AUDIENCIA PROVINCIAL DE BARCELONA

SECCIÓN NOVENA

EJECUTORIA nº 840/20

P.A 259/17

AUTO Nº 72/2021

Ilustrísimas Srías.:

Dª. Mª Fernanda Tejero Seguí

D. Carmen Sucias Rodríguez

D. Javier Lanzos sanz

En Barcelona, a 15 de Febrero de 2021.

ANTECEDENTES DE HECHO:

PRIMERO.- Con fecha 19 de enero de 2018, el juzgado de lo penal número 28 de Barcelona dictó sentencia de conformidad, condenando a Esmeralda y Juan Ignacio como autores de un delito intentado de robo con violencia en las personas, siendo condenados cada uno de ellos a la pena de prisión de un año, inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de condena y la prohibición, ambos, de acceso al centro comercial MERCADONA sito en la calle Frederic Mompou s/n de San Boi de Llobregat por tiempo de dos años, así como al abono de la mitad de las costas causadas en el presente procedimiento, respectivamente.

SEGUNDO.-Por auto de fecha 19 de enero de 2018 se dictaba auto por el que se procedía a conceder la suspensión condicional ambos condenados de la pena privativa de libertad impuesta. Por auto de fecha 12 de febrero de 2018 se dictaba auto de incoación de ejecutoria, requiriéndose a los condenados al cumplimiento de las penas impuestas en la resolución. En fecha 18 de abril de 2018 se procedía a la liquidación de condena por parte del juzgado de lo penal número 24 de Barcelona.

TERCERO.- En fecha 6 de mayo de 2019, por parte de la entidad MERCADONA S.A, se presentaba escrito en el que se venía manifestar que dado que, era prácticamente imposible asegurar por parte de dicha entidad el cumplimiento de la pena accesoria, dado que los trabajadores no podían estar pendientes de la gente que entraba en el supermercado y mucho menos de si éstos habían sido efectivamente condenados, instaba que se acordará permitir a dicha mercantil el uso de medios electrónicos, consistentes en la detección de entrada a los establecimientos de esta cadena respecto de los dos condenados, los señores Juan Ignacio y Esmeralda, tratándose de un sistema automático que detectaría la entrada de los penados, a través de medios electrónicos, esto es, a través de un circuito cerrado de video grabación y con ello se aseguraría la proporcionalidad de los medios utilizados al tiempo que la efectividad de la medida, añadiendo el interés público en virtud del artículo 14 de la Ley de Seguridad Privada y el interés legítimo de la mercantil de asegurar el cumplimiento de las resoluciones judiciales en las que la misma es la víctima/perjudicada.

CUARTO.- Dado traslado del escrito presentado al resto de partes personadas, el Ministerio Fiscal en fecha 21 de agosto de 2019 informó en el sentido de no corresponder al órgano judicial resolver sobre cuestiones de organización interna en el ámbito de las instalaciones a través de medios electrónicos, (aludidos de forma

genérica) de un centro comercial, excediendo la petición de la esfera competencial del órgano judicial de ejecución. Y en fecha 18 de septiembre de 2019, por la defensa del señor Juan Ignacio se informaba en el sentido de oponerse a la petición invocada en cuanto afectaba la protección del imagen legalmente establecida y que no podía ser vulnerada por el simple capricho de la mercantil, cuando los penados no tenían prohibido el acceso a ningún otro supermercado; entendiendo dicha parte que, la medida solicitada resultaba desproporcionada e inaceptable.

QUINTO.- El Juzgado de lo penal número 24 Barcelona dictó auto en fecha 27 de septiembre de 2019 por el que acordaba denegar la autorización a la mercantil MERCADONA S.A. para la utilización de medios automatizados de captación de datos biométricos de los penados en orden a poder detectar su entrada en cualquier establecimiento de dicha cadena. En fecha 25 de noviembre de 2020, por parte de la entidad MERCADONA se presentaba recurso de apelación con base a las alegaciones que consideró de pertinente aplicación, invocando finalmente la revocación del auto de fecha 27 de septiembre de 2019 y la autorización a dicha mercantil del uso de medios electrónicos para el cumplimiento de las medidas accesorias de prohibición de entrada.

En fecha 3 de diciembre de 2020, por la representación procesal del penado, señor Juan Ignacio, se oponía al citado recurso de apelación. No sin embargo, el Ministerio Fiscal, el cual compartía las alegaciones del recurso de apelación interpuesto frente al auto de fecha 20 de noviembre de 2020, interesando su estimación.

Ha sido Ponente de esta resolución, la Magistrada de esta Sección Novena de la Audiencia Provincial de Barcelona, Dª. Mª Fernanda Tejero Seguí, que expresa el parecer unánime del Tribunal previa deliberación y votación.

FUNDAMENTOS DE DERECHO:

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 eficaces 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.

Manifestar en última instancia que, el Ministerio Fiscal, sorpresivamente a lo que ya venía informando mediante escrito de fecha 21 de agosto de 2019, el 17 de diciembre de 2020 manifiesta compartir las alegaciones efectuadas el recurso de apelación, sin motivar en modo alguno la razón de dicha estimación y refiriéndose a un auto de fecha 20 de noviembre de 2020, que no existe en autos, o al menos, en el testimonio de particulares remitidos a esta sección, el mismo no consta. En consecuencia el Ministerio Público informa sobre una resolución inexistente.

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.

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 Juan Ignacio Esmeralda 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.

FALLO:

La Sala acuerda:

DESESTIMAR EL RECURSO DE APELACION interpuesto por la representación procesal de la Entidad Mercantil MERCADONA S.A, contra el Auto de fecha 27 de Septiembre de 2019, dictado por el Juzgado de lo Penal nº 24 de Barcelona, por el que se denegó la autorización a la citada mercantil/la utilización de medios automatizados de captación de datos biométricos de los penados, señores. Esmeralda Juan Ignacio, en orden a detectar su entrada en cualquier establecimiento de dicha cadena, radicado en Cataluña, y, por consiguiente, **SE CONFIRMA ÍNTEGRAMENTE** dicha resolución con declaración de oficio de las costas procesales causadas en este recurso.

Notifíquese la presente resolución a las partes, haciéndoles saber que contra la misma, que es firme, no cabe interponer recurso alguno.

Así lo resuelven y firman los Iltmas. Srías de la Sala; de lo que doy fe.

DILIGENCIA.- Seguidamente se cumple lo acordado en la anterior resolución, doy fe.