, por igualmente imprecisa, la finalidad aducida por el abogado del Estado, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular. Por un lado, los partidos políticos son de por sí "cauces necesarios para el funcionamiento del sistema democrático" (por todas, STC 48/2003, de 12 de marzo (RTC 2003, 48), FJ 5); y, por otro lado, todo el funcionamiento del sistema democrático persigue, en último término, la salvaguardia de los fines, valores y bienes constitucionales, pero ello no alcanza a identificar la razón por la cual haya de restringirse el derecho fundamental afectado.

Finalmente, debe precisarse que no es necesario que se pueda sospechar, con mayor o menor fundamento, que la restricción persiga una finalidad inconstitucional, o que los datos que se recopilen y procesen resultarán lesivos para la esfera privada y el ejercicio de los derechos de los particulares. Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Por otro lado, en cuanto a las garantías que debe adoptar el legislador, la citada sentencia núm. 76/2019 de 22 mayo, después de recordar que "A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental", analiza cuál es la norma que debe contener las citadas garantías:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares” (FJ 8).

Por consiguiente, el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

"En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6)."

De la regulación transcrita, que es transposición de la normativa comunitaria, fácilmente puede colegirse que la misma no cumple con los requisitos establecidos en el artículo 9.2.g), ya que el legislador no ha previsto el uso de datos biométricos como una medida proporcional para la identificación de las personas físicas, estableciendo las garantías específicas y adecuadas que se derivan de los mayores riesgos que implica el tratamiento de dichos datos.

Por consiguiente, pretendiéndose en el proyecto el tratamiento de datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, puesto que se trata de datos biométricos dirigidos a la identificación de las personas físicas, es requisito previo que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1, exigiendo el artículo 9.2. de la LOPDGDD que *"Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.*" no existiendo, como se ha indicado, norma legal que habilite dicho tratamiento al amparo del artículo 9.2.g) del RGPD.

Por lo tanto, dicha prohibición únicamente podrá levantarse en aquellos casos en que el afectado preste su consentimiento expreso, al amparo de la letra a) del artículo 9.2. del RGPD, debiendo concurrir todos los demás requisitos para otorgar un consentimiento válido que se recogen en la definición del artículo 4.11 del RGPD: *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o*

una clara acción afirmativa, el tratamiento de datos personales que le conciernen".

Aunque la ausencia de causa que levante la prohibición del tratamiento de categorías especiales de datos determina, por sí sola, la prohibición del tratamiento realizado por Mercadona, y debe señalarse que tampoco concurre una base jurídica que legitimara, en su caso, el mismo al amparo del artículo 6.1. del RGPD sobre la base del interés público.

El concepto de interés público, o el de interés general, que es más frecuentemente utilizado por nuestro texto constitucional, es un concepto jurídico indeterminado con una doble función: dar cobertura legitimadora a la actuación de la Administración y, por otra parte, constituye una de las formas de limitar las potestades administrativas. De este modo, el interés público que, como señala Parejo Alfonso, tiene una clara función directiva del desarrollo normativo (parlamentario o no) del orden constitucional, actúa como criterio delimitador de la actuación de los poderes públicos, por lo que debe, en primer término, ser identificado por el legislador, al objeto de identificar el ámbito en el que se va a desarrollar la actuación de la Administración, sometida al principio de legalidad y a la que le corresponde servir con objetividad a los intereses generales (artículo 103.CE) y, en todo caso, bajo el control de los tribunales, ya que como recuerda la Sentencia del Tribunal Constitucional de 11 de junio de 1984, "No cabe desconocer que la facultad atribuida por la Constitución al Estado para definir el interés general, concepto abierto e indeterminado llamado a ser aplicado a las respectivas materias, puede ser controlada, frente a posibles abusos y a posteriori, por este Tribunal…".

En primer término, debe partirse de que la existencia de un interés público, no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, y el artículo 8 de la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD) que regula el tratamiento de datos basados en una obligación legal y en una misión realizada en interés público o ejercicios de intereses públicos en su artículo 8, en los siguientes términos:

"1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la

adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley."

Por consiguiente, el interés público requiere, en primer lugar, su concreción por parte del legislador, tomando en consideración todos los intereses afectados, al objeto de determinar las restricciones que pueden sufrir los intereses particulares como consecuencia de la presencia de dichos intereses generales, lo que debe hacerse a través de una norma con rango de ley.

Por otro lado, deberían respetarse los demás principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos.

Especialmente, en relación con el principio de minimización de datos, que requiere que sean *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"* (artículo 5.1.c) del RGPD) hay que señalar que el tratamiento de datos de reconocimiento facial implicará el tratamiento a gran escala de categorías especiales de datos sujetos a un régimen reforzado de garantías. Ello es así por el elevado volumen de afectados y clientes de la mercantil, así como por cuanto que dicho tratamiento podría generalizarse al conjunto de mercantiles del mismo u otro sector comercial.

Por último, a mayores de la ostensible falta de legitimación para el tratamiento de datos personales consistente en el reconocimiento facial, el sistema implantado por la mercantil no cumpliría con los requisitos de proporcionalidad exigidos por el Tribunal Constitucional, ya que dentro del triple juicio de proporcionalidad, si bien puede considerarse idóneo para la finalidad propuesta, el mismo no es necesario, al existir medidas alternativas menos intrusivas, ni es estrictamente proporcional, en la medida en que se deriven más beneficios para el interés público que perjuicios sobre otros bienes o valores en conflicto, teniendo en cuenta que se pretende su aplicación masiva e indiscriminada para todos los clientes y resto de afectados, y que en caso de generalizarse implicaría un tratamiento masivo de categorías especiales de datos que alcanzaría a la práctica totalidad de la población, independientemente del nivel de riesgo que represente convirtiéndose la excepción de la posibilidad de tratamiento de datos biométricos en la regla general, en contra de lo pretendido por el RGPD.

Precisamente, la improcedencia de usar estas técnicas con carácter generalizado, así como la ausencia de conexión entre la medida de seguridad con el interés público, persiguiéndose, por contra, intereses privados o

particulares de la mercantil, se recoge en el Auto de la Audiencia Provincial de Barcelona, de fecha 15/02/2021:

"Expuesto lo que precede en los párrafos precedentes, esta Sala considera que la medida peticionada por parte de la entidad, mercantil, MERCADONA S.A, en modo alguno resulta proporcional, necesaria ni asimismo idónea. Los penados en la presente ejecutoria, señores ***A.A.A. y B.B.B.*** *se les impuso una prohibición de acceso a un concreto supermercado de la entidad Mercadona, concretamente ubicado en la calle Frederic Mompou s/n de la localidad de San Boi de Llobregat; no se ha tenido constancia, o al menos del testimonio de particulares remitidos a esta sección, no consta que los mismos quebrantasen la correspondiente prohibición de acceso al centro comercial ni asimismo que éstos sean reincidentes en dicha conducta. Pero es más, esta Sala no puede compartir que con la medida interesada se esté protegiendo el interés público, sino más bien, los intereses privados o particulares de la empresa en cuestión, pues como ya se ha explicitado en los párrafos anteriores, se estarían conculcando las garantías adecuadas en orden a la protección de los derechos y libertades de los interesados, no ya sólo de los que han sido penados y cuya prohibición de acceso les incumbe, sino del resto de personas que acceden al citado supermercado".*

En las alegaciones formuladas al acuerdo de inicio, Mercadona aduce un interés público subyacente en las resoluciones judiciales en las que se adoptan las medidas de seguridad consistentes en el reconocimiento facial del condenado. Afirma la parte reclamada que "*En consecuencia, en vista de la fijación como medida de seguridad en sentencias penales de métodos de reconocimiento facial por parte de los jueces y tribunales, el interés público esgrimido y aceptado como base legal para los condenados, y tribunales, el interés público esgrimido y aceptado como base legal para los condenados, sería lógicamente extensible a estos efectos a las personas no condenadas".*

Pues bien, una cosa es que la adopción de una medida de seguridad pueda tener efectos beneficiosos en la sociedad y que un juez o tribunal penal valore proporcionalmente lo que supone la adopción de la medida de seguridad (entre la restricción de los derechos del condenado y el interés público, ese beneficio social, que se obtiene de la imposición de la medida de seguridad). Y otra cosa es que la preponderancia del interés público (razón por la que se impone la medida de seguridad) legitime el tratamiento de los datos personales del resto de los ciudadanos, de tal forma que todos los ciudadanos sean tratados como condenados, siendo sometidos al mismo tratamiento que aquel sujeto al que se le ha impuesto la medida de seguridad.

En todo caso, la existencia de ese interés público no es una cuestión pacífica. El precitado Auto de la Audiencia Provincial de Barcelona, examinando específicamente la medida de seguridad consistente en el reconocimiento facial,

considera que no hay interés público, sino que, como ya hemos apuntado, se persiguen estrictamente intereses particulares y privados de la mercantil.

En consecuencia, y en atención a las alegaciones formuladas en este momento procedimental por Mercadona, debemos concluir taxativamente que **el tratamiento de datos basados en el reconocimiento facial con fines de identificación no está autorizado de acuerdo con el artículo 9.2.g) del RGPD y, además, carece de base de legitimación al amparo del artículo 6.1 del mismo y es contraria a los principios de necesidad, proporcionalidad y minimización.**

IV

Por otra parte y como ya se ha señalado, procede traer a colación un resumen del contenido del reciente Auto de la Audiencia Provincial de Barcelona de fecha 15/02/2021, Nº de Recurso 840/2020, y Nº de Resolución 72/2021, en el que la mercantil (MERCADONA) ha sido parte interesada en el auto del que trae causa por hechos referidos al tratamiento objeto ahora de análisis. Se reproduce a los efectos de las referencias a la misma constan en la presente Propuesta de Resolución.

El citado Auto señala lo siguiente (El subrayado es de la AEPD):

<< RAZONAMIENTOS JURÍDICOS

PRIMERO.- La mercantil MERCADONA solicita la adopción de la medida, entendiendo que los datos biométricos se obtienen a través de las cámaras de seguridad cuando un sujeto entra en el recinto. Para ello establece como normativa a seguir el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y Consejo de 27 de abril de 2016 relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. La parte apelante entiende el hecho de que, la categoría de dato biométrico se halle reconocida en dicho Reglamento como dato de especial protección, no excluye su uso, siempre que éste se lleve a cabo con todas las medidas de seguridad pertinentes. Se entiende por parte de dicha mercantil que con las medidas de seguridad planteadas no se lesiona en ningún momento la protección de datos de los sujetos, puesto que, aunque se procesen los datos biométricos de todo usuario que entre en uno de los establecimientos, el sistema detecta instantáneamente (en 0,3 segundos) aquellos individuos que han sido condenados con una prohibición de entrada al citado establecimiento a través de la sentencia firme en un proceso judicial; en consecuencia, no permanecerá en el sistema ningún dato biométrico de persona que no haya sido condenada y será inmediatamente borrado y jamás utilizado.

La parte apelante aboga por considerar que la finalidad del Legislador en el desarrollo del reglamento General de Protección de Datos es, no sólo proteger

los derechos de las personas físicas sino también la libre circulación de los datos atendiendo al progreso de la tecnología. Es por ello que, sería de todo punto ineficaz tratar de solventar un problema como lo es el control de aquellos individuos que han sido condenados en sentencia firme con una prohibición de entrada, tratando de mostrar la imagen de dichos individuos a decenas de empleados de establecimientos para que éstos pudieran identificarlos y denunciarlos. Se aduce que, el no aprovechar las ventajas que el progreso nos ofrece, pudiendo hacerlo asegurando la protección de las personas físicas, es condenar al ser humano, así como al desarrollo legislativo español de las últimas décadas.

La parte apelante invoca la idoneidad, necesidad y proporcionalidad de la medida solicitada. En primer lugar es eficaz, pues aborda el problema que se presenta, en orden a conseguir su objetivo que es el de identificar a todo aquel individuo que, a pesar de tener una sentencia firme que le impide la entrada a uno de sus establecimientos, puede vulnerar la decisión del órgano judicial y asimismo los derechos de la propia empresa. Es necesaria, pues es la única medida que afronta el problema y lo soluciona, dado que las anteriores medidas que se han venido tomando, han resultado del todo ineficaces por la imposibilidad de ejercer un control en todos los establecimientos por parte de todos los empleados; y finalmente, resulta proporcional, pues aporta más beneficios para el interés general que perjuicios para el individuo particular en tanto que, no implica ningún tratamiento de los datos biométricos de los sujetos en términos generales, implicando un tratamiento sólo de aquellos individuos que han sido condenados por sentencia firme …

SEGUNDO.- Pues bien, adentrándonos en el fondo de la petición formulada, lo cierto es que se trata de un tema que levanta muchas dudas a nivel jurídico. Debemos recordar que tras la aprobación y entrada en vigor del Reglamento general de protección de datos - de aplicación directa desde mayo de 2018 - el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

** el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*

** el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*

** el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento*

** el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*

** el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

** el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."*

En otras palabras, el Reglamento contempla la obligatoriedad de que el usuario de su consentimiento para procesar sus datos personales. Cuando hablamos de reconocimiento facial, debemos entender hecha la referencia a datos biométricos. El reglamento los define como "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, como imágenes faciales o datos dactiloscópicos". Por si hubiera alguna duda, el apartado 1 del art.9 del citado texto legal dispone que "Queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

Según señala la mercantil MERCADONA S.A, el, sistema "detecta, única y exclusivamente, la entrada de personas con sentencias firmes y medida cautelar de orden de alejamiento en vigor contra Mercadona o contra alguno de sus trabajadoras o trabajadores. Pero, debería preguntarse ante la medida invocada, de dónde sacan imágenes para el reconocimiento facial, con qué consentimiento, sino es más cierto que las personas con una sentencia firme tengan derecho a la privacidad o por qué mantienen una base de datos de fotografías de gente.

El sistema utilizado "realiza la identificación en tiempo real y borra inmediatamente toda la información, únicamente utilizando los resultados positivos para ponerse en contacto con las autoridades en caso de detección. Mercadona alega que no existe un tratamiento de datos y por eso se refiere a 0,3 segundos. Resulta, no obstante, cuanto menos sorprendente que se amparen en la "rapidez". Por muy rápido que sea, existe una violación de la privacidad. Tanto el argumento de la rapidez como el no tratamiento de datos caen por su propio peso.

Estamos claramente ante lo que la Unión Europea ha llamado "autenticación". En el Libro blanco sobre la inteligencia artificial de la Comisión Europea de 19 de febrero de 2020 se establece que "en lo que se refiere al reconocimiento facial,

por "identificación" se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La "autenticación" (o "verificación"), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos.

Se trata de una cuestión compleja. En palabras de la propia AEPD en su informe 36/2020, "atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno). No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados." En el presente caso, es indudable que la utilización de reconocimiento facial en los sistemas de videovigilancia empleados en el ámbito de la seguridad privada implicaría el tratamiento de un dato biométrico dirigido a identificar de una manera unívoca a una persona física, en un proceso de búsqueda de correspondencias uno-a-varios, constituyendo el tratamiento una categoría especial de datos cuyo tratamiento, en principio, se encuentra prohibido por el artículo 9.1 del RGPD

La Agencia Española de Protección de Datos en un informe de 28 de mayo de 2020 dejaba bastante claro el asunto, al concluir que

** Las técnicas de reconocimiento facial con fines de identificación biométrica suponen un tratamiento de categorías especiales de datos para los que el Reglamento exige garantías reforzadas*

** Para tratar categorías especiales de datos con estos fines, la normativa requiere que exista un "interés público esencial" recogido en una norma con rango de ley que no existe actualmente en el ordenamiento jurídico.*

** La Agencia rechaza que la legitimación reconocida para los sistemas de videovigilancia que sólo captan y graban imágenes y sonidos pueda abarcar tecnologías como el reconocimiento facial, de la forma de andar o de la voz.*

Como acertadamente dictamina la Agencia Española de Protección de Datos en el citado informe, para que el reconocimiento facial pudiera tener un mejor amparo legal necesitaría de una ley específica. No existe hoy día norma alguna en nuestro ordenamiento jurídico relativa al reconocimiento facial.

La existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos. Y en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1. Por consiguiente, el empleo de tecnologías de reconocimiento facial en los sistemas de videovigilancia implica el tratamiento de datos biométricos, tal y como los define el artículo 4.14 del RGPD y supone el tratamiento de categorías especiales de datos reguladas en el artículo 9 del RGPD, al tratarse de "datos biométricos dirigidos a identificar de manera unívoca a una persona física". No estamos ante una simple autentificación, sino ante una identificación, por lo que requiere una doble legitimación.

Si bien el artículo 48 del Código Penal establece "la privación del derecho a residir en determinados lugares o acudir a ellos impide al penado residir o acudir al lugar en que haya cometido el delito" y que "el juez o tribunal podrá acordar que el control de estas medidas se realice a través de aquellos medios electrónicos que lo permitan"; esto se produciría asegurando los derechos fundamentales del condenado, es decir, siempre que este hubiera dado su consentimiento. Debemos recordar que los condenados gozan de todos los derechos fundamentales reconocidos en la Constitución, a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria.

TERCERO.- Más allá de la protección de datos, se podría entrar en otras cuestiones propias de la orden de alejamiento. Detrás del formalismo de una orden de alejamiento, hay muchas cuestiones que se deben tener en cuenta para que se cometa el delito, tales como la notificación y requerimiento previo y expreso al condenado, y la vigencia en dicho momento de la orden de alejamiento. Se trata de cuestiones que harto complejo pueda conocer un tercero con seguridad.

No todo vale en materia de Derechos Fundamentales. Estas tecnologías pueden ser realmente intrusivas y requieren de un debate ético y jurídico sosegado, toda vez que pueden tener efectos muy adversos en los valores fundamentales y la integridad humana.

Este análisis es necesario para poder determinar la licitud o no de este tratamiento, especialmente considerando las particularidades de la categoría de datos que se están tratando, datos biométricos y por lo tanto especialmente protegidos. Esto es así al posibilitar las imágenes de los rostros de los interesados la identificación de forma directa, única e inequívoca de todas las personas que sean grabadas. La recogida de imágenes para su posterior reconocimiento ha de cumplir con los criterios y normas contenidas en el Reglamento General de Protección de Datos, de acuerdo con el cual estamos ante un tratamiento intensivo de datos biométricos, que plantea así situaciones de alta incursión en la esfera privada y en el derecho fundamental de protección de datos personales de los interesados. Tanto es así que para poder autorizarse y confirmar la licitud de este tipo de tratamientos, ha de confirmarse la correcta apreciación de aspectos como la naturaleza y el origen de los datos, el modo de desarrollo del mismo y, sobre todo, la finalidad. Estos elementos han de estudiarse junto con los principios informadores de la normativa que nos ocupa, para así poder determinar si las medidas implantadas son proporcionales a la intrusión en la esfera privada de los interesados que suponen.

De acuerdo con la normativa de protección de datos personales, los tratamientos han de respetar siempre un nivel mínimo de proporcionalidad entre la intrusión que pueden suponer estos tratamientos en la esfera privada de las personas y las condiciones y garantías que acompañan a este para poder subsanar los posibles efectos adversos que conlleven. Así, se establece que para aquellos tratamientos que necesiten de datos de categorías especiales, como es el caso de los datos biométricos, se habrá de recabar el consentimiento explícito del interesado como base para la legitimación de los usos y acciones que se vayan a desarrollar con su información. En el caso que nos ocupa, y por el momento, no se está recabando el consentimiento expreso de los interesados, dándose además una situación en la que difícilmente las dos partes, empresa y cliente, puedan considerarse con la misma capacidad de negociar los efectos de otorgar o no el consentimiento, al traducirse esto directamente en la imposibilidad por parte del cliente directo de seguir realizando sus compras en ese supermercado.

El nivel de intrusión en la vida privada de los interesados ha de entrar en el ya mencionado juicio de proporcionalidad, que según la normativa exige por lo tanto la expresión del consentimiento explícito de los interesados. Si este consentimiento no se recabase explícitamente y no se recogiese por métodos de prueba como puede ser un soporte escrito, como está siendo el caso en este tratamiento de reconocimiento facial, esto debe subsanarse con el respaldo de otra base de legitimación lo suficientemente fuerte como para llegar a justificarse

la necesidad de este tratamiento para obtener los fines deseados, como puede ser el mantenimiento del correcto funcionamiento del negocio y la prevención contra robos, hurtos y situaciones de inseguridad para las trabajadores de la empresa. Esta base de legitimación, asegura Mercadona, a través de su petición, es el "interés público" que se recoge de igual forma como legitimación excepcional en la normativa de protección de datos personales. Sin embargo, esto crea dudas a la hora de interpretar su validez o falta de la misma en este caso, al servir realmente la implantación de esta tecnología de mayor forma a un fin privado de la empresa como sería el garantizar la seguridad de sus instalaciones.

En cuanto a la implantación de tecnologías de reconocimiento facial y su uso apropiado para la garantía y el mantenimiento de la seguridad de lugares físicos, la AEPD dictaminó como respuesta a una consulta por parte de una empresa de seguridad privada, dentro del Informe 010308/2019, que sigue siendo a día de hoy insuficiente el marco normativo dedicado a regular este tipo de tratamientos y considerando que será necesaria la aprobación de "una norma con rango de ley que justificara específicamente en qué medida y qué supuestos, la utilización de dichos sistemas respondería a un interés público esencial" para la correcta definición de los requisitos de licitud de este tipo de tratamientos.

… Pero es más, esta Sala no puede compartir que con la medida interesada se esté protegiendo el interés público, sino más bien, los intereses privados o particulares de la empresa en cuestión, pues como ya se ha explicitado en los párrafos anteriores, se estarían conculcando las garantías adecuadas en orden a la protección de los derechos y libertades de los interesados, no ya sólo de los que han sido penados y cuya prohibición de acceso les incumbe, sino del resto de personas que acceden al citado supermercado.

(…) >>

V

Expuesta la doctrina jurídica a aplicar en el presente caso, procede entrar en las cuestiones propias del procedimiento.

De las actuaciones previas de investigación, se concluye que Mercadona realiza un tratamiento de datos personales de datos biométricos (art. 4.14 del RGPD) con la finalidad de identificar unívocamente a una persona concreta entre varias (en adelante uno-a-varios) entando sujetos a las garantías de lo dispuesto en el art. 9 del RGPD.

El tratamiento no sólo se produce en relación con la identificación de condenados penales con imposición de medida de seguridad, consecuencia de la orden de alejamiento impuesta a aquellos en una sentencia penal, sino que

afecta a cualquier persona que entre en uno de sus supermercados (incluidos menores) y a sus empleados.

El tratamiento de datos implantado por Mercadona incluye la captación, el cotejo, conservación y la destrucción -en caso de identificación negativa- (tras 0,3 segundos de su recogida) de la imagen biométrica captada de cualquier persona que entre en el supermercado (captación, cotejo, conservación y destrucción son cuatro formas de tratamiento conforme la definición del art 4 del RGPD).

Mercadona reconoce expresamente que hay tratamiento de datos personales de carácter biométrico, y así, por ejemplo, en la EIPD aportada señala lo siguiente:

"Los datos se conservarán:

• Relativos a la sentencia y la imagen aportada: Durante el tiempo de vigencia de la sentencia firme que imponga la orden de alejamiento.

• Relativos a los negativos de la cámara: El tratamiento será de 0,3 segundos (tiempo entre la captación y el borrado tras la comparativa).

• Relativos a los positivos de la cámara: Duración necesaria para su puesta a disposición a las Fuerzas y Cuerpos de Seguridad del Estado".

Se debe señalar, que la conservación de las imágenes faciales por el breve lapso de tiempo de 0.3 segundos constituye un tratamiento de datos personales biométricos con finalidad de identificación *"uno-a-varios"*, sin que conste acreditada alguna de las excepciones para el tratamiento que señala el artículo 9.2 del RGPD, por lo que no procede, siquiera, aplicar las bases legales indicadas en el artículo 6 del RGPD.

Los datos que se tratan son datos biométricos, cuya definición se encuentra ínsita en el artículo 4.14 del RGPD: *"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, como imágenes faciales o datos dactiloscópicos".*

En este caso concreto supone el tratamiento de categorías especiales de datos reguladas en el artículo 9 del RGPD, al tratarse de *"datos biométricos dirigidos a identificar de manera unívoca a una persona física".* De igual forma, el considerando 51 del RGPD también razona que *"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".*

El informe 36/2020 del Gabinete Jurídico de la AEPD asevera, sin perjuicio de atender a la complejidad de la cuestión y a la imposibilidad de extraer conclusiones generales, que "*los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se*

sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno)", como en el presente caso.

En el mismo sentido, el Comité Europeo de Protección de Datos (en adelante CEPD) considera el empleo de videovigilancia con reconocimiento facial como categoría especial de datos del artículo 9 del RGPD en su "*Guidelines 3/2019 on processing of personal data through video devices*".

VI

Según manifiesta Mercadona, la finalidad del tratamiento facial y de forma remota del tipo *"uno-a-varios"* es controlar el cumplimiento de una medida de seguridad impuesta por sentencia a un condenado en un procedimiento penal en el que Mercadona ha sido parte.

Liga el establecimiento de este sistema de vigilancia con reconocimiento facial al dictado de varias sentencias en las que se impone una medida de seguridad referente al alejamiento de un condenado por un delito leve.

Dicha medida de seguridad consiste en el alejamiento del condenado a un supermercado o varios concretos de Mercadona o de las tiendas de un determinado territorio durante un periodo especificado en la sentencia que no excede en ningún caso de los seis meses (art. 57.3 del CP).

Asimismo, consecuencia de la petición expresa de esta medida de seguridad por parte de Mercadona en el procedimiento penal, la resolución judicial permite establecimiento de medios electrónicos para controlar tales medidas de seguridad conforme dispone el art. 48.4 del CP.

En algunas sentencias se explicita que tales medios electrónicos pueden ser de reconocimiento facial, tratando datos biométricos (*uno-a-varios*). Eso acontece porque Mercadona, si es preguntado sobre la medida de seguridad en el proceso judicial en el que es parte, solicita que la medida de seguridad se ejecute a través de medios electrónicos, concretándolo en medios electrónicos consistentes en el reconocimiento facial.

De la muestra de Sentencias previamente facilitadas por Mercadona en relación con las medidas de seguridad y la utilización de medios electrónicos, se extrae lo siguiente:

(…)

A la vista de la muestra de Sentencias de las que disponemos, tenemos que concluir que:

- La medida de seguridad acordada por el órgano judicial afecta únicamente al condenado y a su esfera jurídica de derechos.

- La medida de seguridad comprende medios electrónicos con reconocimiento facial. Mas no todas las sentencias autorizan a Mercadona a instalar ese sistema "*uno-a-varios*" (identificación), sino que algunas hacen mención genérica a medios electrónicos que permitan el control de esa medida de seguridad sin concretar que sea el reconocimiento facial y, como ya se ha comentado anteriormente, los medios electrónicos de reconocimiento facial no tienen que ser del tipo *"masivos y remotos".*

La utilización de sistemas de identificación biométrica a distancia de forma masiva, indiscriminada y en modo remoto en espacios de acceso público a efectos de la aplicación de una resolución judicial debe tener en cuenta la naturaleza de la situación que da lugar a la posible utilización, en particular la gravedad, probabilidad y magnitud del daño causado en ausencia de la utilización del sistema y también las consecuencias de la utilización del sistema para los derechos, garantías y libertades de todas las personas afectadas, incluidas los condenados.

Además de existir causa de levantamiento de la prohibición general que señala el art 9.1 del RGPD, el uso de sistemas de identificación biométrica de forma masiva *("uno-a-varios"*), indiscriminada y en modo remoto en espacios de acceso público a efectos de la aplicación de una resolución judicial debería cumplir, además, las salvaguardias y condiciones necesarias y proporcionadas en relación con el uso, también en lo que respecta a las limitaciones temporales, geográficas y personales de los afectados.

En el presente caso, las resoluciones judiciales previamente facilitadas por Mercadona no concretan el modo de llevar a cabo el control de acceso a los supermercados, y las garantías, derechos y libertades de los afectados no pueden quedar al albur de interpretación y decisión unilateral sobre el alcance de las resoluciones judiciales sobre el impacto sobre los afectados (condenados, empleados y clientes, incluido menores) de tales tratamientos por parte de la mercantil responsable (Mercadona).

Respecto al reconocimiento facial masivo y remoto (*"uno-a-varios"*), el libro Blanco sobre la Inteligencia Artificial indica qué es la identificación biométrica remota, en los siguientes términos:

"La identificación biométrica remota debe distinguirse de la autenticación biométrica (esta última es un procedimiento de seguridad que se basa en las características biológicas exclusivas de una persona para comprobar que es quien dice ser). La identificación biométrica remota consiste en determinar la identidad de varias personas con la ayuda de identificadores biométricos (huellas dactilares, imágenes faciales, iris, patrones vasculares, etc.) a distancia, en un espacio público y de manera continuada o sostenida contrastándolos con datos almacenados en una base de datos".

El tratamiento ahora analizado se caracteriza por:

- Utilizar datos biométricos, que son categorías especiales de datos del art. 9 del RGPD (*uno-a-varios*) sobre los que recae una prohibición general de utilización, a salvo excepción prevista en la propia norma. Este tratamiento es, por tanto, excepcional.

- Se produce a distancia en un espacio de acceso al público en general.

- Es un tratamiento continuado que contrasta los datos recogidos con otros almacenados en una base de datos.

- Es un tratamiento automático.

- Es de riesgo extremadamente elevado (inaceptable) al poder derivar en una vigilancia masiva e indiscriminada.

- Como podemos comprobar el tratamiento de datos utilizando identificación biométrica remota es automático, y el dato biométrico se capta (se trata) automáticamente; por ello se considera de riesgo extremadamente elevado (inaceptable) este tratamiento de datos.

A mayor abundamiento, no podemos obviar que la implantación de sistemas de "identificación" biométrica remota del tipo "*uno-a-varios*" (categoría especial de datos personales, art 9 RGPD) recoge mucha más información que otro tipo de tratamiento y, además, de forma involuntaria y sin conocimiento ni consentimiento, al establecer pautas y usar algoritmos prefijados que determinan la elaboración de un determinado patrón (matriz) característico de la imagen tratada de cada persona afectada.

En el tratamiento ahora analizado se observa claramente un sistema de reconocimiento facial indiscriminado y masivo ya que *"dependiendo de los datos biométricos recogidos, pueden derivarse datos del sujeto como su raza o género (incluso de las huellas dactilares), su estado emocional, enfermedades, taras y características genéticas, consumos de sustancias, etc. Al estar implícita, el usuario no puede impedir la recogida de dicha información suplementaria"* -Nota de la AEPD sobre los "*14 equívocos con relación a la identificación y autenticación biométrica"-.* Este exceso de datos tratados también vulnera el principio de minimización dispuesto en el art. 5.1.c) del RGPD.

Es Mercadona (en calidad de responsable del tratamiento) quien ha decidido implantar un sistema de estas características del que no disponía anteriormente, consecuencia de su participación en un proceso judicial penal en el que ha sido parte y ha solicitado que se le autorizara la medida de seguridad concreta consistente en la utilización de un sistema de reconocimiento facial.

Esto nos pone de manifiesto que Mercadona ha solicitado en el proceso judicial la medida de seguridad ligada al reconocimiento facial, antes de realizar una EIPD, antes de valorar si podía llevar a cabo el tratamiento conforme a la

normativa de protección de datos y antes de evaluar los riegos de tal tratamiento de datos. En este sentido, se insiste, no consta en esta AEPD que haya realizado la consulta previa a la que se refiere el art. 36 del RGPD, toda vez que el tratamiento implantado no solo entraña un riesgo extremadamente elevado (inaceptable) de menoscabo de derechos y libertades a los clientes y trabajadores de Mercadona, sino que lo prohíbe el art. 9.1 del RGPD. En este sentido, también se debe señalar que en el análisis de riesgos realizado previamente debió resultar el tratamiento como riesgo inaceptable y, en consecuencia, ser evitado.

Mercadona ha solicitado la adopción de la medida de seguridad en el procedimiento penal y, una vez acordada, la hace valer para justificar la excepción del art. 9.2 del RGPD; esto es, ha preconstituido la legitimación necesaria para llevar a cabo el tratamiento de datos biométricos de forma masiva y remota de *"uno-a-varios*". Recordemos que esta medida de seguridad se dicta únicamente respecto del condenado y que sólo afecta a la limitación de sus derechos en los términos de la resolución judicial sin afectar a terceros ajenos, como pueden ser los clientes y trabajadores de Mercadona. Se ha de realizar el juicio de proporcionalidad antes de solicitar esta medida ante el órgano judicial, como se verá más adelante.

VII

Empezamos por examinar si Mercadona tiene **legitimación** para efectuar este tipo tratamiento en las condiciones citadas.

Mercadona asevera que ostenta legitimación basada en el interés público (art. 6.1.e) del RGPD) con fines de videovigilancia y que concurre previamente la excepción del art. 9.2.f) del RGPD que le permite el tratamiento de datos biométricos de categoría especial, esto es, la circunstancia de que el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones.

La base legal para el tratamiento alegada por la mercantil parte del previo levantamiento de la prohibición general que impone el art. 9.1 del RGPD a través de la aplicación del art. 9.2.f) del RGPD y, posteriormente, se referencia al art. 6.1.e) RGPD. En primer lugar, la excepción del art. 9.2.f) del RGPD no concurre para los potenciales clientes en el tratamiento ahora analizado (ni para los trabajadores) según el informe de la AEPD 010308/2019 ya mencionado y, en segundo lugar, la base legal dispuesta en el art. 6.1.b) RGPD tampoco es válida para los empleados toda vez que se trata de un tratamiento al margen del sistema de videovigilancia.

Como hemos apuntado antes, podemos observar en cuanto a la legitimación, que en el tratamiento examinado hay tres tipologías de interesados afectados por éste. Por una parte, el tratamiento de datos biométricos de un condenado por la imposición de una medida de seguridad de alejamiento en una sentencia penal; por el otro, el tratamiento de datos biométricos de los potenciales clientes

de Mercadona; por último, el tratamiento de los datos biométricos de los propios empleados de Mercadona.

- Legitimación en cuanto a los datos de un condenado.

Mercadona fundamenta el tratamiento en la excepción prevista en el art. 9.2.f) del RGPD para considerar que se encuentran legitimados para llevar a cabo el tratamiento de datos biométricos. El art. 9.2.f) del RGPD levanta la prohibición general prevista en el art. 9.1 del RGPD cuando *"el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial".*

Según el Informe de esta AEPD de referencia 0098/2020, se concluye que:

(i) el RGPD menciona separadamente las reclamaciones extrajudiciales de diversa naturaleza y las administrativas, y por otra parte, aquellas reclamaciones que se promuevan a través de los órganos judiciales.

(ii) debe entenderse el levantamiento de la prohibición de tratamiento de categorías especiales de datos como excepcional, subsidiario y la interpretación de su aplicación debe ser restrictiva, de acuerdo con la especial protección de la que son acreedores este tipo de datos derivada de su naturaleza jurídica.

(iii) el derecho nacional o de la Unión Europea que regule estos tratamientos debe ofrecer garantías suficientes para proteger los derechos de los afectados.

(iv) es que si bien el RGPD establece unos supuestos que excepcionan la prohibición de tratamiento de categorías especiales de datos, a través del derecho de los Estados miembros se pueden introducirse regulaciones ad hoc a fin de adaptar la realidad de los sectores implicados para garantizar una protección efectiva de los derechos de los ciudadanos de la unión.

El citado informe añade que, con carácter general, los supuestos que levantan la prohibición general de tratamiento previstos en el artículo 9.2 RGPD, únicamente sirven a tal fin, es decir, actúan como excepciones a lo dispuesto en el apartado 1, lo que no significa que siempre que se dé alguno de ellos, el tratamiento pueda o deba llevarse a cabo, pues deben cumplirse las restantes obligaciones que se derivan del propio RGPD. Es decir, la mera existencia de una reclamación al amparo del artículo 9.2 f) RGPD, no legitima por si sola, el tratamiento de categorías especiales de datos, sino que debe ir acompañada de otros elementos, que no constan, que hagan que el tratamiento sea conforme al RGPD.

El tratamiento de datos biométricos (*"uno-a-varios"*), en este caso, podría producirse si es necesario para la formulación o el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial. No obstante, en términos estrictos, conforme a la literalidad de la norma jurídica, y para el supuesto ahora examinado, la formulación, el ejercicio o la defensa de reclamaciones ya se han efectuado, pues de la denuncia formulada por Mercadona se deriva la situación en la que ahora nos encontramos.

Mas, podríamos entender que la imposición en una sentencia firme de una medida de seguridad es consecuencia y continuación de la reclamación interpuesta, pudiendo ser así incluida esta medida derivada de la reclamación en el marco del precepto transcrito. Ahora bien, en todo caso, el tratamiento de datos biométricos para la formulación, ejercicio o defensa de reclamaciones quedaría restringido a los datos biométricos de la persona demandada y en los estrictos términos y alcance de la resolución judicial y no de terceros totalmente ajenos al procedimiento y menos aún de la libre interpretación unilateral por la mercantil del alcance de la resolución judicial.

El considerando 52 del RGPD, respecto de la prohibición del tratamiento de categorías especiales de datos personales, autoriza las excepciones *"siempre que se den las garantías adecuadas",* indicando que *"Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial".*

Al tratarse de una autorización excepcional, que requiere a mayores -en caso de poder ser aplicada-el establecimiento de garantías adecuadas, la interpretación que se le otorgue ha de ser restrictiva. Así lo prevé el considerando 51 del RGPD que recoge el carácter restrictivo con el que se puede admitir el tratamiento de estos datos, cuando afirma que "*Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento";* esta interpretación es recogida de forma sistemática por la AEPD en sus resoluciones -por todas, el PS/00145/2019-.

Traigamos a colación el art. 10 del RGPD. Este precepto permite el tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad, en relación con los datos personales concernidos en tales condenas, infracciones o medidas de seguridad. En nuestro caso, y con la dicción del artículo únicamente afectaría a los datos personales del condenado. Y en relación con la excepción del art. 9 del RGPD, a los datos biométricos del condenado.

A mayores, requiere, o bien que se ejecute bajo la supervisión de las autoridades públicas o con autorización el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.

En este supuesto, la supervisión de la Autoridad Judicial se produce si el condenado violenta las medidas de seguridad. La Autoridad Judicial ni revisa ni ha revisado el sistema de reconocimiento facial implantado con carácter general, ni la afectación de la implantación de tal sistema a los derechos y libertades del resto de los ciudadanos (clientes y trabajadores de Mercadona).

De hecho, si la medida de seguridad se aplicara directamente por el órgano judicial no podría hacerla extensiva a otros sujetos que no fueran el condenado o terceros emplazados en el procedimiento y afectados directamente por la medida de seguridad. En consecuencia, lo que no puede hacer un juez en cumplimiento de sus propias medidas, mucho menos un particular que colabore.

Respecto al tratamiento de datos biométricos de forma masiva y remota *"uno-a-varios"* de un condenado por la imposición de una medida de seguridad de alejamiento en una sentencia penal, la mercantil manifiesta que la base jurídica del tratamiento sería la del art. 6.1.e) del RGPD, olvidando así la necesidad del levantamiento previo de la prohibición general que impone el art. 9.1 del RGPD.

Mercadona asevera sobre la medida de seguridad que *"Esta legitimación, si bien no necesita una habilitación legal o una determinación concreta a nivel normativo, sí debe encuadrarse dentro del sistema procesal español".*

Sin embargo, frente a tal afirmación, lo cierto es que el art. 8 de la LOPDGDD es taxativo en el sentido de que "*El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley"*. En consecuencia, es preceptiva habilitación legal para que tal base jurídica surta efectos.

Pues bien, en realidad es que la base jurídica contenida en el art. 6.1.e) del RGPD podría legitimar el tratamiento de datos del condenado respecto de una medida de seguridad concreta (siempre que se disponga de una habilitación entre las del art. 9.2 del RGPD), entendiendo que llevan a cabo una misión en interés público, por mandato del órgano judicial que tiene atribuida por mor de la Ley potestad para ello (art 17 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial). No obstante, como ya se ha señalado, tampoco consta que la medida de seguridad sea un interés público esencial ya que lo que protegería sería un interés privado de la mercantil.

En este sentido el GT29 en su Dictamen 06/2014 sobre el concepto de interés público del responsable del tratamiento de los datos en virtud del art. 7 de la Directiva 95/46/CE, examina qué se entiende por misión en interés público, consignando que *"El artículo 7, letra e), cubre dos situaciones y es pertinente tanto para el sector público como para el sector privado. En primer lugar, comprende situaciones en las que el mismo responsable del tratamiento tiene*

una potestad pública o una misión de interés público (pero no necesariamente una obligación jurídica de tratar los datos) y el tratamiento es necesario para el ejercicio de dicha potestad o para la ejecución de dicha misión".

"No obstante, el tratamiento debe ser «necesario para el cumplimiento de una misión de interés público». Alternativamente, se debe haber conferido un poder oficial bien al responsable del tratamiento bien a la tercera parte a la que este comunica los datos y el tratamiento de datos debe ser necesario para el ejercicio de dicha potestad. También resulta importante poner de relieve que este poder oficial o misión de interés público deberán conferirse o atribuirse normalmente mediante leyes ordinarias u otra normativa jurídica. Si el tratamiento conlleva una invasión de la privacidad o si este se exige de otro modo en virtud de la legislación nacional para garantizar la protección de las personas afectadas, la base jurídica deberá ser lo suficientemente específica y precisa a la hora de definir el tipo de tratamiento de datos que puede permitirse".

En refrendo de lo afirmado, sólo tenemos que examinar el art. 10 del RGPD citado por la mercantil: *"El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas".*

En nuestro caso, esa legitimación que ahora encontramos basada en la misión en interés público y la colaboración con la justicia, sería distinta de la del interés público empleada por la mercantil que legitima, vía el art. 6.1.e) del RGPD y el art. 22 de la LOPDGDD la videovigilancia, especialmente porque, como ya hemos indicado, en algunas de las sentencias examinadas se habla genéricamente de la utilización de medios electrónicos para controlar la medida de seguridad, sin concretar de forma "*específica y precisa a la hora de definir el tipo de tratamiento de datos que puede permitirse"*.

- Legitimación en cuanto a los datos de los posibles clientes de Mercadona.

La mercantil esgrime la excepción prevista en el art. 9.2.f) del RGPD antes citada para proceder al tratamiento de los datos biométricos *"uno-a-varios"* de los clientes de Mercadona.

Como hemos indicado anteriormente, la excepción prevista en el art. 9.2.f) del RGPD, relativa a la formulación, el ejercicio o la defensa de reclamaciones ha de ser interpretada de forma restrictiva y en sus propios términos, por su excepcionalidad en atención a la prohibición contenida en el apartado primero del art. 9 del RGPD.

También hemos significado que la comprensión adecuada del art. 9.2.f) del RGPD limita, conforme a una interpretación literal, sistemática y teleológica de la norma, la utilización de categorías especiales de datos personales a supuestos en los que el tratamiento de tales datos es necesario para la formulación, el ejercicio o la defensa de reclamaciones. Así, podríamos entender que el concepto "formulación", "ejercicio" y "defensa" pudiera no sólo acoger a la formulación, ejercicio o defensa misma de respecto de una reclamación, sino que pudiera extenderse a la ejecución de la resolución obtenida tras la formulación, ejercicio o defensa de la reclamación, en el marco de la tutela judicial efectiva.

Trasladémoslo al derecho interno y al concreto proceso de "reclamación", puesto que la excepción no es indiferente al funcionamiento del sistema procesal español.

En el supuesto examinado, el tratamiento consistente en el reconocimiento facial, que, recordemos, ha sido elegido por la mercantil, deriva de la imposición de una medida de seguridad a una persona concreta, conforme a una sentencia judicial favorable obtenida por Mercadona. Tratándose, en nuestro caso de un procedimiento judicial penal y constriñéndolo a las características y elementos definitorios del mismo fijado en el ordenamiento jurídico, afectaría únicamente a las partes en el procedimiento (incluyendo, en su caso, a un tercero cuando haya sido emplazado por el órgano judicial para que pueda defender lo que a su derecho incumba), sin que pueda extender sus efectos a terceros ajenos al mismo.

El órgano judicial al adoptar la medida de seguridad pondera, como sólo puede ser, la afectación de la medida de seguridad en los Derechos Fundamentales del condenado. El órgano judicial no examina la afectación de la medida de seguridad en terceros ajenos al procedimiento ni valora, ni pondera qué incidencia produce tal medida de seguridad en Derechos Fundamentales de estos últimos (intimidad y protección de datos de carácter personal, entre otros). Y ello porque tal decisión en nada les atañe.

Una sentencia penal entre partes no habilita *per se* el tratamiento de datos biométricos de forma masiva *"uno-a-varios"*, remota e indiscriminada, afectando a un importante e indeterminado grupo de población, incluido menores de edad. Amén de la total desproporción que supone la implantación de este sistema, de la que hablaremos posteriormente. Extrapolándolo, llegaríamos al absurdo que, mediante la imposición de una medida de seguridad para un sujeto o sujetos concretos en una sentencia judicial, o incluso en una resolución administrativa, podría habilitarse el establecimiento de un tratamiento de reconocimiento facial masivo, lo que violentaría la letra y el espíritu del RGPD.

La excepción prevista en el art. 9.2.f) del RGPD, por la afectación a las categorías de datos sensibles y los riesgos inherentes al tratamiento, debe

extremar el cuidado en su interpretación restrictiva cuando afecta a una pluralidad indeterminada y masiva de personas, y que son totalmente ajenas a la resolución judicial dictada.

Tan sólo habilita a las partes en la reclamación a utilizar los datos biométricos precisos para ejercer la reclamación misma, restringiéndolo a la afectación concreta de personas a las que se refiere el proceso y la subsiguiente resolución judicial. Los datos biométricos de cualquier potencial cliente de Mercadona no han sido necesarios para formular la querella. Sin embargo, este tratamiento de reconocimiento facial implantado por Mercadona, visto en su conjunto directamente afecta a todos los potenciales clientes de Mercadona, siendo estrictamente ajeno a la reclamación misma.

En conclusión, el art. 9.2.f) del RGPD podría levantar la prohibición, pero restringiendo tal legitimación a una sentencia concreta y con alcance expreso en la misma y en relación con las concretas medidas de seguridad impuestas, respecto de las personas mencionadas en ella, y para un ámbito territorial (un territorio, o uno o varios supermercados) y temporal limitado. Esto es, sólo respecto del condenado.

Sin embargo, el sistema de reconocimiento facial implantado por Mercadona, que carece de legitimación con base en el art. 9.1 del RGPD, es altamente intrusivo, afectando de manera indiscriminada a una cantidad indeterminada de ciudadanos. Se les impone de manera indirecta una medida de seguridad de naturaleza penal.

Genera un efecto perverso, pues finalmente con esos ***NÚM.2 procesos judiciales que dicen que interponen anualmente en todo el territorio español, prácticamente en todos los supermercados tendrían activado un sistema de reconocimiento facial, monitoreando a todos los clientes de Mercadona, habituales o no. Se traduciría en la práctica en el establecimiento a gran escala de un sistema de reconocimiento facial altamente intrusivo en los derechos y libertades de los afectados. Comporta un riesgo extremadamente elevado no aceptable.

En este sentido, en la “Guidelines on Facial Recognition” de enero de 2021 del “Consultative Committee of the Convention for the protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108”, se afirma que las entidades privadas no pueden desarrollar sistemas de reconocimiento facial en ambientes incontrolados como centros comerciales, especialmente para identificar personas de interés para finalidades de seguridad: “*Private entities shall not deploy facial recognition technologies in uncontrolled environments such as shopping malls, especially to identify persons of interest, for marketing purposes or for private security purposes*”.

(“*Las entidades privadas no utilizarán tecnologías de reconocimiento facial en entornos incontrolados como los centros comerciales, especialmente para*

identificar a las personas de interés, con fines de comercialización o con fines de seguridad privada". La traducción es de la AEPD).

Sobre los derechos, la citada Guía aclara que pueden ser restringidos sólo cuando lo establezca una Ley, esto es, que ahora, en nuestro supuesto, los derechos de los interesados no pueden ser restringidos: "*These rights can be restricted but only when such restriction is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for specific legitimate purposes (such as law enforcement purposes), according to Article 11 of Convention 108+*".

("*Estos derechos pueden restringirse pero solo cuando esa restricción está prevista por la ley, respeta la esencia de los derechos y libertades fundamentales y constituye una medida necesaria y proporcionada en una sociedad democrática para fines legítimos específicos (como fines de aplicación de la ley), de conformidad con el artículo 11 de la Convención 108+*". (La traducción es de la AEPD).

Por otro lado, debemos de examinar si la mercantil tiene legitimación para el tratamiento de los datos biométricos de carácter especial ("*uno-a-varios"*) de los potenciales clientes de Mercadona.

Al margen de la prohibición general que impuesta en el art. 9.1 del RGPD que afecta a los datos biométricos de carácter especial, vamos a volver de nuevo al art. 6.1.e) del RGPD citado por la mercantil. La base jurídica -si no fueran datos biométricos de carácter especial- sería la misma, el interés público, pero en este caso no está basada en la competencia de un órgano judicial que para la ejecución de una media de seguridad permita a una de las partes en el proceso penal el tratamiento de datos personales del condenado (misión en interés público). Es obvio que los ciudadanos, con carácter general, posibles clientes de Mercadona no han sido parte del procedimiento, no se citan en la sentencia, ni han sido considerados a los efectos de implementar medio electrónico alguno, ni son afectados por la misma.

El interés público podría aparentemente encontrarse en este caso ínsito en un tratamiento en la videovigilancia. El artículo 22 de la LOPDGDD regula los tratamientos con fines de videovigilancia cuya legitimación se encuentra, tal y como señala la Exposición de Motivos del texto legal referenciado, en la existencia de una finalidad de interés público incardinable en el artículo 6.1.e) del RGPD, al tener por finalidad *"preservar la seguridad de las personas y bienes, así como de sus instalaciones",* un objetivo que sobrepasa los meros intereses legítimos de un particular.

En el ámbito de la seguridad privada, dicha regulación debe completarse con lo dispuesto en su normativa específica, esto es la Ley de Seguridad Privada (LSP), en cuyo artículo 42 regula los servicios de videovigilancia. Establece que

"Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales".

En el supuesto examinado, la videovigilancia se va a llevar a cabo por una empresa de seguridad privada.

Ahora bien, tal y como se razona en el Informe 31/2019 del Gabinete Jurídico (entrada: 010308/2019) de la AEPD *"los tratamientos de videovigilancia regulados en la LOPDGDD y en la LSP, se refieren exclusivamente a los tratamientos dirigidos a captar y grabar imágenes y sonidos, pero no incluyen los tratamientos de reconocimiento facial, que es un tratamiento radicalmente distinto al incorporar un dato biométrico, como recuerda el propio RGPD en su Considerando 51 al señalar 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.*

Por consiguiente, la incorporación a los sistemas de videovigilancia, dirigidos a la captación y grabación de imágenes y sonidos, de aplicaciones de reconocimiento facial va a implicar el tratamiento de datos biométricos, respecto de los cuales las autoridades de protección de datos venían advirtiendo de los riesgos que implican para los derechos de las personas".

Recoge el precitado informe varios documentos del Grupo de Trabajo del artículo 29, tales como el Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, el documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003 o el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012, en los que se expone la diferencia entre los sistemas de videovigilancia convencionales y el reconocimiento facial, indicándose asimismo un conjunto variopinto de riesgos importantes y significativos como el de discriminación, como el hecho de que el tratamiento pueda realizarse sin conocimiento del interesado, la posible generalización de su uso y los errores que pueden producirse.

De conformidad con lo expuesto, la base jurídica comprendida en el art. 6.1.e) del RGPD en relación con el art. 22 de la LOPDGDD sería suficiente para llevar a cabo un tratamiento de videovigilancia ordinario (no de carácter especial). Pero no sería bastante para un sistema de reconocimiento facial en los términos

expuestos, esto es, un tratamiento radicalmente distinto al utilizar datos biométricos de forma masiva y remota del tipo *"uno-a-varios",* sin que quede levantada previamente la prohibición establecida en el art. 9.1 de RGPD. Por lo tanto, se tendría que determinar cuál es la base jurídica precisa para llevar a cabo un tratamiento de reconocimiento facial *("uno-a-varios"*), así como los requerimientos legales precisos para ello.

El Informe 31/2019 del Gabinete Jurídico (entrada: 010308/2019) considera que *"la regulación actual se considera insuficiente para permitir la utilización de técnicas de reconocimiento facial en sistemas de videovigilancia empleados por la seguridad privada (…) siendo necesario que se aprobara una norma con rango de ley que justificara específicamente en qué medida y en qué supuestos, la utilización de dichos sistemas respondería a un interés público esencial, definiendo dicha norma legal, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos".*

Concluye el informe que la utilización de sistemas de reconocimiento facial de los sistemas de videovigilancia empleados por la seguridad privada es desproporcionada, en atención a la intrusión y los altos riesgos no aceptables que supone para los derechos fundamentales de los ciudadanos. Al menos cuando se le trata de configurar la excepción del art. 9.2.g) del RGPD como un interés público esencial, precisando la necesidad de regulación legal específica (art 8.2 LOPDGDD). El Informe Jurídico 010308/2019 de la AEPD señala *"… tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea "esencial", adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados."*

Por todo ello, podemos vislumbrar en consecuencia que, en atención a las especiales características del tratamiento de datos que se efectúa (con riesgo extremadamente elevado inaceptable), no nos encontramos ante lo que podríamos definir como un sistema de videovigilancia corriente, ordinario; este sistema implantado que incorpora aplicaciones de reconocimiento facial tiene su propia entidad y virtualidad, pues trata datos biométricos dirigidos a identificar de una manera unívoca a una persona física mediante el reconocimiento facial, en un proceso de búsqueda de correspondencias *"uno-a-varios"* (el condenado y el resto personas que accedan a los supermercados, ya sean potenciales clientes o empleados) y de forma masiva y remota. Así lo ha manifestado el CEPD.

- Legitimación en cuanto a los datos de los trabajadores de Mercadona.

A mayor abundamiento, tenemos que significar que hay otro colectivo afectado por el establecimiento de reconocimiento facial. Nos referimos a los trabajadores de la mercantil, que también son identificados biométricamente al entrar a los supermercados.

Pues bien, el tratamiento de los datos biométricos de los empleados de Mercadona mediante un sistema de reconocimiento facial como el analizado tampoco se encuentra amparado por la excepción del art. 9.2.f) del RGPD.

El art. 20.3 del Estatuto de los Trabajadores y las excepciones del art. 9.2.f) y 9.2.h) del RGPD no sostienen la legitimación del tratamiento para la finalidad pretendida, que es la de hacer efectiva una medida de seguridad derivada de un procedimiento judicial entre Mercadona y una persona que ha hurtado productos o producidos daños en sus instalaciones (Mercadona no ostenta la legitimación para defender agresiones y daños personales y patrimoniales sufridos por sus empleados, que corresponde a estos últimos).

Resulta de plena aplicación para los empleados de Mercadona, lo que hemos indicado en el apartado anterior sobre el uso de la base jurídica del art. 6.1.e) del RGPD. Esta base jurídica, sin que se cumpla la excepción del art. 9.2.f), no es posible para legitimar el tratamiento de los datos biométricos de los empleados de Mercadona.

Hemos de significar que el colectivo de los trabajadores del supermercado no ha sido considerado por el responsable del tratamiento a la hora de valorar y elegir el tratamiento consistente en un sistema de reconocimiento facial que respete y pondere los riesgos en la vulneración de derechos y libertades de este colectivo.

Así se puede comprobar del examen del expediente administrativo, puesto que, en la EIPD, las categorías de interesados son *"Sujetos que accedan a los centros de MERCADONA; Sujetos con condena firme",* página 6.

También puede observar que en la EIPD se examina la amenaza consistente en que "*Se realiza un tratamiento que implica una monitorización sistemática de los titulares sin que estos puedan ser conscientes de la actividad y/o alcance del mismo […] El sistema de reconocimiento facial puede evaluar sistemáticamente (aunque siempre con intervención humana) las imágenes de las personas que accedan a centros de MERCADONA",* página 16.

Los empleados no constan como sujetos diferenciados, no son tenidos en cuenta como un colectivo específico afectado por riesgos propios. Sin embargo, están siendo detectados por el sistema de reconocimiento facial cada vez que entran y salen por la puerta del supermercado, ya sea para entrar a trabajar o en el desempeño de sus funciones.

Desde luego que los empleados no pueden ser incluidos entre los “sujetos que acceden a los centros del MERCADONA”; estos últimos son todos los potenciales clientes y es obvio porque sus riesgos, junto con los eventuales riesgos al condenado, son los únicos que se examinan a lo largo de la EIPD. No se examinan los riesgos específicos y singulares de los trabajadores. En este sentido, hay que señalar que la EIPD aportada es incorrecta. En este sentido, se trae a colación lo dispuesto en el dictamen WP248 sobre evaluación de impacto del GT29: *“… En virtud del RGPD, el incumplimiento de los requisitos de la EIPD puede dar lugar a la imposición de multas por parte de la autoridad de control competente. No llevar a cabo una EIPD cuando el tratamiento requiera una evaluación de este tipo (artículo 35, apartados 1, 3 y 4), llevar a cabo una EIPD de forma incorrecta (artículo 35, apartados 2, 7, 8 y 9) o no consultar a la autoridad de control competente cuando sea necesario [artículo 36, apartado 3, letra e)] puede dar lugar a una multa administrativa de hasta 10 millones EUR o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía …)”*.

Así, el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del GT29 (adoptado el 8 de junio de 2017) establece que “*aunque el uso de estas tecnologías puede ser útil para detectar o prevenir la pérdida de propiedad intelectual y material de la empresa, mejorando la productividad de los trabajadores y protegiendo los datos personales de los que se encarga el responsable del tratamiento, también plantea importantes retos en materia de privacidad y protección de datos. Por consiguiente, se requiere una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores”.*

Por ello, “*Independientemente de la base jurídica de dicho tratamiento, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo. Esto puede formar parte de una evaluación de impacto relativa a la protección de datos (EIPD)”.*

En el supuesto examinado no se ha realizado prueba de proporcionalidad alguna en relación a los riesgos y a la afectación de los derechos y libertades de los empleados. Esto se deduce claramente del hecho indubitado de que ni tan siquiera son citados en la EIPD que consta en el expediente administrativo como un colectivo específico a valorar.

Tal y como afirma el GT29 en el Dictamen precitado “*El tratamiento de datos en el trabajo debe ser una respuesta proporcionada a los riesgos a los que se enfrenta un empresario*”. En el supuesto examinado no resulta proporcionada

desde el momento en que ni tan siquiera el colectivo ha sido considerado a la hora de determinar los riesgos.

Resulta ineludible ponderar si el tratamiento (de los datos biométricos de los empleados) es proporcionado, cuáles son los riesgos y considerarlos en todo caso en la EIPD. El Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del GT29 pone de relieve la necesidad de su realización "*en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas".* Y ello porque "*Las tecnologías modernas permiten que los trabajadores puedan ser objeto de seguimiento a lo largo del tiempo, en los lugares de trabajo y en sus hogares, a través de muchos dispositivos diferentes, como teléfonos inteligentes, ordenadores de mesa, tabletas, vehículos y tecnología ponible. Si el tratamiento no tiene límites y no es transparente, existe un alto riesgo de que el interés legítimo de los empresarios en la mejora de la eficiencia y protección de los activos de la empresa se convierta en un control injustificado e intrusivo".*

En todo caso, el tratamiento de datos biométricos de los empleados del supermercado supone un control indirecto de estos (en el sentido de que la finalidad del tratamiento se dirige a identificar unívocamente al condenando). Control a todo punto.

Si hay que estar a la previsión del art. 89 de la LOPDGDD a los efectos de respetar la intimidad de los trabajadores frente al uso de dispositivos de videovigilancia, mucho más si nos encontramos ante un tratamiento diferenciado de la videovigilancia, más invasivo, con riesgos más específicos y mayores, que conlleva la utilización de datos biométricos. Si tal precepto impone la medida de información previa a los empleados y a sus representantes, también deberá procederse en el supuesto examinado por mor de la transparencia. La información ha de ser suministrada, en todo caso a los representantes de los trabajadores y a estos últimos en virtud del art. 13 del RGPD.

En el supuesto de Mercadona, en atención al número de trabajadores de que disponen, el órgano de representación será el Comité de Empresa, dado que el art. 63 del Estatuto de los Trabajadores establece que "*El comité de empresa es el órgano representativo y colegiado del conjunto de los trabajadores en la empresa o centro de trabajo para la defensa de sus intereses, constituyéndose en cada centro de trabajo cuyo censo sea de cincuenta o más trabajadores".*

Hay que señalar, a título informativo, la reciente modificación del artículo 64.4.d) de la *Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre* (Estatuto de los Trabajadores), que queda redactado de la siguiente manera en consonancia con el artículo 13.2.f) del RGPD:

<<d) Ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a

la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles.>>

Amén de las obligaciones de información y transparencia derivadas de la protección de datos, los representantes de los trabajadores tienen derecho a ser informados y consultados en determinados casos previstos normativamente.

El art. 64 del Estatuto de los Trabajadores (a fecha de los hechos), sobre este particular, indica que "*El comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores, así como sobre la situación de la empresa y la evolución del empleo en la misma, en los términos previstos en este artículo.*

Se entiende por información la transmisión de datos por el empresario al comité de empresa, a fin de que este tenga conocimiento de una cuestión determinada y pueda proceder a su examen. Por consulta se entiende el intercambio de opiniones y la apertura de un diálogo entre el empresario y el comité de empresa sobre una cuestión determinada, incluyendo, en su caso, la emisión de informe previo por parte del mismo".

Sigue el mismo indicando que el comité de empresa también ejercerá una labor de, art. 64.7.a) "*1.º De vigilancia en el cumplimiento de las normas vigentes en materia laboral, de seguridad social y de empleo, así como del resto de los pactos, condiciones y usos de empresa en vigor, formulando, en su caso, las acciones legales oportunas ante el empresario y los organismos o tribunales competentes*", para lo cual precisará información de las actuaciones empresariales.

Este último precepto le podemos conectar con el art. 5.1.a) y arts. 12, 13 y 14 del RGPD y el art. 89 de la LOPDGDD.

Consta en el expediente administrativo comunicación al Comité Intercentros de Mercadona sobre este particular. El comité intercentros es un órgano representativo de segundo nivel, establecido por convenio colectivo y con las funciones previstas en el mismo (art. 63 del ET) que no puede arrogarse las funciones del Comité de Empresa, que es al que, por los motivos expresados, debe comunicársele estas cuestiones de implantación de un sistema de reconocimiento facial. Sin embargo, conforme a la alegación presentada por la mercantil, se debe señalar que, efectivamente, en el presente caso consta legalmente asumida la competencia del Comité de Empresa en el Comité Intercentros.

En todo caso la comunicación efectuada pone de manifiesto que, considerado a este colectivo por la mercantil como afectado por el tratamiento de reconocimiento facial, sin embargo, falta toda referencia a los riesgos sobre los derechos de los trabajadores en la EIPD. (art 35 RGPD y lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos). En este sentido, como ya se ha señalado, la incorrecta evaluación de impacto es motivo de sanción conforme a lo dispuesto en la directriz del CEPD de referencia WP248, rev.01, apartado I *in fine*.

Ese control del sistema de reconocimiento facial en los términos expuestos produce también una presión coercitiva sobre los trabajadores y puede suponer un riesgo extremadamente elevado inasumible que coarte la libertad de los empleados, personal y profesionalmente. Es un riesgo de seguimiento de sus actividades sin que conste causa suficientemente justificada y, sobre todo, que no se ha tenido en cuenta en la elaboración del EIPD.

Como bien determina el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del GT29, *"Los sistemas que permiten a los empresarios controlar quién puede entrar en sus instalaciones, y/o en ciertas zonas de sus instalaciones, también pueden permitir el seguimiento de las actividades de los trabajadores*". En relación con la videovigilancia sigue señalando que "*La videovigilancia sigue presentando los mismos problemas para la privacidad de los trabajadores que antes: la capacidad de grabar de forma continuada el comportamiento del trabajador".*

No hemos de obviar otros riesgos que de todo ello se infieren, pues sigue indicando el Dictamen precitado que *"Aunque estos sistemas existen desde hace años, las nuevas tecnologías destinadas a hacer un seguimiento del empleo del tiempo y la presencia de los trabajadores se están generalizando, incluidas las que tratan datos biométricos y otras como el seguimiento de dispositivos móviles*" y que "*Aunque estos sistemas pueden constituir un componente importante del seguimiento efectuado por el empresario, también plantean el riesgo de proporcionar un nivel invasivo de conocimientos y control sobre las actividades del trabajador en el lugar de trabajo".*

Así nos encontramos con el riesgo altamente plausible de combinar datos obtenidos del sistema de videovigilancia y biométricos, el de "seguir" de forma continuada el comportamiento del trabajador, aunque el tratamiento de reconocimiento facial no haya sido establecido primigeniamente para ello.

Como termina indicando el GT29, "*Por tanto, los empresarios deben abstenerse de utilizar tecnologías de reconocimiento facial. Puede haber algunas excepciones marginales a esta regla, pero tales escenarios no pueden utilizarse para invocar una legitimación general del uso de esta tecnología".*

Parafraseando al GT29, el cumplimiento de una medida de seguridad destinada a una sola persona concreta no puede utilizarse para invocar una legitimación

general del uso de esta tecnología en los términos expuestos, ni respecto de los empleados ni de cualquier otro ciudadano.

Por todo lo antedicho, podemos concluir que el tratamiento en su conjunto no cuenta con legitimación para llevarlo a cabo, por lo que vulnera lo dispuesto en los arts. 9 y 6 del RGPD, infracciones tipificadas en el art 83.5.a) de dicha norma y consideradas muy graves a efectos de prescripción en el art. 72.1.e) y a), respectivamente, de la LOPDGDD.

VIII

Es precisa la realización del juicio de **proporcionalidad** antes de iniciar cualquier tratamiento.

En este sentido, el Tribunal Constitucional ha señalado, por todas la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero, que *"para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"*.

Y ello basado en la jurisprudencia fijada por el Tribunal Europeo de Derechos Humanos, esto es, la superación de un triple juicio, en el sentido de determinar si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

Lo primero que hemos de indicar es que, respecto del tratamiento de reconocimiento facial de Mercadona -que afecta al tratamiento de datos no sólo del condenado, sino de todos los potenciales clientes y empleados-, el juicio de proporcionalidad en sentido amplio debe de ser realizado en tiempo oportuno.

No obstante lo anterior, autorizado por el órgano judicial un medio electrónico genérico o uno específico como el reconocimiento facial sin indicar la forma o modo de llevarlo a cabo (ver sentencias), sigue siendo preciso realizar el juicio de proporcionalidad antes de iniciar el tratamiento para valorar qué medio es más idóneo, si es necesario para cumplir con la finalidad permitida por la sentencia y examinar la proporcionalidad de la medida.

Segundo, que el juicio de proporcionalidad cuando abarca el tratamiento de datos biométricos requiere un examen especialmente cuidadoso y pormenorizado.

El GT29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométrica indica que "*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado".*

Tercero, y ya entrando en el examen del juicio de proporcionalidad, respecto de la idoneidad, sí puede ser idóneo el sistema de reconocimiento facial para cumplir con la medida de alejamiento respecto del condenado, pero no es necesario, al existir medidas alternativas menos intrusivas, ni es estrictamente proporcional, en la medida en que se deriven más beneficios para el interés público que perjuicios sobre otros bienes o valores en conflicto, teniendo en cuenta que se pretende su aplicación masiva e indiscriminada para todos los potenciales clientes, con independencia del nivel de riesgo que represente y convirtiéndose la excepción de la posibilidad de tratamiento de datos biométricos en la regla general, en contra de lo pretendido por el RGPD.

De esta forma, en las sentencias anteriormente citadas se considera que la medida de seguridad solicitada por la mercantil es posible aplicarla sin pronunciarse sobre las garantías sobre los derechos y libertades de los afectados que debe llevar asociada su implantación ni justifica la aplicación de ninguna de las exenciones del art. 9.2 del RGPD. Ahora bien, como es lógico, el órgano judicial no se manifiesta respecto de la restricción de derechos fundamentales ni para el condenado ni para el resto de los ciudadanos con la implantación del sistema generalizado de reconocimiento facial, pues excede del ámbito de su competencia. Y en este sentido ya se ha señalado, y se insistirá más adelante, que dicho tratamiento resulta prohibido en aplicación del art. 9.1 del RGPD.

Tomemos como ejemplo la Sentencia precitada de Santander en la que se indica que *"Se solicita igualmente que se autorice al establecimiento al control de esta medida a través de los medios electrónicos de los que dispone la entidad Mercadona en orden al reconocimiento facial, con arreglo al art. 58.4 CP, que dispone: "El juez o tribunal podrá acordar que el control de estas medidas se realice a través de aquellos medios electrónicos que lo permitan". No hay absolutamente ningún inconveniente en conceder aquello que se pide, puesto que la afectación a la esfera de derechos o intereses de la condenada es*

mínima, tratándose tan solo de un medio o instrumento del que dispone el propio establecimiento para hacer cumplir lo acordado con mayor eficacia".

Así, autoriza respecto del condenado la implantación de la medida de seguridad valorando los intereses en conflicto, sin examinar siquiera la incidencia en los clientes y trabajadores de Mercadona (pues ninguno de ellos es parte en el procedimiento penal). Puede ser, por tanto, una medida idónea respecto del condenado, pero no lo es respecto del resto de ciudadanos, específicamente clientes y trabajadores de Mercadona, a quienes les afecta de manera indiscriminada.

Por ello, el tratamiento de reconocimiento facial en su conjunto, integrando el tratamiento de los datos biométricos de los potenciales clientes y empleados de Mercadona, no es idóneo. Podrían establecerse otros sistemas o modo de llevarlo a cabo de forma que no afectasen a sus derechos y libertades públicas.

Recordemos que aun entendiendo que este tratamiento de datos biométricos implantado por Mercadona sea el autorizado por el órgano judicial, lo sería sólo para la finalidad de adoptar una medida de seguridad en relación con el condenado y, aun así, respetando sus derechos fundamentales, salvo resolución judicial en contra.

En todo caso, existen medios menos invasivos en los derechos y libertades de los posibles clientes y de los empleados del supermercado para conseguir la finalidad pretendida; algunos de los cuales podrían recaer directamente sobre el condenado (como por ejemplo y junto a la prohibición de acudir a determinados lugares, imponerle al condenado una penal leve de localización permanente o imponerle un sistema de localización, lo cual sería valorado por el órgano judicial a petición de la parte concernida) sin afectar para nada y en ningún momento a los derechos y libertades de nadie más; otros, podrían ser los tradicionalmente utilizados de colgar la fotografía del condenado en el lugar -de acceso restringido y controlado- donde se visualicen las imágenes de videovigilancia ordinaria, o bien que la fotografía del condenado incluida en un dispositivo electrónico sea comparada de forma manual *"uno-a-uno"* a la entrada del establecimiento.

Cuarto, y ya tomada la decisión de instalación del sistema, éste debe de ser necesario "*en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia".*

Debe examinarse si para llevar a cabo el tratamiento es necesario realizarlo de una determinada manera preestablecida o si, de entre todas las opciones disponibles debe de elegirse aquella más moderada y con menor incidencia en los derechos y libertades de los ciudadanos concernidos y en consonancia con la normativa RGPD y LOPDGDD.

Partiremos del concepto de necesidad del tratamiento, que no debe confundirse con utilidad del mismo. Un sistema de reconocimiento facial puede ser útil, pero

no tiene por qué ser objetivamente necesario (siendo esto último lo que realmente debe estar presente). Como establece el GT29 - Dictamen 3/2012 sobre la evolución de las tecnologías biométricas- debe examinarse "*si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable".*

En este sentido, la AEPD, analizando la necesidad de un tratamiento concluye que, *"Si es necesaria o no, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia por poder llevarse a cabo manualmente la actividad. El termino necesidad no debe confundirse con útil sino si el tratamiento es objetivamente necesario para la finalidad"* -por todas, PS/00052/2020-.

Si no hay necesidad objetiva del tratamiento objeto ahora de análisis, si no es esencial para satisfacer esa necesidad, el tratamiento no es proporcional ni lícito. En consecuencia, está prohibido.

En el supuesto examinado el sistema de reconocimiento facial puede ser útil, mas no necesario, ya que no siendo el único con el que se puede lograr la finalidad pretendida al existir múltiples alternativas, sí es el único que puede producir una injerencia devastadora en los derechos y libertades de los ciudadanos. En consecuencia, se insiste, está prohibido.

En este mismo sentido se manifiesta el SEPD, en un artículo el 28 de octubre de 2019 titulado "Facial Recognition: A solution in search of a problem?" abordando este tipo de tratamientos. Así, requiere que el tratamiento mediante reconocimiento facial sea "*demostrablemente necesario*", esto es, objetivamente necesario y que no existan otros medios alternativos menos intrusivos mediante los cuales se obtenga el mismo objetivo y señala expresamente que *"la eficiencia y conveniencia no constituyen suficiente justificación".*

(Recuperado el 22 de febrero de 2020 de https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.)

Pero es que, además, a mayor abundamiento y, a los efectos meramente ilustrativos, no podemos soslayar el hecho de que el condenado puede burlar con facilidad el sistema de reconocimiento facial con una simple máscara -como se explica en la nota de la AEPD sobre los "*14 equívocos con relación a la identificación y autenticación biométrica"*, con lo que, podría pasar que implantado el sistema éste no fuera, además, ni útil ni efectivo para la finalidad pretendida por el supermercado.

Aquí, el principio de intervención mínima entra en juego (art. 5.1.c) y art. 25.1 RGPD), porque, además, se tiene que acreditar que no hay otra medida más moderada para la consecución de la finalidad pretendida con igual eficacia, en el marco de la responsabilidad proactiva del responsable del tratamiento.

Aunque el juzgado autorice genéricamente el sistema de reconocimiento facial, no obliga a instalarlo ni imposibilita el establecimiento de otro con el que pueda

lograrse la misma finalidad por otros sistemas menos intrusivos. Esto es, nada pasaría si, en vez de instalar este sistema de reconocimiento facial como el ahora analizado, Mercadona optara por otro que le permitiera hacer efectiva la medida de seguridad (ej. sistema de vigilancia ordinario con o sin vigilante de seguridad, es decir, de forma no remota *"uno-a-uno"*).

Además, la autorización del órgano judicial no es en absoluto una carta blanca, ni confiere un derecho ilimitado para Mercadona, sino que deberá cumplir con la normativa de protección de datos. Especialmente, porque el establecimiento de este sistema de reconocimiento facial puede suponer de facto la implantación indebida de una medida de seguridad para todos los clientes y empleados de Mercadona, como así ha ocurrido.

En este mismo sentido, el Informe 36/2020 del Gabinete Jurídico de la AEPD, referente al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, señalaba que *"la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos. Y en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1".*

En cuarto lugar, y en cuanto a la proporcionalidad en sentido estricto, debemos de examinar cuántas sentencias condenatorias han obtenido, cuál es la medida acordada en cada una de ellas, respecto de cuántas personas, a cuántos supermercados afectan tales sentencias y si todo ello es proporcional en relación con el número de clientes que cada día entran en los sus centros y el número de supermercados global que tienen en el territorio español.

Así, debemos considerar si la adopción de tal tratamiento es ponderado, equilibrado, derivarse de él más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Frente al interés de Mercadona de hacer efectiva una orden de alejamiento (respecto de quien ha cometido un delito leve en sus instalaciones), se alzan los derechos a la intimidad y a la protección de datos de todos los clientes y de sus empleados.

De un simple vistazo, resulta que el tratamiento es excesivo. Pues para hacer efectiva una medida de seguridad para una media de ***NÚM.3 personas al año en todo el territorio del Estado español -según sus cálculos, sobre una media de ***NÚM.2 procesos judiciales- por un periodo limitado y establecido en sentencia -que como máximo puede ser de seis meses al tratarse de un delito leve- se

podría llegar a monitorizar una vez implantado en todos los centros comerciales a una media de ***NÚM.7** clientes anuales (**…**). Esta medida también afectaría al colectivo de sus trabajadores, que cifran en más de 100.000 trabajadores. Mercadona cuenta en territorio español con 1.624 establecimientos.

O, dicho de otra forma, para controlar el acceso a Mercadona de una única persona se van a controlar a una media ***NÚM.1** potenciales clientes diarios por tienda (que habrá que multiplicar por el número de establecimientos afectados por la medida de seguridad).

Mercadona alega que solo se ha instalado el sistema en ***NÚM.8** centros, y en consecuencia los números anteriores son incorrectos. En este sentido, de debe señalar que los citados ***NÚM.8** establecimientos se refieren a modo “prueba” y la intención altamente plausible es su extensión a la totalidad de establecimientos de la mercantil.

Si para adoptar una medida de seguridad de un ciudadano tiene que tratarse de forma masiva e indiscriminada los datos personales del resto de los ciudadanos, el tratamiento es claramente desproporcionado. Sumemos ahora que nos encontramos con el tratamiento de datos biométricos destinados a identificar unívocamente a una persona. Se instalaría en el ámbito privado un sistema que no está siendo utilizado por las Fuerzas y Cuerpos de Seguridad del Estado que persiguen la consecución de finalidades de interés general.

Respecto de la inmensa cantidad de datos recabados, se debe añadir, además, que no consta que se hayan tomado las medidas técnicas adecuadas para evitar una posible transferencia de esos datos a terceros, incluidos terceros países fuera del EEE. La medida tomada se limita a una prohibición contractual de tipo formal entre la mercantil y la entidad encargada y dueña del software aplicado ***(***EMPRESA.2),*** basada en una autorización previa del responsable, sin estudios previos que acrediten de forma fehaciente la imposibilidad técnica de realizar la citada transferencia a terceros países dado el riesgo extremadamente elevado (inaceptable) que conllevaría en merma de los derechos, garantías y libertades de los afectados.

Debemos reseñar respecto de la desproporción del tratamiento, que se tratan datos personales de cualquier persona que entre al supermercado, compre o no, incluyendo menores de edad inimputables. Los menores de edad inimputables en ningún caso pueden encontrarse afectados por una sentencia condenatoria. La mercantil aduce que no es posible detectar la edad de las personas afectadas, pues con más razón para no llevar cabo este tipo de tratamiento. El riesgo extremadamente elevado asumido en el tratamiento es inaceptable.

También por estos motivos se estaría produciendo una vulneración del principio de minimización de datos (art. 5.1.c) RGPD).

Así se puede comprobar del simple examen del expediente administrativo, ya que en la EIPD y sobre la amenaza consistente en que "*Se tratan datos inadecuados, no pertinentes, excesivos o innecesarios para la finalidad prevista*" no se hace mención ninguna a estos datos que son a todo punto excesivos, página 13. Se limitan a considerar únicamente los datos del condenado respecto del principio de minimización, puesto que señalan que "*Únicamente se tratan los datos derivados de sentencias firmes, en los que MERCADONA sea parte y se hayan aportado imágenes en el transcurso del procedimiento como prueba, que determinen la orden de alejamiento haciéndose efectiva mediante la posible utilización de nuevas tecnologías".*

El principio de minimización al que obliga en todo tratamiento de datos personales el artículo 5.1.c) del RGPD, a la vista de la documentación remitida y a la descripción del tratamiento efectuado, podemos considerar que el sistema de reconocimiento facial implementado por Mercadona en cuarenta (******NÚM.8***) de sus centros comerciales trata datos biométricos dirigidos a "identificar" de una manera unívoca a una persona física, en un proceso de búsqueda de correspondencias "*uno-a-varios"* sujetos a lo dispuesto en el artículo 9 del RGPD, tratamiento también denominado por la doctrina "*masivo y de forma remota*", a fin de diferenciarlo de otros tratamientos automatizados faciales también biométricos de tipo comparativo *"uno-a-uno"* dirigidos a "autenticar" a una persona con una base de datos (podría ser también de imágenes faciales) automatizada o con intervención humana en cada una de las comprobaciones, de características menos intrusivas. Es el caso de disponer en un equipo electrónico la base de datos de imágenes a comparar (personas indubitadas) y limitarse de forma manual a realizar la comparativa *"uno-a-uno"* para "autenticar"*,* lo que la doctrina denomina tratamiento *"masivo no remota"*. No hay duda de que este último tipo de tratamiento minimizaría considerablemente los riesgos de vulnerar los derechos, garantías y libertades de las personas que entran en el establecimiento al limitarse a lo necesario y pertinente (principio de minimización, art. 5.1.c) RGPD).

En consecuencia, esta operación de tratamiento en los términos expuestos vulnera lo dispuesto en el art. 5.1.c) del RGPD, infracción tipificada en el art. 83.5.a) de dicha norma, considerada muy grave a efectos de prescripción en el art. 72.1.a) de la LOPDGDD, al tratar datos personales excesivos para la finalidad a la que va dirigida.

IX

Es precisa la realización de la **evaluación de impacto** antes de iniciar cualquier tratamiento de alto riesgo a fin de poder detectar, en su caso, aquellos inaceptables que impediría el tratamiento.

En el supuesto analizado, además, debe de realizarse una EIPD. En este sentido resulta precisa cuando *"sea probable que las operaciones de tratamiento*

entrañen un alto riesgo para los derechos y libertades de las personas físicas", considerando 84 RGPD, *"antes del tratamiento",* considerando 90 RGPD, y se realizará en los términos del art. 35 del RGPD. El tratamiento pretendido por Mercadona se encuentre incluido en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4). La EIPD debe conllevar ínsita el juicio de proporcionalidad señalado.

Antes de implantar un sistema de reconocimiento facial del tipo *"uno-a-varios"* el responsable debe de valorar primero si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad**.** El apartado 72 de la Guía 3/2019 del CEPD "on processing of personal data through video devices", aclara en este sentido que "*The use of biometric data and in particular facialrecognition entailheightened risks for data subjects' rights.It is crucial that recourse to such technologies takes place with due respect to the principles of lawfulness, necessity, proportionalityanddata minimisation as set forth inthe GDPR. Whereas the use of these technologies can be perceived as particularly effective,controllers should first of all assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing".*

(*"La utilización de datos biométricos y, en particular, el reconocimiento facial conlleva riesgos mayores para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando los principios de legalidad, necesidad, proporcionalidad y minimización de los datos establecidos en el RGPD. Considerando que el uso de estas tecnologías puede percibirse como especialmente eficaz, los responsables deberían, en primer lugar, evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos para lograr su objetivo legítimo de la transformación".* La traducción es de la AEPD).

Sin embargo, Mercadona ha solicitado la adopción de medida de seguridad en los tribunales consistente en el tratamiento de reconocimiento facial antes de valorar la concurrencia de riesgos y la necesidad de realizar una EIPD, lo que no consta en el expediente administrativo -como se pone de manifiesto en el hecho de que la EIPD es posterior a la solicitud de tal medida de seguridad en una pluralidad de procedimientos penales-. Aun cuando la EIPD sea anterior a la ejecución del tratamiento, la comprensión adecuada de la responsabilidad proactiva y de la privacidad desde el diseño implican valorar desde el momento primigenio del bosquejo de un tratamiento de datos personales si este puede llevarse a cabo. Así, el primer instante en que se proyectó la idea de solicitar la medida de seguridad consistente en un tratamiento de reconocimiento facial ante los juzgados y tribunales, debió ser la ocasión de valorar y detectar los riesgos en los derechos y libertades de los ciudadanos.

Hay que añadir que los riesgos derivados de tal automatismo son altos por sí mismos y, de hecho inaceptables al no poder disminuir el riesgo inherente inicial

a niveles adecuados (riego residual) al existir una prohibición legal conforme señala el artículo 9.1 del RGPD. Tal tratamiento se produce sin intervención humana en cuanto se instala y activa el sistema correspondiente, de tal forma que la persona concernida no puede impedir el tratamiento de sus datos personales en su vertiente del ejercicio del derecho de supresión y oposición, lo que puede suponer infracción del art. 35 del RGPD, tipificada en el art 83.4.a) de dicha norma y considerada grave a efectos de prescripción en el art. 73.t) de la LOPDGDD (en este sentido, ver GT29 248 ya mencionado).

X

En este planteamiento, obvian y no consideran la posibilidad de que los datos de todos los posibles clientes que entren al supermercado estén siendo tratados de forma inadecuada, no pertinente, excesiva o innecesaria para la finalidad prevista. No se han planteado ni por un momento que esta es la situación de los **menores inimputables**.

Si bien en principio los datos personales de los menores de edad no se encuentran especialmente salvaguardados en atención simplemente a la edad de estos, también lo es que el ordenamiento jurídico les protege especialmente, por su especial vulnerabilidad. Esta protección se despliega específicamente en protección de datos personales desde el Convenio 108 del Consejo de Europa –"*specific attention shall be given to the data protection rights of children and other vulnerable individuals*"-, pasando por el RGPD y la LOPDGDD, hasta la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.

Esta última consagra en su artículo 2 que el "*Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado",* concretando en su art. 4 lo relativo a su derecho al honor, a la intimidad personal y familiar y a la propia imagen y en su art. 22 quáter lo referente al tratamiento de datos de carácter personal.

El art. 28.2 de la LOPDGDD previene como uno de los mayores riesgos a los que deben atender el responsable y el encargado del tratamiento que la *"e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad*".

En este sentido destacaremos el considerando 38 del RGPD que establece que *"Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen*

servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños".

Por ello, la AEPD ha aclarado en sus guías las especiales recomendaciones de protección a los menores de edad, como acontece en materia de videovigilancia en relación con la captación de imagen en entornos escolares.

XI

En cuanto a la transparencia, en relación con la información que se suministra a los interesados, varios son los aspectos que reseñar.

Previa, en el presente caso, se debe señalar que el tratamiento analizado no cumple con las normas del RGPD tal y como se ha indicado anteriormente, por lo que es un tratamiento prohibido. No obstante, se procede a analizar sucintamente la cartelería informativa.

Primero, en cuanto a la cartelería, indican que es "*para detectar únicamente aquellas personas con una orden de alejamiento o medida judicial análoga, en vigor que puedan suponer un riesgo para su seguridad*".

Estas personas condenadas generan riesgo a los bienes e instalaciones del supermercado, que es por lo que les han condenado. El riesgo para la seguridad de los clientes es claramente indirecta y muy tangencial. Y quedaría cubierta la seguridad de los clientes por el sistema de videovigilancia ordinario. No hay transparencia en la información.

En el expediente administrativo, en la EIPD, se establece en un contexto -se copia literalmente- *"Sistema de reconocimiento facial para identificar a agentes externos con orden de alejamiento vigente dictada en el marco de una sentencia firme, posibilitándose la utilización de medios tecnológicos para su efectividad, perjudiciales para los empleados y centros de MERCADONA"*, página 4.

De igual forma lo encontramos cuando en el citado documento determinan la finalidad del tratamiento, que restringen de nuevo a la seguridad de sus empleados y la de sus bienes (centros Mercadona): "*Sistema de reconocimiento facial para identificar a agentes externos con orden de alejamiento vigente dictada en el marco de una sentencia firme, posibilitándose la utilización de medios tecnológicos para su efectividad, perjudiciales para los empleados y centros de MERCADONA",* página 6 (intereses privados).

No citan a los clientes de la cadena de supermercados como potenciales objetivos de "su seguridad". Sorpresivamente sí lo hacen en la cartelería citada anteriormente y en la información que muestran a sus empleados para que den explicaciones a los potenciales clientes.

La información suministrada no es correcta, ni se ajusta a la finalidad (hacer efectiva una medida de seguridad), ya que el sistema no se pone en marcha para proteger a los clientes, sino a Mercadona, consecuencia de la obtención de una sentencia favorable a sus intereses (que contiene una pena para el condenado). En todo caso, el sistema de seguridad ordinario es suficiente para garantizar la seguridad de los clientes (art. 22.1 de la LOPDGDD). No es preciso establecer sistema de reconocimiento facial como el ahora analizado para garantizar la seguridad de los clientes, pues si fuera necesario a tales efectos, sería el que ordinariamente se establecería en todo tipo de instalaciones. Sin embargo, este sistema de reconocimiento facial es un sistema de seguridad extraordinario al tratarse datos biométricos con la finalidad de identificar unívocamente a una persona "*uno-a-varios"* y de forma remota se encuentran incluidos en la categoría especial de datos personales (art. 9 del RGPD).

Como hemos apuntado antes, la información suministrada en la cartelería de los supermercados es la misma, sin indicar específicamente en cuál de ellos está activado el sistema o si por el simple hecho de colgar el cartel se encuentra activado, ni durante cuánto tiempo está activado (duración de la medida de seguridad), ni se explicita la finalidad concreta.

Se traslada a los clientes la impresión de que en todos los supermercados está instalado el sistema y de manera permanente. Se hurta a los potenciales clientes la posibilidad de no entrar en el supermercado concreto y elegir otro en el que no esté instalado el sistema de reconocimiento facial. Se está limitando de facto el derecho de autodeterminación, la libertad y la intimidad. Los riesgos derivados de esta información incorrecta son claros, el menoscabo de sus libertades y derechos fundamentales.

La información debería indicar si está instalado o no el sistema. Máxime si tal y como afirma Mercadona sólo va a utilizar el sistema "*en el supuesto de que sea parte de un procedimiento judicial en el que mediante resolución firme se determine el uso del reconocimiento facial para hacer efectivas las órdenes de alejamiento".*

Segundo, que tratándose de tecnologías tan invasivas y, con base en los razonamientos antes expuestos sobre los menores y otros colectivos vulnerables que merecen una especial protección, la información suministrada debería ser específica para los mismos.

El considerando 58 RGPD, sobre el principio de transparencia (información) *"… Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender*". Y artículo 12 RGPD señala que *"El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en*

forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño…".

Si bien en la EIPD se indica que *"El uso de tecnologías innovadoras como el reconocimiento fácil supone un riesgo para los sujetos por la novedad que presentan los mismos y el desconocimiento sobre su funcionamiento. MEDIDAS; Se informa de manera clara y transparente sobre el tratamiento y tecnología utilizada",* página 17, no se establece ninguna medida adicional, específica para trasmitir la información adecuadamente a los menores y a otros colectivos vulnerables. La información suministrada es la misma para todo el mundo.

Tercero, en cuanto a la transparencia y a las posibles transferencias internacionales, que aseveran que no se van a producir, lo cierto es que en el contrato de encargado de tratamiento se significa que cabe la posibilidad de transferencia internacional en determinados supuestos: *"8.2. En caso de transferencia de datos personales a un tercer país que no pertenezca a la Unión Europea, un país que no cuente con un nivel de protección adecuado, o una organización internacional, el Encargado del Tratamiento deberá obtener la autorización previa por escrito del Responsable del Tratamiento y cooperar para garantizar un marco de protección adecuado en virtud de la normativa vigente, mediante la aplicación de normas corporativas vinculantes, la formalización de cláusulas contractuales estándar adoptadas por la Comisión Europea o, en su caso, la obtención de la autorización de la transferencia por parte de la autoridad competente*". No informan a los clientes de tal posibilidad ni establecen cómo se informaría si finalmente se produjera este supuesto. Anteriormente ya se ha señalado la ausencia de medidas técnicas para evitar posibles transferencias internacionales indebidas.

La falta de transparencia en la información que impide advertir a los afectados que el tratamiento implantado no es posible, mejor dicho, se encuentra prohibido, constituye otro de los elementos volitivo de la responsabilidad.

En consecuencia, la información facilitada por la mercantil tanto al público en general como a los empelados infringe lo dispuesto en el art. 12 del RGPD al incumplirse los requisitos citados en los arts. 13 de dicha norma, infracción tipificada en el art 83.5.b) y considerada muy grave a efectos de prescripción en el art. 72.1.h) de la LOPDGDD.

XII

Lo anterior es extensible a la información facilitada en la "*política de privacidad*", en la que se limita a informar de forma genérica -respecto al tratamiento del sistema de reconocimiento facial o sistema de detección anticipada-, lo siguiente:

Categorías de datos: biométricos (en aquellas tiendas de España donde esté implantado el sistema de detección anticipada).

Finalidad: "*Llevar a cabo las actuaciones precisas para proteger los intereses vitales de los clientes cuando así sea necesario, o el cumplimiento de las resoluciones judiciales y las medidas en ellas acordadas*".

Tiempo de mantenimiento de los datos: "*En relación con la protección del interés vital de las personas y la ejecución de las sentencias o resoluciones que conlleven órdenes de alejamiento sobre los centros de trabajo y/o personas, los datos serán tratados y custodiados el tiempo imprescindible para dar cumplimiento a las medidas judicialmente de aquellas personas condenadas a dicha orden de alejamiento (en aquellas tiendas de España donde está implantado el sistema de detección anticipada.*

No obstante, los datos recogidos accesoriamente para cumplir con dicha finalidad permanecerán en el servidor únicamente en el proceso de comprobación (esta comprobación dura décimas de segundo). Una vez realizada esta comprobación procederá a ser destruida definitivamente (en aquellas tiendas de España donde está implantado el sistema de detección anticipada)".

Transferencias internacionales: "*En aquellos casos en los que Mercadona cuente con prestadores de servicio o proveedores que se encuentren fuera de la Unión Europea, las transferencias internacionales realizadas con ellos están plenamente garantizadas atendiendo a las normas establecidas por el Reglamento (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de Abril de 2016, y criterios de la Agencia Española de Protección de Datos*".

Legitimación: "*En el caso del tratamiento de los datos de carácter sensible serán tratados por razones de interés público con las consiguientes consideraciones previstas por la normativa de protección de datos, que debe ser proporcional al objetivo perseguido, que es hacer cumplir la ley, respetando los restantes principios de la normativa de protección de datos y estableciendo las medidas adecuadas y específica para proteger los intereses y derechos de los interesado, sobre la base del Derecho de la Unión o de los estados miembros (en aquellas tiendas de España donde está implantado el sistema detección anticipada)*".

Comunicación de datos: "*Las fuerzas y Cuerpos de Seguridad del estado en virtud de lo establecido en la ley*".

Otros datos: "*De igual modo te informamos que, con el fin de mejorar la seguridad de clientes y empleado, Mercadona, en base al interés público puede tratar su imagen o su perfil facial biométrico para identificar a sujetos con una orden de alejamiento 8º medida judicial análoga) en vigor contra Mercadona o contra cualquiera de sus trabajadores (en aquellas tiendas de España donde está implantado el sistema de detección anticipada).*

Estas imágenes únicamente se tratarán internamente por Mercadona, siendo exclusivamente comunicadas a las Fuerzas y Cuerpos de Seguridad para proteger la seguridad de los clientes y trabajadores de Mercadona y el cumplimiento de las medidas decretas judicialmente (en aquellas tiendas de España donde está implantado el sistema de detección anticipada)".

Derechos: (…) respecto al de oposición, *"En determinadas circunstancias y por motivos relacionados con su situación particular al tratamiento de sus datos, los interesados podrán oponerse al tratamiento de sus datos. Mercadona dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones*".

XIII

Por otro lado, los riesgos derivados de los errores de identificación de una persona que no tiene prohibido el acceso por la medida de seguridad, ligado de forma intrínseca al diseño por defecto que señala el art. 25.1 del RGPD.

En estos sistemas de reconocimiento facial, se utiliza un patrón para elaborar el reconocimiento facial -fruto de un tratamiento inicial de datos personales por lo que constituye asimismo un dato personal elaborado y contenido en el alcance del derecho de acceso que en su caso se ejercite-, pero es conocido que *"la información biométrica almacenada (p. ej. el patrón) permite reconstruir parcialmente la información biométrica original (p. ej. la cara). Dicha reconstrucción parcial tiene en ocasiones la fidelidad suficiente para que otro sistema biométrico la reconozca como el original" -14 equívocos con relación a la identificación y autenticación biométrica de la AEPD-*. Y ello nos enlaza con la necesidad de implementar evaluaciones regulares que permitan verificar la pertinencia y suficiencia de las garantías otorgadas (apartado 4 de Guidelines3/2019 on processing of personal data through video devices, del CEPD).

Diversos son los estudios en el marco del reconocimiento facial, tanto del tipo "*uno-a-uno"* (dato biométrico) como "*uno-a-varios*" (dato biométrico de categoría especial), que hacen referencia a las elevadas tasas de error en determinados supuestos propias de la incipiente tecnología y escasa datificación de los sistemas de inteligencia artificial aplicada. En este sentido, la gran demanda global de "datos" para alimentar este tipo de software, hace que se deban tomar medidas, al menos técnicas, para evitar cesiones indebidas y, en especial, posibles transferencias internacionales que hagan posible en el futuro la identificación del afectado en entornos y finalidades muy diferentes a los iniciales.

A tales efectos son importantes los estudios realizados por ***C.C.C.***, quien pone de manifiesto que las altas tasas de error en la identificación de individuos mediante el reconocimiento facial se producen cuando se trata de individuos de color y de mujeres (en este último caso, cualquiera que sea el color de su piel).

En este segundo supuesto los equívocos se originan derivado de la mínima cantidad de imágenes de mujeres que contienen los *sets* de entrenamiento y los *sets* de testeo (que utilizan mayoritariamente imágenes de hombres blancos). También considera que el reconocimiento facial no funciona bien en niños y adultos de edad avanzada. ***C.C.C.*** percibe la existencia de lo que denominan el sesgo algorítmico.

(***URL.1)

***URL.2

Además, debemos traer a colación el error en la identificación que se puede producir en la actualidad por la situación pandémica que nos exige llevar obligatoriamente mascarillas a todas las personas. El Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) ha llevado a cabo desde 2002 diversas evaluaciones independientes a los sistemas comerciales de TRF. Se trata de las *Face Recognition Vendor Test.* Una de sus evaluaciones se centra en el uso masivo de mascarillas, concluyendo que la tasa de error en los algoritmos de reconocimiento facial más utilizados en la actualidad se dispara entre el 5% y el 50%.

(Recuperado el 22 de febrero de 2021 de https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

https://pages.nist.gov/frvt/html/frvt_facemask.html

https://www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software)

También se producen errores de identificación en relación con familiares y hermanos, tal y como recoge la AEDP en su nota sobre los "*14 equívocos con relación a la identificación y autenticación biométrica*".

Es cierto que las cuestiones relativas a la tasa de error predecibles desde el diseño es una cuestión controvertida, pues el mayor desarrollo tecnológico en el futuro más o menos próximo mejorará la tasa de exactitud.

(Recuperado el 22 de febrero de 2021 de https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms)

Mas, a día de hoy, es un riesgo más que no podemos permitirnos, pues la inexactitud es predecible desde el propio momento del diseño de este tipo de sistemas de información a la hora de identificar al condenado y su confusión con otra persona puede generar un riesgo de discriminación y exclusión social inaceptable. Y ello a mayor abundamiento de todas las consideraciones esgrimidas sobre la falta de normativa que lo legitime (tratamiento prohibido) y

garantice el nivel adecuado de proporcionalidad frente a los derechos y libertades para los afectados.

La vulneración de la protección de datos desde el diseño infringe el artículo 25.1 del RGPD, tipificada en el art 83.4.a) y considerada grave a efectos de prescripción en el art. 73.d) de la LOPDGDD.

XIV

Respecto de **los riesgos derivados del tratamiento**, se ha de tener en cuenta que el reconocimiento facial se encuentra configurado como un método involuntario de identificación a través del uso de datos biométricos, tal y como se establece en las Directrices Éticas para una IA Fiable, documento presentado en 2019, elaborado por el Grupo de expertos de alto nivel sobre inteligencia artificial bajo el amparo de la Comisión Europea.

Los riesgos derivados de tal automatismo son muy altos por sí mismos, pues una persona no puede impedir el tratamiento de sus datos personales, porque tal tratamiento (la captación y posterior tratamiento se sus datos biométricos de su cara en el supuesto del reconocimiento facial) se produce automáticamente, sin intervención humana en cuanto se instala y activa el sistema correspondiente.

De hecho, en el documento citado se recoge como una de las primeras y mayores preocupaciones la identificación y el seguimiento de personas mediante técnicas de inteligencia artificial y, en cuanto a lo que nos interesa, que *"la identificación automática plantea serias preocupaciones tanto desde el punto de vista legal como ético, dado que puede tener efectos inesperados en muchos niveles psicológicos y socioculturales";* por ello, diferencian "*entre la identificación de una persona frente a su seguimiento y rastreo, y entre una vigilancia selectiva o masiva".*

Asimismo, aseveran que la aplicación de este tipo de tecnologías debe estar claramente justificada en la legislación existente, que no es el caso.

A mayor abundamiento, no podemos obviar que la implantación de un sistema de reconocimiento facial como el ahora analizado recoge mucha más información del sujeto que otro tipo de tratamientos, no pudiendo ser impedido por la persona afectada, consecuencia de la automatización y algoritmos aplicados, ya que "*dependiendo de los datos biométricos recogidos, pueden derivarse datos del sujeto como su raza o género (incluso de las huellas dactilares), su estado emocional, enfermedades, taras y características genéticas, consumos de sustancias, etc. Al estar implícita, el usuario no puede impedir la recogida de dicha información suplementaria*" -Nota de la AEPD sobre los "*14 equívocos con relación a la identificación y autenticación biométrica*"-.

Respecto a los riesgos de exclusión social, riesgos discriminatorios y principio de exactitud, se debe señalar que podemos percibir dos riesgos importantes de

exclusión social derivados de un eventual mal funcionamiento del sistema implantado por la mercantil.

En este sentido se recoge en la Guidelines 3/2019 on processing of personal data through video devices (Version for public consultation. Adopted on 10 July 2019), que "*In addition to privacy issues, there are also risks related to possible malfunctions of these devices and the biases they may induce. Researchers report that software used for facial identification, recognition, or analysis performs differently based on the age, gender, and ethnicity of the person it's identifying. Algorithms would perform based on different demographics, thus, bias in facial recognition threatens to reinforce the prejudices of society. That is why, data controllers must also ensure that biometric adopted 5 data processing deriving from video surveillance be subject to regular assessment of its relevance and sufficiency of guarantees provided*".

("*Además de los problemas de privacidad, también hay riesgos relacionados con posibles mal funcionamiento de estos dispositivos y los sesgos que pueden inducir. Los investigadores informan que el software utilizado para la identificación, el reconocimiento o el análisis faciales se realiza de manera diferente en función de la edad, el género y la etnia de la persona que está identificando. Los algoritmos se realizarían sobre la base de diferentes demografías, por lo tanto, el sesgo en el reconocimiento facial amenaza con reforzar los prejuicios de la sociedad. Por ello, los responsables del tratamiento de datos también deben garantizar que el tratamiento de datos biométrico adoptado en 5 derivado de la videovigilancia se someta a una evaluación periódica de su pertinencia y su suficiencia de las garantías proporcionadas*". La traducción es de la AEPD).

Por un lado, nos encontramos con un riesgo a largo plazo de discriminación de una persona condenada penalmente (incluso después de que haya cumplido la condena y estén cancelados los antecedentes penales) que se siga identificando como en situación de alejamiento de los supermercados.

En la EIPD deben considerarse todas aquellas cuestiones relacionadas con el principio de exactitud; de la realizada por la mercantil no consta que se hayan valorado y se consideren específicamente estos riesgos señalados anteriormente, lo que ha inducido a realizar operaciones de tratamiento indebidas con menoscabo de las garantías, derechos y libertades para los afectados. A lo que hay que añadir que tampoco se contempla en la EIPD facilitada por la mercantil evaluación de impacto alguna sobre los menores que acceden a los locales y sus empleados, y deja vacío de contenido en el ejercicio de ciertos derechos recogidos en los arts.12 y 13 y 15 a 22 del RGPD.

Estas deficiencias en la elaboración de la EIPD con las consecuencias citadas deben considerarse un defecto sustancial que invalida *de facto* la EIPD realizada. En consecuencia, la falta de conocimiento de los posibles impactos del

tratamiento de datos implantado sobre las libertades y derechos de los afectados y, en consecuencia, ausencia de medidas correctoras que lo minimicen o, como es el caso, que lo invaliden, supone una infracción de lo dispuesto en el artículo 35 del RGPD, infracción tipificada en el art 83.4.a) de dicha norma y considerada grave a efectos de prescripción en el art. 73.t) de la LOPDGDD.

A los meros efectos ilustrativos significaremos que algunas empresas han abandonado sus negocios y programas de reconocimiento facial por intromisiones en la privacidad y claros riegos de discriminación racial.

Existe también un riesgo general de utilización de datos biométricos de reconocimiento facial al convertir a todas las personas que entren en el supermercado en posibles sospechosos, sujetos a una vigilancia biométrica indiscriminada (no discrimina ni por colectivo, ni por edad, ni por vulnerabilidad, etc.) lo que supone un abuso del uso de los datos biométricos y una clara injerencia en los derechos fundamentales y libertades públicas de los ciudadanos. Así se ha entendido mediante la Iniciativa Ciudadana Europea (ICE) titulada «Iniciativa de la sociedad civil para la prohibición de las prácticas de vigilancia biométrica masiva» (Civil society initiative for a ban on biometric mass surveillance practices) presentada ante la Comisión Europea en enero de 2021.

Respecto de los riesgos específicos de sujetos vulnerables, la Agencia Europea de Derechos Fundamentales (European Union Agency for Fundamental Rights, conocida por su acrónimo UEFRA) ha realizado en 2019 un documento titulado "Facial recognition technology: fundamental rights considerations in the context of law enforcement". En el mismo examina, además de los riesgos a la privacidad, a la protección de datos personales y a la discriminación concernidos por un tratamiento con un sistema de reconocimiento facial, otros derechos, libertades y bienes jurídicos afectados.

Hace mención específica a determinados colectivos más vulnerables cuales son los menores edad, a las personas mayores o las personas discapacitadas.

Respecto de los menores señala que "*Facial recognition systems affect the rights of children in different ways. […] The child's best interests must also be given a primary consideration in the context of using facial recognition technology for law enforcement and border management purposes. […] Due to the particular vulnerability of children, the processing of their biometric data, including facial images, must be subject to a stricter necessity and proportionality test, compared to adults. […] Software tests clearly indicate that images of younger people result in considerably more false negatives (misses) compared to other age groups, most probably due to rapid growth and change in facial appearance".*

("*Los sistemas de reconocimiento facial afectan a los derechos de los niños de diferentes maneras. [...] Los mejores intereses del niño también deben recibir una consideración primordial en el contexto de la utilización de la tecnología de reconocimiento facial para la aplicación de la ley y la gestión de fronteras. [...]*

Debido a la particular vulnerabilidad de los niños, el procesamiento de sus datos biométricos, incluidas las imágenes faciales, debe estar sujeto a una prueba de necesidad y proporcionalidad más estricta, en comparación con los adultos. [...] Las pruebas de software indican claramente que las imágenes de las personas más jóvenes resultan en negativos considerablemente más falsos (faltas) en comparación con otros grupos de edad, lo más probable es que debido al rápido crecimiento y cambio en la apariencia facial". La traducción es de la AEPD).

Por ello, dada la especial protección que el ordenamiento jurídico procura a la infancia, la evaluación respecto a la proporcionalidad del tratamiento de los datos personales de los menores por sistemas biométricos ha de estar sujeta a un juicio de necesidad proporcionalidad mucho más estricto que el que se referiría a los adultos. Esto no se trasluce en la EIPD realizada por Mercadona. El examen es absolutamente generalista y omite colectivos en alto riesgo, circunstancia que, de haberse tenido en cuenta, hubiera informado un resultado de riesgo extremadamente elevado inaceptable y, por lo tanto, prohibido.

Respecto de los riesgos sobre los derechos y libertades de los empleados de Mercadona ni tan siquiera se han considerado en la EIPD presentada.

Anteriormente hacíamos mención al derecho de autodeterminación. Unido al mismo, junto con el derecho a la intimidad, surge el riesgo cierto de pérdida de libertad y de intimidad. La Sentencia 600/2019 de la Sala Primera de lo Civil del Tribunal Supremo, de 7 de noviembre de 2019 (Rec. 5187/2017) examinaba lo que al derecho a la intimidad suponía el establecimiento de una cámara ficticia; así, se reconoce como parte del derecho a la intimidad el derecho a no tener que soportar una incertidumbre permanente en relación con una cámara que puede o no estar activada, real o ficticia. Es cierto que se refiere a una cámara orientada a una finca privada y no a un espacio público, pero nos sirve para ilustrar el impacto que sobre la privacidad produce. El hecho indubitado es que nadie se comporta igual si está siendo grabado o así lo cree; si una cámara falsa puede producir un impacto más que significativo en la intimidad, esté situada en un espacio privado o público, imaginemos la repercusión de una cámara plenamente operativa y, más allá, la conmoción de la utilización de técnicas de reconocimiento facial masivo e indiscriminado del tipo *"uno-a-varios"*. El riesgo se ve incrementado por la falta de información adecuada en la cartelería, tal y como hemos expresado en apartados anteriores.

El Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del GT29 considera que *"No obstante, estos sistemas utilizados a gran escala pueden producir efectos secundarios graves. En el caso del reconocimiento facial, donde los datos biométricos pueden capturarse fácilmente sin conocimiento del interesado, un uso amplio podría terminar con el anonimato en los espacios públicos y permitir un seguimiento continuo de las personas".*

Hay que añadir, respecto de los riesgos derivados del ejercicio de derechos, podemos ver como en la EIPD presentada por la empresa, página 17, se comprende como una de las amenazas para el colectivo de personas que acceden a los supermercados la de que "*No se han puesto a disposición medios o no se ha informado al interesado sobre su opción de oposición a la toma de decisiones automatizadas"*, explicando que "*Si bien se ha aportado la información a los sujetos de la posibilidad del ejercicio de su derecho de oposición (con base a la legitimación del artículo 6 de RGPD), este puede presentar ciertos riesgos".*

Posteriormente, entre las medidas a adoptar indican que *"con base en el artículo 21.1 MERCADONA deberá de dejar de tratar los datos salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".*

Dado que el tratamiento de datos del sistema de reconocimiento facial es automático, masivo y remoto y la imagen se capta y se trata automáticamente, esta medida es imposible de llevar a cabo (hacer efectivo el derecho de oposición/supresión) a salvo de desinstalar el sistema establecido en todos los supermercados. Si un interesado ejerce su derecho de oposición/supresión y tiene derecho al mismo, su oposición afecta al tratamiento de los datos por el supermercado desde la misma captación de la imagen facial, independientemente del lugar donde se encuentre el supermercado al que acceda al interesado.

En la documentación aportada por la mercantil (doc 7.1 y Doc. 7.2) no se justifica la denegación del derecho de oposición ejercido, con base genérica en la existencia de *"… un interés público imperioso …".* El considerando 69 del RGPD señala: *"(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado".* En el mismo sentido lo señala el art 21.1 del RGPD: *"… El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones ..."*

Se estaría dejando sin contenido y de facto el derecho de oposición o supresión, recordando que sólo puede establecerse una limitación a estos derechos por

mor de disposiciones legislativas de la UE o de los Estados miembros, en los términos del considerando 73 y de los artículos 23 y 89 del RGPD.

XV

Además, no es único este planteamiento a nivel europeo toda vez que otras autoridades de control lo siguen.

En este sentido, la Autoridad de Control de los Países Bajos (Netherlands) emitió una advertencia formal a un supermercado por el uso de la tecnología de reconocimiento facial.

El sistema implantado, la finalidad de su establecimiento, la cuestión relativa a su falta de legitimación en relación con el tratamiento de reconocimiento facial utilizado por una cadena de supermercados holandeses es casi idéntica al supuesto de Mercadona.

Así, este tratamiento se implanta para evitar que determinadas personas puedan acceder a los supermercados, en atención a una prohibición emitida al efecto. El supermercado esgrime que el sistema de reconocimiento facial había sido implantado con la finalidad de proteger a sus clientes y personal y evitar el robo en las tiendas. Las cámaras también se encontraban situadas en la entrada de las tiendas y, de igual forma que Mercadona, se procede a escanear a todas las personas que entren en la tienda, comparándolo con la base de datos de personas con prohibición de entrada y, si se produce el descarte, borrando los datos tratados tras varios segundos.

La vicepresidenta de la Autoridad de Control de los Países Bajos, ha manifestado que *“Es inaceptable que este supermercado, o cualquier otra tienda de los Países Bajos, empiece a utilizar la tecnología de reconocimiento facial”,* afirmando que el uso de esta tecnología está prohibido en casi todos los casos. Sigue explicando que *“El reconocimiento facial nos hace a todos caminar códigos de barras”,* y que *"Tu cara se escanea cada vez que entras en una tienda, un estadio o un estadio deportivo que utiliza esta tecnología. Y se hace sin tu consentimiento. Al poner su cara a través de un motor de búsqueda, existe la posibilidad de que su cara podría estar vinculada a su nombre y otros datos personales. Esto podría hacerse cotejar su cara con su perfil de redes sociales, por ejemplo”.*

La Autoridad de Control de los Países Bajos considera asimismo que con la implantación de cámaras de reconocimiento facial podemos ser monitoreados continuamente. Y que existe un riesgo extremadamente elevado (inaceptable) de utilización posterior de la información que nos califique como sospechosos o de interés o perfilarnos.

La citada Autoridad de Control sigue indicando que hay dos supuestos de uso permitido de uso de reconocimiento facial. El primero se basa en el consentimiento explícito del cliente para tratar sus datos; no constituyendo

consentimiento explícito la advertencia informativa al cliente del uso de la tecnología en las tiendas. Entrar en un supermercado no puede entenderse como prestar un consentimiento.

En nuestro supuesto examinado, Mercadona pretende tratar los datos biométricos de los posibles clientes sin solicitarles consentimiento, basándose en una de las excepciones que señala el art. 9.2 del RGPD que, como hemos explicado, no resulta de aplicación.

Y la segunda excepción es si la tecnología de reconocimiento facial es necesaria para fines de seguridad, pero sólo en lo que se refiere a un interés público sustancial. El supermercado afirma que este es el caso. Pero la citada Autoridad de Control no lo considera así. La vicepresidenta de la Autoridad de Control de los Países Bajos indica que el único ejemplo en su país es la de seguridad en una central nuclear.

(Recuperado el 19 de febrero de 2021 de https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_es)

Por su parte, el Supervisor Europeo de Protección de Datos, como hemos indicado anteriormente, publicó un artículo el 28 de octubre de 2019 titulado "Facial Recognition: A solution in search of a problem?" abordando este tipo de tratamientos.

(Recuperado el 22 de febrero de 2020 de https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en)

En dicho artículo, se indica que *"The purposes that triggered the introduction of facial recognition may seem uncontroversial at a first sight: it seems unobjectionable to use it to verify a person's identity against a presented facial image, such as at national borders including in the EU. It is another level of intrusion to use it to determine the identity of an unknown person by comparing her image against an extensive database of images of known individuals*",

("*Los propósitos que desencadenaron la introducción del reconocimiento facial pueden parecer incontrovertidos a primera vista: Parece inobjetable utilizarla para verificar la identidad de una persona frente a una imagen facial presentada, como en las fronteras nacionales, incluso en la UE. Es otro nivel de intrusión utilizarlo para determinar la identidad de una persona desconocida comparando su imagen con una extensa base de datos de imágenes de individuos conocidos*". La traducción es de la AEPD)

Esto es, plantea dudas más que razonables por la intrusión que supone "*usarlo para determinar la identidad de una persona desconocida comparando su imagen con una extensa base de datos de imágenes de personas conocidas"* (uno-a-varios).

Y, añade, que "*any interference in fundamental rights under the Article 52 of the Charter must be demonstrably necessary. The bar for this test becomes higher the deeper the interference. Is there any evidence yet that we need the technology at all? Are there really no other less intrusive means to achieve the same goal? Obviously, 'efficiency' and 'convenience' could not stand as sufficient".*

("*toda injerencia en los derechos fundamentales en virtud del Artículo 52 de la Carta debe ser demostrablemente necesaria. La barra para esta prueba se vuelve más alta cuanto más profunda es la interferencia. ¿Hay alguna evidencia todavía de que necesitamos la tecnología para todo? ¿Realmente no hay otros medios menos intrusivos para lograr el mismo objetivo? Obviamente, la «eficiencia» y la «conveniencia» no podrían ser suficientes*". La traducción es de la AEPD).

Otra cuestión que destacamos de su artículo es la referencia al respeto de los principios de minimización de datos y de exactitud, cuando menciona que "*Facial recognition technology has never been fully accurate, and this has serious consequences for individuals being falsely identified whether as criminals or otherwise. The goal of 'accuracy' implies a logic that irresistibly leads towards an endless collection of (sensitive) data to perfect an ultimately unperfectible algorithm. In fact, there will never be enough data to eliminate bias and the risk of false positives or false negatives"*

("*La tecnología de reconocimiento facial nunca ha sido completamente exacta, y esto tiene graves consecuencias para las personas a las que se identifica falsamente, ya sea como delincuentes o de otro tipo. El objetivo de la 'exactitud' implica una lógica que conduce irresistiblemente a una colección interminable de datos (sensibles) para perfeccionar un algoritmo que en última instancia es posible. De hecho, nunca habrá suficientes datos para eliminar el sesgo y el riesgo de falsos positivos o falsos negativos*". La traducción es de la AEPD).

XVI

En el presente caso, **se debe concluir que el tratamiento de datos personales a través de reconocimiento facial en los términos que la mercantil ha implantado en sus supermercados, no permite aplicar la exención del artículo 9.2.f) del RGPD a la prohibición general que impone el artículo 9.1 de dicha norma**. En consecuencia, desde ese momento no es posible legitimar el tratamiento con base en los criterios de licitud del artículo 6 del RGPD. El tratamiento implantado se encuentra prohibido conforme a lo dispuesto en el art. 9.1 del RGPD, con independencia de las medidas de seguridad y condiciones de licitud expuestas en el artículo 6 del RGPD.

No obstante lo anterior, tampoco sería lícito acudir directamente a lo dispuesto en el artículo 6.1.e) toda vez que no se puede compartir que con la medida de identificación implantada se esté protegiendo el interés público, sino más bien,

los intereses privados o particulares de la empresa en cuestión, interés público que en todo caso deberá ser esencial. En el mismo sentido, la base legal dispuesta en el art. 6.1.b) RGPD tampoco es válida para los empleados toda vez que se trata de un tratamiento al margen del sistema de videovigilancia. Además, no consta normativa legal que lo permita según lo dispuesto en el artículo 8 de la LOPDGDD. Se debe insistir en que el tratamiento analizado se encuentra prohibido de su origen conforme señala el artículo 9.1 del RGPD

Por otro lado, la mercantil tampoco cumple con el derecho de información requerido en el artículo 12 y 13 del RGPD. En este sentido, no se informa de forma significativa sobre la lógica aplicada en el tratamiento de reconocimiento facial aplicado, ni permite a los afectados ejercer sus derechos dada la inmediatez del tratamiento. Se debe insistir en que el tratamiento analizado se encuentra prohibido de origen conforme señala el artículo 9.1 del RGPD

Tampoco consta que se cumpla el principio de minimización manifestado en el artículo 5.1.c) del RGPD. Los tratamientos llevados a cabo a través de tecnología de reconocimiento facial son tratamientos de riesgo extremadamente elevado (inaceptable), con alta probabilidad de incidencia y gravedad lo que hace que el riesgo inherente sea muy alto y muy complicada su disminución a riesgo residual aceptable, lo que permitiría con alta probabilidad que se realizaran tratamientos de diversa índole (incluidos los afectados por el artículo 9.1 del RGPD) y con gran impacto al margen de lo estrictamente necesario. Ante un nivel de riesgo “inaceptable” se debe recurrir a lo dispuesto en el artículo 36 del RGPD, consulta previa, que no consta realizada. Además, hay que tener en cuenta la incorrecta evaluación del impacto sobre los derechos y libertades de los afectados cuando no contempla la totalidad de los sujetos implicados. Se debe insistir en que el tratamiento analizado se encuentra prohibido de origen conforme señala el artículo 9.1 del RGPD

A mayor abundamiento, y sin perjuicio de que el tratamiento analizado se encuentra prohibido de origen conforme señala el artículo 9.1 del RGPD con independencia de las medidas de seguridad implantadas, el tratamiento analizado no dispone de las debidas salvaguardas de seguridad desde el diseño, toda vez que el sistema implantado realiza una evaluación sistemática y exhaustiva de aspectos personales de personas físicas a gran escala de datos de categoría especial. De hecho, consta que la entidad encargada de la lógica aplicada al tratamiento se compromete a garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: la seudonimización. En consecuencia, desde el diseño se admite la posibilidad de que el tratamiento de datos se lleve a cabo sobre personas identificadas de forma remota, masiva e indiscriminada.

Por último, y teniendo en cuenta todo lo anterior, en especial el alto nivel de riesgo sobre la vulneración de los derechos y libertades de los afectados por el tratamiento objeto de análisis, se considera proporcional el mantenimiento de la

medida cautelar impuesta al tratarse de un tratamiento prohibido desde su origen en aplicación de lo dispuesto en el art. 9.1 del RGPD.

XVII

Los hechos analizados podrían ser constitutivos de infracción, imputable al reclamado*,* por vulneración:

- del art. 9 del RGPD (tratamiento de categorías especiales de datos), tipificada en el art 83.5.a) de dicha norma y considerada muy grave a efectos de prescripción en el art. 72.1.e) de la LOPDGDD, pudiendo ser sancionada con multa de hasta 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5.a) del RGPD.

- del art. 6 del RGPD (licitud de tratamiento), tipificada en el art 83.5.a) de dicha norma y considerada muy grave a efectos de prescripción en el art. 72.1.a) de la LOPDGDD, pudiendo ser sancionada con multa de hasta 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5.a) del RGPD.

- de los arts. 12 y 13 del RGPD (transparencia de la información facilitada a los diferentes colectivos afectados), tipificada en el art 83.5.b) y considerada muy grave a efectos de prescripción en el art. 72.1.h) de la LOPDGDD, pudiendo ser sancionada con multa de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5.b) del RGPD.

- del art. 5.1.c) (principio de minimización de datos) y tipificada en el art. 83.5.a) y considerada muy grave a efectos de prescripción en el art. 72.1.a) de la LOPDGDD, pudiendo ser sancionada con multa de 20.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.5.a) del RGPD.

- del art. 25.1 del RGPD (protección de datos desde el diseño) tipificada en el art 83.4.a) y considerada grave a efectos de prescripción en el art. 73.d) de la LOPDGDD, pudiendo ser sancionada con multa de 10.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.4.a) del RGPD.

- del art. 35 del RGPD (evaluación de impacto), tipificada en el art 83.4.a) y considerada grave a efectos de prescripción en el art. 73.t) de la LOPDGDD, pudiendo ser sancionada con multa de 10.000.000 € como máximo o, tratándose de una empresa, de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía, de acuerdo con el artículo 83.4.a) del RGPD.

Asimismo, se considera que procede graduar las sanciones a imponer de acuerdo con los siguientes criterios conforme señala el art 83 del RGPD:

Art 83.1 del RGPD. efectiva, proporcional y disuasoria (tamaño de la empresa)

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias".

La reclamada tiene una cifra de negocios en 2019 (último informe de auditoría publicado) de más de 25.000 millones de euros y 90.000 empleados, por lo que constituye una gran empresa, con 1.636 tiendas abiertas.

Art 83.2 RGPD.

"a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido"

Los datos objeto de tratamiento son de categoría especial y el volumen de datos tratados puede superar los ******NÚM.7*** al año de reconocimientos faciales, incluyendo a menores y personas vulnerables. El tratamiento se realiza de forma remota, masiva e indiscriminada.

"b) la intencionalidad o negligencia en la infracción"

El desarrollo del sistema de detección anticipada ha sido promovido por el responsable. No consta que la reclamada haya optado por realizar consulta previa a la AEPD conforme señala el art. 36 del RGPD, aun cuando el tratamiento implantado constituye un riesgo extremadamente elevado inaceptable de origen para los derechos y libertades de los clientes y empleados de la mercantil.

"d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32"

El grado de responsabilidad es plenamente imputable a la reclamada y consta que las deficiencias e incompatibilidades del tratamiento son de decisión y responsabilidad propia, en concreto finalidad y medios.

"g) las categorías de los datos de carácter personal afectados por la infracción"

Desde el diseño del sistema se seguridad implantado consta que realizará una evaluación sistemática y exhaustiva de aspectos personales de personas físicas a gran escala de datos de categoría especial.

"h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida"

Consta que la AEPD tuvo conocimiento del tratamiento ahora analizado a través de dos reclamaciones ajenas a la reclamada.

"k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Artículo 76 de la LOPDGDD. Sanciones y medidas correctivas.

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

Como factores agravantes:

a) El carácter continuado de la infracción.

Costa que el tratamiento se está realizando desde 1 de julio de 2020, hasta el 6/05/2021.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

La reclamada es una gran empresa del sector de la distribución generalista con código CNAE 4711, sector "Comercio al por menor" en establecimientos no especializados, y realiza tratamiento de datos personales de clientes y trabajadores forma habitual.

(…)

f) La afectación a los derechos de los menores.

Consta que el tratamiento de datos implantado afecta a menores de edad y personas vulnerables que accedan a los establecimientos.

(…)

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 58.2 del Reglamento (UE) 2016/679.

4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica. Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación."

Como factores atenuantes:

Art 83.2) RGPD:

e) No consta reincidencia ni reiteración. Este atenuante ha sido de especial relevancia para establecer la cuantía de la multa pecuniaria ahora propuesta.

De lo anterior, se considera proporcional, efectivo y disuasorio imponer las siguientes multas administrativas conforme señala el art. 58.2.i) del RGPD que a continuación se indica:

- Por la supuesta infracción de los arts. 6 y 9 del RGPD, tipificadas en el art 83.5.a) de dicha norma y consideradas muy graves a efectos de prescripción en el art. 72.1.a) y e), respectivamente, de la LOPDGDD, multa administrativa de cuantía 2.000.000 €.

- por la supuesta infracción del art. 5.1.c) del RGPD, tipificada en el art 83.5.a) de dicha norma y considerada muy grave a efectos de prescripción en el art. 72.1.a) de la LOPDGDD, multa administrativa de cuantía 500.000 €.

- Por la supuesta infracción de los arts. 12,13 del RGPD, tipificada en el art 83.5.b) de dicha norma y considerada muy grave a efectos de prescripción en el art. 72.1.h) de la LOPDGDD, multa administrativa de cuantía 100.000 €.

- Por la supuesta infracción del art. 25.1 del RGPD, tipificada en el art 83.4.a) de dicha norma y considerada grave a efectos de prescripción en el art. 73.d) de la LOPDGDD, multa administrativa de cuantía 500.000 €.

- Por la supuesta infracción del art. 35 del RGPD, tipificada en el art 83.4.a) de dicha norma y considerada grave a efectos de prescripción en el art. 73.t) de la LOPDGDD, multa administrativa de cuantía 50.000 €.

XVIII

El art. 69 de la LOPDGDD, señala lo siguiente:

"Artículo 69. Medidas provisionales y de garantía de los derechos.

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación".

El Preámbulo I de la LOPDGDD dice: *"La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de*

Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno. El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. (…). Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva".

El artículo 56 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en cuanto resulte de aplicación, señala lo siguiente:

"1. Iniciado el procedimiento, el órgano administrativo competente para resolver, podrá adoptar, de oficio o a instancia de parte y de forma motivada, las medidas provisionales que estime oportunas para asegurar la eficacia de la resolución que pudiera recaer, si existiesen elementos de juicio suficientes para ello, de acuerdo con los principios de proporcionalidad, efectividad y menor onerosidad.

2. Antes de la iniciación del procedimiento administrativo, el órgano competente para iniciar o instruir el procedimiento, de oficio o a instancia de parte, en los casos de urgencia inaplazable y para la protección provisional de los intereses implicados, podrá adoptar de forma motivada las medidas provisionales que resulten necesarias y proporcionadas. Las medidas provisionales deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

3. De acuerdo con lo previsto en los dos apartados anteriores, podrán acordarse las siguientes medidas provisionales, en los términos previstos en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil:

a) Suspensión temporal de actividades.

b) Prestación de fianzas.

c) Retirada o intervención de bienes productivos o suspensión temporal de servicios por razones de sanidad, higiene o seguridad, el cierre temporal del establecimiento por estas u otras causas previstas en la normativa reguladora aplicable.

d) Embargo preventivo de bienes, rentas y cosas fungibles computables en metálico por aplicación de precios ciertos.

e) El depósito, retención o inmovilización de cosa mueble.

f) La intervención y depósito de ingresos obtenidos mediante una actividad que se considere ilícita y cuya prohibición o cesación se pretenda.

g) Consignación o constitución de depósito de las cantidades que se reclamen.

h) La retención de ingresos a cuenta que deban abonar las Administraciones Públicas.

i) Aquellas otras medidas que, para la protección de los derechos de los interesados, prevean expresamente las leyes, o que se estimen necesarias para asegurar la efectividad de la resolución.

4. No se podrán adoptar medidas provisionales que puedan causar perjuicio de difícil o imposible reparación a los interesados o que impliquen violación de derechos amparados por las leyes.

5. Las medidas provisionales podrán ser alzadas o modificadas durante la tramitación del procedimiento, de oficio o a instancia de parte, en virtud de circunstancias sobrevenidas o que no pudieron ser tenidas en cuenta en el momento de su adopción.

En todo caso, se extinguirán cuando surta efectos la resolución administrativa que ponga fin al procedimiento correspondiente".

En el tratamiento de datos sobre el reconocimiento facial ahora analizado y que consta que la reclamada estaba llevando a cabo desde el 1 de julio de 2020 (hasta el 6/05/2021) en diversos centros abiertos en España (al menos cuarenta), es un tratamiento de datos personales expresamente prohibido por el artículo 9.1 del RGPD

Consta que con fecha 6/05/2021, la reclamada llevó a cabo la ejecución de la medida cautelar impuesta aportando documentación fehaciente que lo acredita, apagando los sistemas implantados de reconocimiento facial y retirando la cartelería.

La adopción de esta medida provisional en el Acuerdo de Inicio y su confirmación y elevación a definitiva en la presente Propuesta de Resolución, pondera todos los derechos e intereses en conflicto y no deja sin efecto la medida de seguridad adoptada por los órganos judiciales, sino tan sólo el medio de reconocimiento facial para llevarlo a cabo, sin perjuicio de que el responsable del tratamiento pueda adoptar otros sistemas menos intrusivos para la consecución de tal finalidad.

En consecuencia, el tratamiento de datos basados en el reconocimiento facial con fines de identificación implantado por MERCADONA se encuentra prohibido por lo dispuesto en el artículo 9.1, al no constar ninguna causa que permita levantar la prohibición entre las expuestas en el art. 9.2 del RGPD, por lo que no procede ampararse en las causas de licitud del art. 6.1 del mismo. Tal prohibición no puede obviarse mediante la aplicación de medidas de seguridad proactiva, ya que la prohibición del tratamiento señalada en el art 9.1 del RGPD determina que sean irrelevantes, por lo que no se procede al análisis de las mismas.

A la vista de lo expuesto se procede a emitir la siguiente

PROPUESTA DE RESOLUCIÓN

Que por la Directora de la Agencia Española de Protección de Datos se sancione a **MERCADONA S.A.**, con NIF **A46103834**, por la infracción de los siguientes artículos y sanciones:

- art. 6 y 9 del RGPD, tipificadas en el art. 83.5.a), de dicha norma, multa administrativa de cuantía 2.000.000 € (dos millones de euros).

- art. 12 y13 del RGPD, tipificadas en el art. 83.5.b), de dicha norma, multa administrativa de cuantía 100.000 € (cien mil euros).

- art. 5.1.c) del RGPD, tipificada en el art. 83.5.a), de dicha norma, multa administrativa de cuantía 500.000 € (quinientos mil euros).

- art. 25.1 del RGPD, tipificada en el art. 83.4.a), de dicha norma, multa administrativa de cuantía 500.000 € (quinientos mil euros).

- art. 35 del RGPD, tipificada en el art. 83.4.a), de dicha norma, multa administrativa de cuantía 50.000 € (cincuenta mil euros).

- Confirmar la medida provisional impuesta a MERCADONA en el Acuerdo de Inicio sobre la suspensión temporal de todo el tratamiento de datos personales relativo al reconocimiento facial en sus establecimientos al resultar dicho tratamiento prohibido conforme a lo dispuesto en el RGPD y normativa conexa y sea elevada a definitiva.

Asimismo, de conformidad con lo establecido en el artículo 85.2 de la LPACAP, se le informa de que podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá una reducción de un 20% del importe de la misma. Con la aplicación de esta reducción, la sanción quedaría establecida en 2.520.000 € (dos millones quinientos veinte mil euros) y su pago implicará la terminación del procedimiento. La efectividad de esta reducción estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de la cantidad especificada anteriormente, de acuerdo con lo previsto en el artículo 85.2 citado, deberá hacerla efectiva mediante su ingreso en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa, por pago voluntario, de reducción del importe de la sanción. Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para proceder a cerrar el expediente.

En su virtud se le notifica cuanto antecede, y se le pone de manifiesto el procedimiento a fin de que en el plazo de DIEZ DÍAS pueda alegar cuanto considere en su defensa y presentar los documentos e informaciones que considere pertinentes, de acuerdo con el artículo 89.2 de la LPACAP). >>

SEGUNDO: En fecha 19 de julio de 2021, la parte reclamada ha procedido al pago de la sanción en la cuantía de 2.520.000 € haciendo uso de la reducción prevista en la propuesta de resolución transcrita anteriormente.

TERCERO: El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere la propuesta de resolución.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en el art. 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), la Directora de la AEPD es competente para sancionar las infracciones que se cometan contra dicho Reglamento.

II

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores",* dispone lo siguiente:

"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado, la Directora de la AEPD,

RESUELVE:

PRIMERO: DECLARAR la terminación del procedimiento sancionador de referencia PS/00120/2021 de conformidad con lo establecido en el artículo 85 de la LPACAP,

sancionando a **MERCADONA, S.A.**, con NIF **A46103834**, por la infracción de los siguientes artículos:

- art. 6 y 9 del RGPD, tipificadas en el art. 83.5.a), de dicha norma,
- art. 12 y13 del RGPD, tipificadas en el art. 83.5.b), de dicha norma,
- art. 5.1.c) del RGPD, tipificada en el art. 83.5.a), de dicha norma,
- art. 25.1 del RGPD, tipificada en el art. 83.4.a), de dicha norma,
- art. 35 del RGPD, tipificada en el art. 83.4.a), de dicha norma,
- Prohibir todo el tratamiento de datos personales relativo al reconocimiento facial en sus establecimientos, de acuerdo con el artículo 58.2.f).

SEGUNDO: NOTIFICAR la presente resolución a **MERCADONA, S.A.**, con NIF **A46103834** y con domicilio en Paseo de la Castellana n.º 259 C, 28046 Madrid.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

968-160721

Mar España Martí
Directora de la Agencia Española de Protección de Datos