 Procedure No.: PS/00120/2021

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

Of the procedure instructed by the Spanish Agency for Data Protection and with

based on the following

BACKGROUND

FIRST: On May 5, 2021, the director agreed to initiate a procedure

sanctioning MERCADONA, S.A. (hereinafter the claimed party). notified on

initial agreement and after analyzing the arguments presented, on June 29,

2021, the proposed resolution was issued, which is transcribed below:

<< Procedure no.: PS/00120/2021

Of the procedure instructed by the Spanish Agency for Data Protection and

based on the following:

BACKGROUND

FIRST: On July 6, 2020, the Director of the Spanish Agency

of Data Protection (hereinafter, AEPD) agrees to initiate actions of

investigation in view of the news published in the media

regarding the implementation that Mercadona, S.A. (hereinafter, Mercadona or

claimed) would be carrying out in its establishments a system of

detection of those people with final sentences and restraining orders

in force against Mercadona or against any of its workers.

Subsequently, two claims were registered with the AEPD in relation to the

same facts:

On July 15, 2020, registration number 025103/2020, from the

ASSOCIATION OF CONSUMERS AND USERS IN ACTION-FACUA (NIF

G91344986).

On July 27, 2020, registration number 026511/2020, from APEDANICA (NIF G80593254).

SECOND: In view of the facts denounced in the claim and the documents provided by the claimant / of the facts and documents of the that this Agency has been made aware of, the Subdirectorate General for Inspection of Data proceeded to carry out preliminary investigation actions to the clarification of the facts in question, by virtue of the powers of investigation granted to the control authorities in article 57.1 of the Regulation (EU) 2016/679 (General Data Protection Regulation, in hereinafter RGPD), and in accordance with the provisions of Title VII, Chapter I, Second section, of Organic Law 3/2018, of December 5, on Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD).

As a result of the research actions carried out, it is found that the data controller is the claimed party.

In addition, the following extremes are noted:

INVESTIGATED ENTITIES

During these proceedings, investigations have been carried out on the following entities:

Mercadona, S.A., with NIF A46103834 and with address at Paseo de la

Castellana no. 259 C, 28046 Madrid.

The claimed company has a turnover in 2019 of more than 25,000 million billing euros and more than 94,000 employees, according to the latest audit report issued by the entity, which is why it constitutes a great business.

RESULT OF THE INVESTIGATION ACTIONS

The writing of these results is based on the information provided by Mercadona (entry registration numbers 026455/2020, 026457/2020, 026459/2020,

026463/2020,

026464/2020, and 027549/2020) and in the following documents incorporated into the this file through the corresponding diligence:

026461/2020,

026460/2020,

026462/2020,

Reference number 1: Official Gazette of the Mercantile Registry (hereinafter

-

BORME) of ***DATE.1, (...).

-

Reference number 2: BORME of ***DATE.2, (…).

Reference number 3: consultation made on November 5, 2020 of the

-

entity ***EMPRESA.1 in the Axesor business information service.

Reference number 4: report of the legal office of the AEPD of

-

reference number 010308/2019.

-

Reference number 5: guidelines on individual decisions

automated and profiling for the purposes of Regulation 2016/679

of the Working Group on the protection of personal data of article 29.

Reference number 6: extract of Law 5/2014, of April 4, of

-

Private security.

Reference number 7: extract of the Organic Law 10/1995, of 23

-

November, of the Penal Code.

Reference number 8: extract from the Royal Decree of July 24, 1889

-

by which the Civil Code is published.

-

Reference number 9: extract from the Spanish Constitution.

Reference number 10: report of the legal office of the AEPD of

-

reference number 36/2020.

Reference number 11: opinion of the ICO (Information Commissioner's

-

Office) entitled “The use of live facial recognition technology by law enforcement

in public places”, published on October 31, 2019.

-

Reference number 12: privacy policy published on the site of

Internet of Mercadona whose last update, according to the own

document, was produced on October 5, 2020.

It is noted that where this report refers to demonstrations,

descriptions, or statements made by Mercadona "in its writing" this

expression refers to the entry letter registered on July 25,

2020 with the number 026455/2020.

In order to achieve the greatest possible expository clarity, the

research results in the following sections:

1.

two.

3.

Four.

5.

6.

7.

8.

Context and deployment

Participants, recipients, and international data transfers

Contribution of the image to the judicial procedure and inclusion in the

Early Detection System (hereinafter SDA)

SDA activation, detection, and alert

Reception and validation of the alert, and communication to the Forces and

State Security Corps (hereinafter FCSE)

Periods of conservation of personal data

System architecture, impact assessment, and security measures

Purpose, legality, and proportionality

9.

Compliance with the duty of information

1. Context and deployment

Mercadona, as defined in its own writing, is a "global company that engages, among other activities of its corporate purpose, in the exploitation of a food supermarket chain. Thus, according to the data facilitates, has "1,636 stores and approximately 95,000 workers in Spanish territory". It also adds that, “at a generic level, it could be determined that a [sic] the approximate number of people who access each day to a MERCADONA store is ***NUMBER 1”.

It also states that "each year, the Company has approximately ***NUMBER 2 judicial processes that can end in more than ***NUMBER 3 judicial resolutions in his favor in which the accused is firmly condemned with restraining orders on MERCADONA's facilities”. To the

In this regard, he cites that they are the subject of a complaint and therefore “susceptible to being request an order prohibiting access to a Company store” the people who:

-

-

“They are repeat offenders in the crime of robbery or theft against MERCADONA.

Have stolen a large quantity of salable products

Have been reported and convicted of crimes related to the

-

facilities, goods or workers of MERCADONA

Threaten or attack their own workers or security guards

-

that provide service in MERCADONA stores

-

They commit illicit acts on MERCADONA's clients”.

In line with the above, it states that "the implementation of a system early detection using facial recognition technology in their stores […] motivated by the risk derived from the commission of criminal acts, with its corresponding risk for MERCADONA's customers and employees Due to the large number of crimes committed in its more than 1,600 centers distributed throughout the Spanish geography, against their employees or estate".

Mercadona explains that "a facial recognition process consists of compare a dubious biometric sample, obtained through one or several images of a person, against a database of biometric samples already indubitably associated with the identity of a person, which have been previously registered through one or several photographs”. To do this, add “Doubtful biometric samples are transformed into patterns. Subsequently, through facial recognition, the biometric samples are compared to the previously saved undoubted template, through algorithmic calculations that are evaluated based on matching thresholds previously established”.

Mercadona describes that the procedure consists of the following phases (the document number 1 of document 026457/2020 lists, in addition to these phases, the actions that each of them includes):

-

-

-

-

-

-

-

Contribution of the image to the judicial procedure.

Inclusion of the image in the SDA.

Activation of the SDA.

Detection phase.

alert phase.

Reception and validation of the alert.

Communication with FCSE.

The condensed information of the treatment can be consulted in the extract of the record of processing activities provided by Mercadona as part of the

document number 29 of document 026463/2020 that includes the activities of

processing of data related to the SDA. The next one is anticipated

information on it, the details of which are expanded upon in the following sections:

-

Data processing: management of the early detection system

Category of data processed: identification data; image; profile

-

biometric

Category of interested parties: subjects who access the centers of

-

Mercadona; subjects with a firm sentence.

-

Data origin:

Indubitable image: through the image provided in a final judgment in

either

which Mercadona is a part.

Real-time image: data capture through cameras

either

with facial recognition system of the centers in which said is active

system.

-

either

Legitimation:

Public interest

Sensitive data: treatment necessary for the formulation, exercise, or

either

the defense of claims

-

Recipients: FCSE; Courts and tribunals

Regarding the deployment of the system, Mercadona states "that on July 1, 2020 the Pilot Project of the Early Detection System in ***NUMBER 4 stores". It adds, however, that "the system solely and exclusively is active in ***NUMBER.5 stores of ***LOCALITY.1, that is, in the stores that are currently affected by a firm judicial resolution, in which that a restraining order be decreed as a measure, having provided MERCADONA the corresponding images in the procedure and establishing the possibility by the Court, to make it effective, the use of technological means.

In relation to future deployment, Mercadona explains that the purpose of the system is to protect the safety of customers and employees, "so the criteria to be followed in the deployment will obey will be evaluated [sic] according to the most vulnerable areas, where there may be a greater risk for customers or employees of MERCADONA, based on the number of court proceedings in progress. Regarding the number of interested include in the SDA states that "within those ***NUMBER 3 restraining orders on MERCADONA's facilities, the maximum number could be estimated of stakeholders included annually [sic] in the System”. However, it clarifies that

“These numbers are an approximation and may be increased or decreased accordingly.

function of the own knowledge of the technology by the courts or by

requests that could be made directly by the FCS”.

2. Participants, recipients and international data transfers

In its letter, Mercadona lists the following participants in the project:

-

The Mercadona Security Department.

Specifically, the following profiles are mentioned:

either

(…)

Mercadona reports that Mercadona staff have signed a commitment

specific confidentiality agreement relating to this project (in addition to the

commitments signed by any Mercadona worker). Thus, it facilitates

document number 8 of document 026464/2020, an example copy of this

confidentiality commitment.

either

(…)

The provision of the service implies the performance by ***EMPRESA.2 of the

either

treatment of registration, conservation and deletion of personal data, in the to the extent necessary for its execution.

Mercadona guarantees and declares that it has a legal basis

either

sufficient for the treatment of the data of the interested parties object of this

Agreement, in accordance with the provisions of the data protection regulations

data.

In general, subcontracting with third parties of

either

the services that imply the access and/or treatment, partial or total, of data

unless *** COMPANY.2 has prior, express authorization

and in writing from Mercadona.

Mercadona's personal data will be processed by ***COMPANY.2

either

solely to carry out the provision of the service. Yes ***COMPANY.2

It is considered necessary to carry out data processing with a

different purpose, you must previously request the written authorization of

Mercadona. In the absence of said authorization, ***EMPRESA.2 will not be able to carry out

said treatment.

The categories of interested parties whose data will be processed by the

either

***COMPANY.2 under this agreement are: Mercadona customers, people

with a restraining order or similar judicial measure to the installations of

Mercadona, people captured by the facial recognition system.

***EMPRESA.2 will only process identification data (name,

either

surnames and image) and the personal data associated with the biometric pattern in under this Agreement.

*** COMPANY.2 undertakes to guarantee, taking into account the

either

state of the art, application costs, and the nature, scope,

context, and the purposes of the treatment, as well as the risks of probability and

variable seriousness for the rights and freedoms of natural persons, the

application of appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk, which, where appropriate, includes, among others: the

pseudonymization and encryption of personal data; the ability to guarantee

confidentiality, integrity, availability and permanent resilience of the

systems; the ability to restore availability and access to data

quickly in the event of a physical or technical incident; a process of

regular verification, evaluation and assessment of the effectiveness of the measures

technical and organizational to guarantee the security of the treatment.

***EMPRESA.2 undertakes to notify Mercadona, without delay

either

improperly and within a maximum period of 72 hours, violations of the security of

the personal data of which it has knowledge, giving support in the

notification to the AEPD or other competent Control Authority and, where appropriate, to

the interested parties, of the security violations that occur, as well as to

provide support, when necessary, in carrying out impact assessments of privacy and in the prior consultation with the AEPD or other Control Authority

competent, when applicable.

*** COMPANY.2 agrees to keep, in writing, a record of all

either

the categories of processing activities carried out on behalf of

Mercadona.

***EMPRESA.2 undertakes to make available to Mercadona all

either

the information necessary to demonstrate compliance with the obligations

established in this Agreement and to allow and contribute to the realization of

audits, including inspections, by Mercadona or a third party

authorized by Mercadona.

The seventh stipulation of the agreement details the obligations of secrecy and

either

confidentiality (as well as the establishment of measures for its protection) to

which both parties are subject to even after the relationship has ended

contract in relation to the information and personal data to which they have

access.

either

(…)

***COMPANY.2 warrants that, in connection with the performance of the Agreement,

either

no processing of personal data will be carried out outside the Union

European Union or in a country that does not have an adequate level of protection.

The previous agreement also contains an annex dedicated to measures of

security in relation to: (…)

***EMPRESA.3, as a provider of private security and maintenance

-

of facial recognition systems. Refers to the profile of Responsible for

Production, exclusively for Mercadona as stated, as

responsible for directing and coordinating the exclusive technicians for the service in

Mercadona.

Attached as document number 10 of document 026459/2020, the Agreement of

Confidentiality and treatment of Personal Data on behalf of a third party

signed on December 29, 2011 between Mercadona and

***COMPANY.4.

According to BORME publication (reference number 1) ***EMPRESA.4 was

absorbed (...) by ***COMPANY.6 Subsequently, on ***DATE.2, the

published in the BORME (reference number 2) the entry as sole partner of

***COMPANY.5 in ***COMPANY.6. Likewise, it is stated (reference

number 3) the relationship of coincidence by corporate body and domicile between

***COMPANY.5 and ***COMPANY.3.

The purpose of the agreement is to regulate the treatment to be given to the entire

confidential information and personal data to which you have access

in the context of the services provided. It is referred to in the document, given the

date of signing, the personal data protection regulations made up of

Organic Law 15/1999 and its implementing regulations. The following stands out contents:

(…)

The treatment manager is obliged to:

either

either

(…)

“Adopt all technical and organizational measures required by the data protection regulations that are necessary to guarantee the security and confidentiality of personal data, avoiding the unauthorized alteration, loss, treatment, access or transfer.”

“Once the provision of services has ended, the personal data must be destroyed or returned to the issuing party (at the option of the latter), the same as any support or document containing any personal data treatment object.”

“All personal data provided is confidential, and under no circumstances can they be revealed.”

“The Treatment Manager must communicate and enforce their employees the obligations established in this Agreement and, specifically, those related to the duty of secrecy and security measures.”

On the other hand, in relation to the recipients of the information, it clarifies Mercadona in its writing that the only planned data communications are those derived from the disclosure of breaches of orders of removal from the FCSE, and from the competent courts and tribunals in the procedures. Likewise, document number 29 of document 026463/2020 which includes the definition of the treatment activity related to the management of the SDA, points out that these transfers would be made within the framework of a "legal obligation" of the person in charge.

Lastly, Mercadona points out that within the framework of this project no carry out international transfers of personal data.

3. Contribution of the image to the judicial procedure and inclusion in the SDA

In relation to the "indubitable" images against which the comparison, Mercadona points out that "it has taken into account that, without reliable and sharp images, meeting certain technical requirements explained later, it would not be possible to carry out the intended activity".

It indicates that, "for this reason, prior to the implementation of the System, made numerous tests (...) verifying that the system works correctly correct". He adds that, "all this, tending to avoid errors in the systems biometrics that, where appropriate, could lead to serious consequences for the person and, in particular, the erroneous denial to authorized persons and the erroneous acceptance of unauthorized persons that could cause serious problems at very different levels, as evidenced by the Agency in its Report 010308/2019" (reference number 4).

On this particular Mercadona attaches a document (document number 3 of writ 026457/2020) that details "the technical requirements for images of the system". From this document, written in English and entitled "Face Enrollment Best Practices", the following content is underlined:

-

(…)

About the source from which these images would be obtained, first Mercadona states that “regarding the final convictions that are the result of criminal proceedings in which MERCADONA is a party to the proceedings, The images are obtained from the video surveillance cameras that it has in its facilities and that were provided in the procedure as evidence, being validly obtained and admitted by the Court or Tribunal competent".

Specifically, Mercadona indicates that when a complaint is made for facts that are related to the facilities, goods or workers of Mercadona, the lawyers responsible for the stores request via email to the CAS the images of the facts and the author or authors. Next, "(…)". aim Mercadona that the people in charge of locating and extracting the images “have the classification of “Manager” of viewing images, a position that requires specific training in security and video surveillance, as well as specific training on the operation of this system”.

Next, it expresses that the images “(…)”.

Mercadona indicates at this point that it has a registry, which it calls “DAM images request”, which consists of “a list of internal work and exclusive to the CAS with the following fields:

-

-

-

-

-

Area: number of the store area to which the center belongs

Center: store number.

Name: name of the center.

Population: municipality where it is located.

Province: in which it is located.

Image request date: date on which the lawyer requests the

-

images to the CAS.

-

-

-

Observations: annotations that you want to record.

Delivered: to FCSE, Court or blank if not done.

Trial date.

Sentence: prohibition of access, restraining order or blank if not

-

has been dictated.

Settlement of sentence: upon receiving it, it is filled with a yes, in case

-

Otherwise, pending is indicated.

Start date: in the liquidation of sentence it appears from which day the

-

condemned person cannot enter.

End date: end date of the sentence of prohibition of access or

-

Restraining order.

***FILE.1: unique identifier that matches that of the

-

Court procedure.

Identification date: day and time on which 100% of the

-

person condemned to not be able to enter that store.

Identification store: center where 100% of that store has been identified.

-

person.

CAS Managers: Names of the Viewing Managers present in the

-

confirmation of identification of that person."

As he explains, at this moment the petition is registered in the list and the

different fields are completed as appropriate throughout the

different phases.

Mercadona attached (document number 2 of letter 026457/2020) on

document "DAM images request".

It adds that “in the event that the judicial decision determines the order of remoteness, the images contributed to the procedure would become indubitable biometric sample and, consequently, would be transformed into template". Regarding the territorial scope, it states that "it will be defined by the firm judicial resolution, which may be limited to one store, several or the territory determined by the pertinent Court”.

Second, “in relation to those convictions in which MERCADONA is not a party to the procedure (in the case of restraining orders for crimes committed against MERCADONA employees - alleged violence of gender, for example-) and the Courts and Tribunals directly request the collaboration with MERCADONA, in relation to the scope of the order of removal to the victim's workplace, to enforce the orders of removal, it will be the Courts and Tribunals themselves who will communicate, to through the appropriate judicial resolution, to MERCADONA the need for its collaboration to guarantee said effectiveness, as well as the terms of said measure, in relation to aspects such as the duration of the same and stores on which it would be applicable”. As he states, “in these cases, these images will have been provided in the procedure of which the judicial resolution brings cause and justification for its use will be determined by the requirement of use of technological means for the specific restraining order”. Y adds that in these cases it would need that "the Courts and Tribunals directly, or through the FCSE, delivered valid images, which meet the stated requirements that the facial recognition system needed to establish a prior indubitable sample”.

It also exposes the case in which "the request comes directly from FCSE or ***ORGANISMO.1, based on an investigation found to be carrying out or issues related to *** SUBJECT.1”. About,

states that “in order to use the analyzed system, it must be provided, likewise, of the guarantees exposed (specifically, when appropriate, the established by the regulations on data protection), namely, order based on law, photograph on which the certificate can be obtained biometric pattern, temporal delimitation of the measure and stores on which would be applicable."

In relation to the inclusion of the images in the SDA, Mercadona points out that, “once MERCADONA has a firm judicial resolution that determine the imposition of a restraining order or similar judicial measure regarding one or several MERCADONA stores, the lawyer responsible for the file, send an email to the CAS” indicating the number of judgment, the centers affected, and the period of validity, and attached the “pdf document. with liquidation of sentence/precautionary measure”. Thus, detail Mercadona that "the image is incorporated into the system with the territorial limitation of the area or stores determined in the judicial resolution, indicating the limitation temporary term or expiration of the restraining order, which comes determined in the court decision.

According to Mercadona, this process involves completing the information of the “DAM images request” register. After that, the Department Security, in order to make a new registration in the system, uses a “file” with the following information:

- Judicial procedure number.

- Description, including telephone numbers of the FCSE to call and of the surveillance service if available in the center, start date and end date of detection, and a brief description of the judicial measure. Document number 4 of document 026457/2020 contains the telephone list associated with the different Mercadona centers.

- Cluster: (…).

In the event that the judicial decision is acquittal or the measure is denied injunction, Mercadona points out that "the lawyer responsible for the case would send a email to the CAS, for the elimination of the blocked images”. It would cause the deletion of the images and the updating of the list "Petition DAM images.

4. SDA activation, detection and alert

As Mercadona describes, (...).

To track the completion dates of the judicial measure, use the application “***APPLICATION.1”. (...). Add that access to the system requires individual username and password that are provided by the

Computer Department.

Once the system is activated, “through facial recognition cameras,

The images captured in real time will be verified with the

undoubted image or images that have been included. This process of

check lasts tenths of a second (0.3 seconds today) between

that an image is captured and verification is performed against the image

indubitably included in the System”.

In relation to the cameras installed in each center, the following is underlined

information contained in the letter:

-

(…)

Mercadona "has proceeded and will proceed to comply with the duty of

-

information (...) in those centers in which the

installation of said cameras, even if they are not activated

to meet the privacy expectation of customers and employees.”

In relation to capturing the image by the camera, Mercadona provides the

following documents:

Document number 5 of document 026457/2020, (...), qualified as

-

confidential. This document written by “***EMPRESA.2” in English and

entitled "***TITLE.1" presents the results obtained after analyzing the potential

gender bias and skin color in the facial recognition system

“***APPLICATION.2” of ***COMPANY.2. The document concludes that the system

is not biased based on these attributes.

Document number 6 of document 026459/2020, “description of the system

-

used by ***APPLICATION.2, in the extraction of the biometric pattern and its comparison in relation to the anonymization process used”. The document, drawn up in English by ***COMPANY.2, is titled “***TITLE.2”.

Some of the system features described in the document are:

either

(…)

Document number 7 of document 026459/2020, “***DOCUMENT.1”. The

-

document, drawn up in English by ***EMPRESA.2, is titled “***TITLE.3” and includes an explanation of the facial recognition process, which follows the following phases: detection, feature extraction, adjustment, and recognition. Define result as the distance between the analyzed pattern and the

inscribed comparison pattern. He adds that the probabilities that this distance are greater between different subjects increase if the quality is improved of the images.

Likewise, Mercadona describes in its letter (pages 24-33) the evaluation that has carried out in order to assess the effectiveness of the detection system. As he explains, the tests have been carried out with a detection threshold of X,XX since it would be the one recommended by the manufacturer ***COMPANY.2. to optimize the relationship between detections and false positives. Thus, it states that "a person detected with score X,XX means that it has a similarity of at least YY% to the

system reference image.”

It also adds that the tests have been carried out using the solution

“*** APPLICATION.2 version 2.2 of the manufacturer *** COMPANY.2” on different

camera types, configurations, reference images (...) and scenarios (...)

that have allowed you to select the combination that offers the best results.

As stated in the letter, in the tests carried out there would have been no

no false positive.

In addition, it points out in relation to the process of detecting a person with

mask that:

“The IT solution provider has developed an enhancement with

in order to identify people with their faces semi-hidden by these masks, as

as can be seen in the images provided throughout the writing.

In this sense, it is important to point out that the

facial recognition based identification by collecting information from the

periocular area of the face (...).

The system loses information since part of this area is hidden, for

which has optimized the reading of the visible part without lowering the threshold (treshold

[sic]) of identification.”

Having made these clarifications regarding the tests of the system's effectiveness,

describes the process of generating the alert:

“Once the Early Detection System has been activated in the store(s)

object of the final judgment and in the event that any of the chambers of

facial recognition installed in stores to detect the access of a

person whose image is included in the ***APPLICATION.2 system,

would generate an alert that would initiate the process of confirmation and notice to the FCSE.

This alert that detects the coincidence in the cameras of the store is

sent by email to a specific address prepared for this purpose […]

Only the following have access to this email account:

profiles:

-

-

-

-

The Project Manager.

CAS Coordinator.

Managers, shift managers at the CAS.

Image viewing managers.

[…] If someone else needed to access this account, they would have to

expressly request the person in charge of the Project, the need for this new

access.

This alarm mail indicating the coincidence of the images in a

specific store, it is generated by each of the store teams”

Mercadona provides an example of the email sent in its letter (pg. 21). Is according

indicates, the following information is sent in the mail:

-

-

-

-

-

-

-

-

-

-

"Title: (…)

Name: (…)

Cluster: (…)

Center: (…)

Camera: (…)

Date and time of detection.

Coincidence: (…)

Description: (…)

Reference image: (…)

Detection Image: (…)

5. Reception and validation of the alert, and communication to the FCSE

As Mercadona describes, the process involves "a double factor of verification of the positives to avoid the risks derived from a treatment exclusively automated. Thus, it emphasizes that "once the alert is received, the same will be contrasted by the Viewing Managers of the Attention Center to Security present at that time, being confirmed (only in the case of that all Viewing Managers confirm that it is the same person) or unconfirmed (if any of them presents doubts at the time of confirm that it is the same person). In the event that it is not confirmed, the image will be destroyed, studying the technical reasons for the alarm and the process will end. As he points out, "the CAS Viewing Managers they have sufficient experience and training to carry out this verification".

Mercadona emphasizes in its letter that "this verification by the responsible for the Department of Security is totally mandatory in the process". Thus, he understands that "due to the subsequent verification process, In no case would there be a treatment through an automated decision".

To make this statement, it is based on the "Guide of the Working Group of the Article 29 on automated decisions published on October 3, 2017" (reference number 5).

After confirming the alarm, as Mercadona describes, a Manager of viewing will take care of:

(…)

Once this process is closed, the image will be extracted object of detection, to avoid unnecessary treatments on it more beyond its contribution to the competent authorities."

6. Periods of conservation of personal data

Mercadona states in its letter that "(...)"

Next, Mercadona differentiates between two assumptions. So, first of all, describes the behavior of the system during the detection phase in relation to with people whose image does not match any of the images

stored in the system:

“All necessary technical and organizational measures have been taken

in order to minimize any potential data processing and

limit it to mere technical residual storage (strictly necessary

for the proper functioning of the system).

“The facial recognition system will detect (automatically and

for an insignificant amount of time) and will analyze the images individually that

receive from each center. (…)

Regarding the assumption of detection of a positive (coincidence with

an image from the database), Mercadona expresses the following:

(…)

All of the foregoing is consigned, in a summarized manner, in the evaluation of

impact of privacy (document 30 of document 026463/2020). So this one

states that:

“The data will be kept:

(…)

Lastly, it is stated that, as observed in the activity log

of treatment (attached extract as document number 29 of the written

026463/2020), the management of the SDA and video surveillance are activities of

independent treatment. In the case of the processing of personal data

Regarding the video surveillance activity, the consigned conservation period is

thirty days.

7. System architecture, impact assessment, and security measures

Document number 29 of document 026463/2020 includes the risk analysis

related to the management of the SDA. This gives this treatment activity a

medium inherent risk and low residual risk after implementation of measures

mitigating. Among other issues, the analysis indicates that the activity involves:

"(...)". This leads you to determine the need to run a “PIA”.

Document number 30 of document 026463/2020 corresponds to the

privacy impact assessment of the project. This includes the evaluation

of the risk inherent to the treatment through the analysis of ***NUMBER 6 threats.

The result you get is that the level of risk is “tolerable”. It underlines the

content related to the following threats:

(…)

Likewise, it is stated in the impact assessment that "there has been a

examine the Project, once operational, to verify that the risks

detected have been properly addressed and that no other

new".

The privacy impact assessment also includes the content

following in the fifth section dedicated to the conclusions:

“(…)”

On the other hand, Mercadona describes in his writing (pp. 35-49) the architecture of the SDA and the security measures implemented. According to it, the elements that make up the architecture are:

-

(…)

-

Store equipment.

Store cameras.

(…)

-

(…)

-

(…)

-

either

-

CAS teams.

System ***APPLICATION.2 version 2.2.0. of ***COMPANY.2.

About the stores:

(…)

About the CAS:

(...) from the Mercadona Security Division or have an authorization

either

this.

-

(…)

-

either

About the facial recognition program:

Regarding Mercadona's own systems on which the SDA is based:

(…)

7. Purpose, legality and proportionality

Mercadona points out that "it can be concluded that the purpose served by the installation of the Early Detection System is to comply with the judicial resolutions in which the defendant has been sentenced with a restraining order, as a consequence of facts related to

the facilities, goods or workers of MERCADONA, in certain special circumstances and whenever established by a judicial resolution sign".

Regarding the basis of legitimacy, Mercadona states that "the treatment of data carried out by MERCADONA in order to preserve the safety of people and property, as well as its facilities is place in the public interest." Thus, Mercadona also cites in its letter the following content of Report 010308/2019 of the AEPD (reference number 4):

“In the present case, we have already mentioned how article 22 of the LPDGDD regulates processing for video surveillance purposes whose legitimacy is found, as indicated in its Opinion by the Council of State and has collected by the Law in its Statement of Motives, in the existence of a purpose of public interest incardinable in article 6.1.e) of the General Regulations, as it has for the purpose of "preserving the safety of people and goods, as well as their installations".

To this end, Mercadona states that "the treatment carried out to preserve the safety of people and property, as well as its facilities (the mentioned by the AEPD in the mentioned Report, as an example of treatment protected in the public interest) is the main purpose of the treatment of data carried out by MERCADONA”.

On the other hand, Mercadona brings up that "article 8 of the Organic Law 3/2018 […] contains the following: “The processing of personal data may only be be considered founded on the fulfillment of a mission carried out in the interest public or in the exercise of public powers conferred on the controller, in the terms provided for in article 6.1 e) of Regulation (EU) 2016/679, when derives from a competence attributed by a norm with the force of law”. Based on the foregoing, it is in the interest of this part to mention that the norm with the rank of law that enables MERCADONA to adopt mechanisms that detect and mitigate the commission of fraudulent conduct regarding the treatment carried out to preserve the safety of people and property, as well as their facilities, is Law 5/2014, of April 4, on Private Security (such as example article 4 on the purposes of the rule or article 8 on its guiding principles).”

Included in the file, reference number 6, is an extract of the aforementioned Law 5/2014 in which the wording of articles 4 and 8 appears.

On the other hand, Mercadona states that "there is no doubt that the treatment of data carried out by a facial recognition system would fall within

of the special data category. Regarding this, he states that "he will only

use the System in the event that it is part of a procedure

in which, through a firm resolution, the use of

facial recognition to enforce restraining orders. Therefore, my

represented considers that the analyzed treatment has a place in the article

9.2.f) by virtue of which sensitive data could be processed when “the treatment

it is necessary for the formulation, exercise or defense of claims”. In

In connection with the above, add the following:

"(...)".

This argument is defended by the Courts and Tribunals, when

position themselves in favor of the defended MERCADONA option, authorizing the

said sentence is controlled through electronic means, in order to

facial recognition, by virtue of the provisions of article 48.4 of the CP.”

An extract of the Law has been incorporated into the file (reference number 7).

Organic 10/1995, of November 23, of the Penal Code that contains the

wording of article 48.

In addition to the foregoing, he also adds that:

“it is worth bringing up article 1 of the CC in which the

Next:

"1. The sources of the Spanish legal system are the law, custom and general principles of law.

2. Provisions that contradict another of high rank shall be invalid.

higher.

(…)

6. The jurisprudence will complement the legal system with the

doctrine that, in a reiterated way, establishes the Supreme Court when interpreting and

apply the law, custom and general principles of law.

7. The Judges and Courts have the inexcusable duty to resolve in

In any case, the matters of which they are aware, adhering to the system of sources

established."

Therefore, it could be concluded that, since the Judges and Courts have

the inexcusable duty to resolve in any case the matters that they know,

attending to the established system of sources, the fact that a Judge has

considered appropriate to use a facial recognition system to

guarantee compliance with restraining orders in the facilities of

MERCADONA, would have enough weight to legitimize the treatment.

Moreover, it is worth mentioning article 24 of the CE, which rises to the

category of fundamental right and that regulates the right of defense within the

which includes the right to effective judicial protection, according to which all

people have the right of access to the jurisdiction, that is, they must have the

possibility of going to the jurisdictional bodies and formulating before them guardianship petitions. Likewise, the right to effective judicial protection also includes the right to have the jurisdictional bodies rule on the claim made and thus issue a resolution on the merits of the matter, motivated and founded on Law.

In addition, the Constitutional Court has understood that within the right to effective judicial protection is found, as a manifestation necessary, the right that the defendants have to have the sentences that ordinary courts have issued for the protection of their rights and interests legitimate are forcefully enforced. This right to forced execution thus links with the jurisdictional power that the EC recognizes to the courts in its article 117.

[…] And, in addition, all legal entities (public or private) has the obligation to comply with final judicial resolutions and must collaborate with the courts and tribunals in the execution of the resolution, as provided article 118 of the CE.

In any case, the beneficiary of a court decision has an authentic subjective right, which has the character of a fundamental right, connect directly with the right to effective judicial protection of article 24.1 of the CE, and is qualifiable as public subjective law, since it is required with respect to the jurisdictional organs of the State."

An extract from the Real Decree of July 24, 1889 by which the Civil Code is published that contains the wording of articles 1 and 3. Likewise, it has also been included (reference number 9) an extract of the Spanish Constitution that includes articles 24, 117 and 118.

Regarding the legality of the treatment, Mercadona concludes that "it

compliance with the provisions of the AEPD in its Reports 36/2020 and
010308/2019, based on the fact that “the existence of a public interest does not legitimate
any type of processing of personal data, but must be, in
firstly, to the conditions that the legislator may have established, such as
provides for article 6 RGPD, in its sections 2 and 3 […]. And in case they go
to be subject to treatment any or some of the personal data included
in the special categories of data referred to in article 9.1 RGPD, which
concurs any of the circumstances contemplated in its section 2 that
lift the ban on the processing of said data, established on a

general in its section 1”, insofar as the treatment would be legitimized
by article 6.1.e) RGPD based on the public interest derived from the need
to preserve the safety of customers, staff and facilities and for the
article 9.2.f) to be able to respond to the processes in which it is a party and in which
that the use of said technology has been determined as a measure to recognize
to the subjects subject to a restraining order.”

Report 36/2020 has been incorporated into the file (reference number 10)
issued by the legal office of the AEPD.

On the other hand, Mercadona states that the purpose of the system implies the
processing of data related to criminal convictions and infractions. explain, not
However, this type of data was already processed prior to the implementation
of the system since it is a common practice in the sector to identify those

people who may pose a risk to ensure the safety of the workers and customers. Consequently, he states that “the system studied in this writing comes to carry out this same treatment, not assuming a different activity in relation to the processing of personal data relating to criminal penalties or convictions.

To support the legitimacy of the treatment of this type of data, in its written Mercadona (referring to articles ten of the RGPD and the LOPDGDD) states that it “processes data related to convictions and infractions prisons under the supervision of public authorities, since the treatment carried out by MERCADONA is fully legitimized, because it is only carried out backed by the Administration of Justice or the FCSE.[…] the treatment will be carried out only on those judicial resolutions in which MERCADONA is a party, so it is not would generate a database of criminal convictions, being the use of data biometrics a specialization within the already existing and necessary treatment, since MERCADONA is part of the procedure or has been required by the Courts and Tribunals themselves.

In relation to the suitability, necessity and proportionality of implementation of the system, Mercadona states that:

“Compliance with a restraining order in a store can only

-

ensured effectively through electronic means, given that MERCADONA has 1,636 stores and approximately 95,000 workers in Spanish territory and each year, the Company has approximately ***NUMBER 2 judicial processes that can end in more than ***NUMBER 3 judicial resolutions in his favor in which the accused is firmly condemned with restraining orders on MERCADONA's facilities".

"A large part of these judicial resolutions are against people who

-

they act within organized gangs or are especially dangerous

for bosses and workers, on which it is unfeasible to comply

to judicial resolutions and enforce sentences without the use of

technological mechanisms, since the convicts go to the shops

MERCADONA with a very different physical appearance (costumes, wigs, etc.), which

that makes visual recognition difficult for security personnel.

security to those people who have a prohibition of access, more

even taking into account that, approximately, ***NUMBER 1 people enter the

day in a MERCADONA store".

Although the end pursued could be achieved by other means

-

(through security guards who control access to stores, for

example) these do not guarantee the reliability of technological solutions based on

in biometrics, which allow achieving the goal pursued by MERCADONA

with greater guarantees and reliability and, therefore, greater legal certainty".

"the requirement that data processing be "strictly"

-

necessary, likewise, it is justified insofar as the measure of immediate intervention is necessary in cases of flagrante delicto, such as Noncompliance with a sentence that precisely tries to prevent recidivism and, above all, the safety of MERCADONA's clients and workers".

On this point Mercadona adds that "this argument is reinforced by the British Data Protection Authority, Information Commissioner's Office, in the document "The use of live facial recognition technology by law enforcement in public places 31"[sic] of October 2019, indicating that "the The purpose for which the facial recognition system is deployed is to great importance since there is a considerable difference between the use of facial recognition to mitigate certain serious or violent crimes and widespread deployments of facial recognition technology to identify known thieves."

The document entitled

"The use of live facial recognition technology by law enforcement in public places" published by the ICO (Information Commissioner's Office)

"the treatment in question only generates benefits and advantages for the

-

general interest, as well as for MERCADONA's clients and workers, as for the Courts and Tribunals themselves, since it is the only way efficient to make effective the measures decreed by them and; for the FCSE, by guaranteeing the System a collaboration with them, facilitating the performance of their duties".

It concludes that the system “meets the requirements of proportionality and is strictly necessary to fulfill the intended purpose, since it does not there are less intrusive means for user privacy that allow to obtain the objective pursued, as it is technically impossible effectively control the entry of sentenced persons with a prohibition of access to the facilities without the use of a mechanism technological". Thus, it expresses that “opting for an alternative mechanism would imply, without a doubt, an alteration of the purpose of the treatment pursued”.

Thus, it adds that "due to MERCADONA's interest in the implementation of the facial recognition system, since March 2019, in the judicial procedures in which it has been a party, it has been requested to the Administration of Justice the establishment of measures against reported in relation to access to MERCADONA establishments of a certain territorial area, according to the reported facts, for a certain period of time, making effective the control of said measured through electronic means in order to facial recognition” obtaining as a result that “each and every one of the Courts to which has made the request, they have considered the facial recognition system a adequate means to ensure compliance with restraining orders (…) by virtue of the provisions of article 48.4 of the Penal Code.”

8. Compliance with the duty of information

In its brief, Mercadona lists the following mechanisms used to comply with the duty of information:

Informative posters about the facial recognition system placed

-

visible at the entrances to each of the stores.

Attached, document number 18 of document 026461/2020 and document 18 of written 026463/2020, a copy of the signage that has been installed in “the accesses to sales room” in which the SDA has been implemented. The poster includes, under the heading “EARLY DETECTION ZONE”, information on the person responsible for treatment, the operation of the system, the recipient of the information (FCSE), the legal basis of the treatment, and the possibility of exercising the rights of data protection and to file a claim with the AEPD. Also,

Several ways are provided to consult additional information about the treatment (store interior, telephone, website).

In this regard, it also expresses that "the informative badges have a size enough so that any user can read its content and they are located in a sufficiently visible place, at the entrance of the store, taking into account

Note that the duty of information must be prior to the processing of the data, for the sake of rigorous respect of this part with the principle of transparency and the own duty of information.”

-

The Privacy Policy of the Mercadona website

Attached, document number 19 of document 026461/2020, copy of the policy of privacy of Mercadona published on the Internet whose last update, according to states in the document itself, it occurred on July 1, 2020.

In the section on categories of data processed, the "data biometrics (in those stores in Spain where it is implanted [sic] the early warning system).

In the section corresponding to the purposes, it mentions: “carry out the precise actions to protect the vital interests of customers when so necessary, or compliance with judicial resolutions and measures in them agreed.”

In the section dedicated to retention periods, it expresses the following:

“In relation to the protection of the vital interest of people and the execution of the sentences or resolutions that entail restraining orders on the work centers and/or people, the data will be processed and guarded for the time essential to comply with the judicial measures [sic] of those persons sentenced to said restraining order (in those stores in Spain where the early detection system is implemented).

However, the data collected incidentally to comply with said purpose will remain on the server only in the process of check (this check lasts tenths of a second). One time

Once this verification has been carried out, it will proceed to be definitively destroyed (in those stores in Spain where the detection system is implemented advance)."

Regarding legitimacy, the privacy policy states that “in the case of treatment of sensitive data will be treated for reasons of public interest with the consequent considerations provided by the regulations of data protection, which must be proportional to the objective pursued, which is enforce the law, respecting the other principles of the regulations of data protection and establishing the appropriate and specific measures to protect the interests and rights of the interested parties, based on the Law of the Union or of the Member States (in those stores in Spain where the early detection system is in place).”

Likewise, the section entitled “Other data that we process at Mercadona” contains the following paragraphs:

"In the same way we inform you that, in order to improve the security of customers and employees, MERCADONA, based on the public interest, may treat its image or your biometric facial profile to identify subjects with a warrant removal (or analogous judicial measure) in force against MERCADONA or against any of its workers (in those stores in Spain where it is early detection system implemented).

Said image will only be used for this purpose and will remain in the central server only in the verification process (this verification lasts tenths of a second). Once this verification is done, it will proceed to be definitively destroyed (in those stores in Spain where it is early detection system implemented).

These images will only be processed internally by MERCADONA, being exclusively communicated to the Security Forces and Corps for protect the safety of MERCADONA's clients and workers and the compliance with the measures decreed judicially (in those stores of Spain where the early detection system is implemented).

It has been incorporated (reference number 12) the privacy policy published in

Mercadona's website whose last update, as stated

in it, it occurred on October 5, 2020.

-

The customer service phone.

Attached, document number 20 of brief 026461/2020, copy of the arguments

phone number used in connection with the SDA describing the

system operation.

Informative forms made available to those interested in the

-

stores to deliver them to them if requested.

Attached, document number 21 of document 026461/2020, copy of the form in the

which describes the operation of the system, exposes the legal basis of the

treatment, informs of the possibility of exercising the rights of protection of

personal data and to file claims with the AEPD, and refers to the

privacy policy in order to obtain more information.

Similarly, attached Mercadona (document number 28 of the letter

026464/2020), the copy of the email that, according to what he states, he directs in

“Security Manager” to the “Store Managers”. In it, it is reported

on the documents that should be printed and provided to customers and

workers requesting more information about the SDA.

-

Mercadona's communication plan.

Attached, document number 22 of document 026462/2020, an extract from the document "Communication Plan for Early Detection" whose date of creation, as stated therein, is June 1, 2020.

In addition to the foregoing, Mercadona states in its letter that, on a Prior to the launch of the pilot project, he directed a press release (attach copy as document number 23 of document 026462/2020) at news agencies of the affected cities in order for it to be published in the media and thus make the project known to residents of these areas. Likewise, it indicates that on July 3, 2020, I send these same agencies “some FAQs about the project” (provides a copy as a document number 24 of letter 026462/2020). Among other issues, it focuses on this list of questions and answers in which "two systems coexist in stores independent of each other. On the one hand, conventional video surveillance, and on the other another, early detection.” This issue is also reflected in the record of treatment activities (attached extract as document number 29 of writ 026463/2020), in which the management of the SDA and video surveillance are listed as separate processing activities.

Likewise, Mercadona indicates that it has informed its workers about the treatment carried out by the SDA through various actions. Thus, it facilitates document number 25 of document 026462/2020, the text that, according to what it states, would be available through the “employee portal”. This text includes information about the person in charge, the purpose, the legal basis, and the possibility of exercising the personal data protection rights as well as to file a claim before the AEPD. Document number 26 of document 026462/2020 is corresponds to the information addressed to the "Intercenter Committee". In this writing, dated June 30, 2020, the start-up date of July 1, 2020 of the system in various stores. Lastly, it states that the Department of Communication would have produced a video "so that their workers understood the Project perfectly”. Contribute (document number 27 of the letter 026463/2020) the argument of the same.

To conclude, Mercadona mentions that "since the System was installed, MERCADONA has only received a request to exercise rights which has been treated accordingly.” And then it states that “This fact allows us to conclude that the interested parties consider that the information that MERCADONA provides them through the aforementioned channels gives strictly comply with the provisions of the regulations for the protection of data and that the purpose followed by MERCADONA for the purpose of the Project is proportionate and adequate.

On May 28, 2020, the AEPD published a press release entitled: “The AEPD analyzes in a report the use of facial recognition systems by part of the private security companies.

This communication has also been incorporated into this file through of the corresponding diligence.

THIRD: On May 5, 2021, the Director of the Spanish Agency of Data Protection agreed to initiate sanctioning procedure to the claimed, in accordance with the provisions of articles 63 and 64 of Law 39/2015, of 1

October, of the Common Administrative Procedure of the Administrations

(hereinafter, LPACAP), for the alleged violation of Article 5.1.c) of the

GDPR, Article 6 GDPR, Article 9 GDPR, Article 12 GDPR, Article

35 of the RGPD, Article 13 of the RGPD, Article 25 of the RGPD, typified in the

Article 83.5 of the RGPD, and the precautionary measure consisting of the suspension of

all processing of personal data relating to facial recognition in your

establishments.

FOURTH: Once the initiation agreement was notified, the respondent requested a copy of the

file and extension of the term to present arguments, which was granted

in the legally established terms. Subsequently, the defendant filed

in due time and written form of allegations in which it states, in summary, what

following regarding substantive aspects:

1.

RGPD) to ensure compliance with judicial decisions.

That its legitimacy resides in the public interest (art. 6.1.e) of the

two.

That the RGPD allows the use of biometric data whenever it is

adopt the appropriate security measures, focusing not so much on the

legitimation, which it takes for granted, but that what is important are the measures of

security. It adds that, with adequate security measures, the processing

can be carried out, even in the case of special categories of data

personal.

He alleges and affirms that the treatment now analyzed is the only measure

3.

capable of solving this problem and indicates that it is necessary, suitable, effective and proportional.

Four.

Alleges and affirms that the rights of other subjects that

enter the supermarket since there is no data processing because it is

produces in 0.3 seconds. Thus, it considers that only the data would be processed

identifiable biometric data of those sentenced by firm judicial resolution, being

impossible to identify those people who are not in the database

indubitable data.

The treatment now analyzed has been previously validated by various

5.

court rulings.

The AEPD has not carried out a detailed analysis of the system

6.

implanted, and has included innumerable references to “guides, articles and

guidelines” that are not binding. Consequently, there is a violation

to the principles of typicity and legality, violating the principle of interdiction of

the arbitrariness of public powers (art 9.3 of the C.E.).

7.

It has been duly, sufficiently and adequately informed of the implementation

in operation of the System and its implications, as well as the means to

exercise the rights recognized to those affected.

The implanted system now analyzed took into consideration from the

8.

design the potential impact on people's privacy.

Regarding non-substantive or formal aspects, carry out the following

allegations:

Ignorance of the two claims (Facua and Apedanica), which

A.

It is contrary to the usual practice of the AEPD.

The employer of a person does not constitute personal data, for

b.

what is not needed legal basis for its treatment.

The implemented system does not collect information additional to the condition of

c.

sentenced included in its database.

d

The proposal for a Regulation on artificial intelligence (COM (2021)

206. Annexes 1 to 9) published on 04/21/2021, considers that the system would be

possible and in accordance with the measures proposed in said proposal.

AND.

He alleges the inexistence of a subjective element of guilt.

MERCADONA's main activity is not linked to processing

F.

of data but to the management of a supermarket chain.

It alleges that both the AEPD and MERCADONA have been adopting the System and

g.

adjusting it to the requirements of the Agency.

Due to the foregoing, MERCADONA requests that the disciplinary file be archived.

FIFTH: There is no evidence in the claimed request for taking evidence, therefore previous investigation actions are taken as incorporated, as well as the documents provided by the claimed party and the inspection of this AEPD. Nor is there a contribution of the "expert opinion on facial recognition" announced in the Second Addendum to the pleadings brief.

PROVEN FACTS

FIRST: The processing of personal data implemented on the date 06/1/2020 and continued until 05/6/2021 by MERCADONA in forty establishments of the mercantile relative to facial recognition of those people who access its shopping centers, constitutes a treatment of special category data of those regulated in art. 9 of the RGPD and art 9 of the LOPDGDD.

SECOND: In the treatment of biometric personal data now analyzed (special category data) there is no accredited concurrence of the circumstances set forth in article 9.2 of the RGPD, so that according to the provisions in art. 9.1 of the RGPD the treatment is prohibited. It consists accredited the inadmissibility of applying the exceptions of art. 9.2.f), g) and h) of the RGPD to lifting of the general prohibition indicated in article 9.1 of said regulation.

THIRD: In addition, without prejudice to what is stated in the Facts proven First and Second, in the treatment of biometric personal data now analyzed (special category data) there is no legitimate basis as stated in art. 6

of the RGPD, nor legal regulations that allow it according to art. 8 of the

LOPDGDD.

FOURTH: In the treatment of biometric personal data now analyzed

(special category data), without prejudice to what is stated in the Facts proven

First and second, the information required in art. 13

In relation to the general obligation imposed by art. 12 of the RGPD and, in

especially, the provisions of 12.1 regarding "children". It is also not accredited

compliance with the requirements established in article 7 of the LOPDGDD

regarding minors.

FIFTH: In the treatment of biometric personal data now analyzed, without

Despite what is stated in the First and Second Proven Facts, there is no evidence

accredited compliance with the principle of minimization set forth in art.

5.1.c) since the recognition system implemented by MERCADONA

could treat in a highly plausible way data of diverse nature apart from

those strictly necessary, such as those indicated and qualified by category

special in the art. 9.1 of the RGPD and 9 of the LOPDGDD.

SIXTH: In the treatment of biometric personal data now analyzed, without

Despite what is stated in the First and Second Proven Facts, there is no evidence

accredited that from the design the safeguards have been established in order

to guarantee the freedoms and rights of all those affected, as stated in the

art. 25.1 of the GDPR.

SEVENTH: In the treatment of biometric personal data now analyzed,

without prejudice to what is stated in the First and Second Proven Facts,

The correct risk analysis and the mandatory evaluation of

impact, since it does not contemplate, neither in one nor in the other, all the subjects affected (FD V), as is the case of workers and minors.

EIGHTH: Being, therefore, a prohibited treatment, said prohibition

cannot be circumvented through the application of proactive security measures, since

that the prohibition of processing determines that they are irrelevant.

NINTH: In accordance with what is stated in the Facts proven First,

Second and Eighth, the precautionary measure imposed in the agreement of

beginning.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each

control authority, and according to the provisions of articles 47 and 48 of the

LOPDGDD, the Director of the Spanish Data Protection Agency is

competent to initiate and resolve this procedure.

II

In relation to the brief of allegations to the initial agreement presented by the

mercantile, it must mean, in summary, the following:

Regarding the allegations included in the FOURTH background of type

substantial and numbered from 1 to 8, it should be noted that all of them have already been

found distorted and motivated -through a detailed analysis

result of the exhaustive preliminary investigation carried out by this Agency-

its inadmissibility in the Grounds of Law (FD) of the agreement itself

Start of this sanctioning procedure and those indicated in this

Resolution Proposal. However, they are now answered succinctly, without

prejudice to expansion in subsequent Legal Grounds:

Responding to the allegations presented by MERCADONA, it means the

Next:

On the legitimacy: Mercadona does not allege in its allegations to the

□

this procedure no exception among those contemplated in art. 9.2

of the RGPD that legitimizes the treatment of the biometric data of the sentenced person; I know

limits itself to citing the legitimacy of the treatment under the pretext that "it is not injured in

at no time the data protection of the subjects”.

The foregoing confirms what is indicated in the Start-up Agreement: Mercadona does not hold

legitimacy to carry out the processing of personal data consisting of

facial recognition.

Likewise, through the allegations made by Mercadona, they corroborate

the initial evidence appreciated by this Agency, that is, that the company

was preconstituting the exception of art. 9.2 of the RGPD for the purposes of

be able to process the biometric data regulated in art. 9 of the GDPR. well once

obtained the judicial resolution that allows in a generic way the implantation of

the security measure, the supermarket chain interprets

unilaterally the scope of the judicial resolution and uses it for the purpose of justifying that holds legitimacy in the sense of art. 9.2.f) of the RGPD not only for the condemned, but also for the rest of the citizens affected by the system when they access supermarkets - which the company includes under the name of "unconvicted"-.

The initial agreement already stressed the lack of legitimacy to carry out carried out the treatment consisting of facial recognition: it was pointed out that where there is no concurrence of one of the exceptions indicated in the article 9.2 of the RGPD, there is no legitimacy to process biometric data of anyone, with independence of the causes of legality indicated in art. 6 of the RGPD, at all times than art. 9.1 prohibits it; although, we understood that there was legitimacy regarding of the processing of the biometric data of the convicted person because he had, in the course examined and raised by Mercadona, with the corresponding measure of security adopted in a judicial resolution. The AEPD respects the judicial resolutions, not being able to oppose what is consigned in them.

However, the extensive and unilateral interpretation of the terms exposed in the judicial resolution by Mercadona is contrary to the principles of necessity, proportionality and minimization indicated by the RGPD (arts. 5.1.c), 25, 35.7.a) and considering clauses 4, 156 and 170, by all).

At this time we have to bring up the Order of the Provincial Court of Barcelona of 02/115/2021, Appeal No. 840/2020, and Resolution No. 72/2021. The aforementioned Order examines the adoption of the security measure consisting of the facial recognition requested by Mercadona for the condemned. It concludes that the provisions of article 48 of the Criminal Code have to be complemented with the consent of the sentenced person so that such treatment of personal data of facial recognition can be carried out with sufficient legitimacy: "Although article 48 of the Criminal Code establishes "the deprivation of the right to reside in certain places or go to them prevents the sentenced to reside or go to the place where the crime was committed" and that "the judge or The court may agree that the control of these measures be carried out through those electronic means that allow it"; this would occur by ensuring the fundamental rights of the convicted person, that is, as long as he had given your consent. We must remember that the damned enjoy all the fundamental rights recognized in the Constitution, with the exception of the that are expressly limited by the content of the conviction, the sense of punishment and penitentiary law”.

In addition, the Order considers that the treatment is not protecting the public interest but rather, the private or particular interests of the trade.

Necessity of the measure: It also means that the company focuses on

the usefulness of the measure because it is effective, confusing “utility” with the objective "need" of the measure. The measure implemented may be effective, but in no way necessary.

From the foregoing, and from the following legal foundations, all the legal support used by MERCADONA to carry out the treatment of data that it intends, as it is prohibited as indicated in art. 9.1 of the GDPR, and There is no exception that lifts the ban.

As for the rest of the arguments presented by MERCADONA (outlined

from A to G), the following should be noted:

Regarding non-substantive or formal aspects, carry out the following

allegations:

<<Ignorance of the two claims (Facua and Apedanica), which

A)

which is contrary to the usual practice of the AEPD.>>

In this sense, to mean that the AEPD proceeded to initiate preliminary investigations

in order to verify the alleged violations of the RGPD as indicated in the

Title VIII of the LOPDGDD, arriving later a series of

claims motivated by general procedural aspects and not

singular claims of specific affected parties, the AEPD. It must be added that,

After the Home Agreement, the respondent has disposed of the entirety of the

documentation that works in the administrative file.

In response to the allegations of the company, remember that the transfer is a

Optional and non-mandatory procedure, derived from the presentation of a

claim. The transfer is a process outside the sanctioning procedure.

Furthermore, the respondent party does not specify in what way his rights are violated.

right of defence, which must be material and not formal.

<<The employer of a person does not constitute a personal data,

b)

therefore, no legal basis is needed for its treatment>>.

The genesis of the Biometric Pattern starts from the collection of physical characteristics

of the subject (the photograph, which by itself is personal data as it is

subsequently object of treatment and, consequently, identifiable) in a

such that it characterizes it unequivocally, so that, by the very definition of personal data, as it is identifiable, both the photograph and the Pattern

biometric constitute personal data and their treatment is subject to the RGPD.

That Mercadona treats the image of any person who enters its

establishments, captures it, obtains a pattern from it, compares it with that of the

sentenced person and delete it is a treatment of personal data

personal (facial recognition). The pattern thus obtained from the personal image

constitutes in itself, a personal data. There are not two patterns

the same (Doc 6 of the NRE brief: 026459/2020).

Furthermore, and in response to the allegations made by the

mercantile, we must remember that the image of a person is a datum of

personal nature and this is continually reiterated by the AEPD; the image of the face of

a person, from whom the biometric pattern is extracted, fully identifies

this without further action. Within the framework of consistent data processing

in facial recognition, that the company does not have the name of the people

whose biometric data they treat, as if they possess that of the convicted person, does not imply that

It is not about personal data. that do not have previously

stored the image of a person other than the condemned, to compare it

with a database through a pattern, it also does not mean that we do not

we are faced with a treatment of personal data.

<<The implanted system does not collect information additional to the condition

c)

of condemned included in its database.>>

In this regard, it should be noted that the information collected from the sentenced to

from the indubitable database that MERCADONA has and processes, it is

contrasted with additional information from third parties in order to "match"

biometric characteristics of both and, subsequently, based on algorithms

and in quality criteria, identity by pairing is allowed or else

inadmissible In both cases, additional information is always collected based on

characteristics and personal data that enriches the system and that lacks

legal basis for its treatment.

D)

<<The proposal for a Regulation on artificial intelligence (COM (2021)

206. Annexes 1 to 9) published on 04/21/2021, considers that the system would be

possible and in accordance with the measures proposed in said proposal>>.

In the Initiation Agreement, mention was already made of the aspects that are now alleged

regarding the aforementioned draft regulation on artificial intelligence. In this

In this sense, article 5 of the cited Regulation states:

“The following artificial intelligence practices are prohibited:

(…)

(a)

the use of "real-time" remote biometric identification systems in

publicly accessible spaces for law enforcement purposes, unless and to the extent

insofar as such use is strictly necessary for one of the purposes

following:

the specific search for possible victims of crimes, including

(Yo)

missing children;

the prevention of a specific, substantial and imminent threat to life or

(iii)

the physical safety of individuals or from a terrorist attack;

(iii)

The detection, location, identification or prosecution of a perpetrator or

suspected of a criminal offense referred to in Article 2(2) of the

Framework Decision 2002/584/JHA of the Council and sanctioned in the Member State of which

is treated with a custodial sentence or a detention order for a period

maximum of three years, as determined by the legislation of that Member State."

In the present case, there is no evidence that exceptions (i) to (iii) are met.

Furthermore, in addition to the fact that the aforementioned regulation is in

processing, data protection regulations always require an analysis

detailed information on the specific case in question for the purpose of verifying whether

holds legitimacy for a specific processing of personal data, away

always such an analysis of automatism.

AND)

<<Alleges the non-existence of a subjective element of guilt.>>

Although it is not possible to impute an infringement in the absence of the volitional element of

liability (strict liability), in the present case the commercial

responsible was aware of the activity that was going to start hiring

specialized entities for its implementation. The fact of having proceeded to perform a poor risk analysis by omitting not only all the

affected subjects but not to evaluate as a risk the prohibition of the treatment that

contemplated in article 9.1 of the RGPD, already configures the volitional element of

culpability. Having assessed the risk of the planned treatment, the result

would have been that we are faced with a prohibited treatment and, in

consequence, unacceptable, which in his case would have led to the application of the

provided in article 36 of the RGPD (prior consultation), which at no time

has been taken into account and would have given rise to the pronouncement of this AEPD

on the processing of personal data now analyzed.

Furthermore, to the unacceptable deficiency committed in the elaboration

the risk analysis prior to treatment must be added the also deficient

subsequent impact assessment, by not involving all the subjects affected,

which also constitutes a serious deficiency by not determining the serious

consequences for the rights and freedoms of the data subjects. All the

citizens who access a Mercadona shopping center with a

implanted facial recognition are treated as doomed.

The foregoing configures the presence of the volitional element of guilt required

by art. 28 of Law 40/2015, of 1/10, of RJSP.

<<The main activity of MERCADONA is not linked to the

F)

data processing but to the management of a supermarket chain>>.

Although MERCADONA's main activity is the management of supermarkets,

It is also true that said management implies, as a daily parallel activity and

continues the processing of personal data of both its online customers and

face-to-face and their workers, the latter amounting to more than one hundred thousand.

<<It alleges that both the AEPD and MERCADONA have been adopting the

g.

System and adjusting it to the requirements of the Agency>>.

This allegation must be rejected since at no time is this AEPD

has taken any position with the establishment of the treatment now

analyzed and, as already mentioned, Mercadona has not used the

regulatory mechanism established for this purpose in the RGPD (art. 36 RGPD).

h.

<<Alleges disproportionality in the amount of the sanction>>.

In this sense, the amount of the penalty is stated in the initial agreement.

In this regard, note that the GDPR itself, art 83.1, states that: “1. Each

control authority will guarantee that the imposition of administrative fines

under this Article for infringements of this Regulation

indicated in sections 4, 5 and 6 are in each individual case effective,

proportionate and dissuasive”.

In the present case, the effectiveness, proportionality and dissuasive nature

is guaranteed. The amount of the administrative fine is adjusted to levels

much lower than the maximum allowed (for each one, 10 or 20 million

euros, or 2% or 4% of the total annual global turnover of the financial year

previous financial, opting for the highest amount.

Consequently, the claims must be dismissed in their entirety.

III

In order to systematize the reading and comprehension from the beginning of the

this Motion for a Resolution, the doctrine of this Resolution is set out below.

AEPD regarding the treatment now under analysis, which will be

reference, among others, throughout the Motion for a Resolution.

Regulation (EU) 2016/679, of the European Parliament and of the Council of 27

April 2016 on the protection of natural persons with regard to the

treatment of personal data and the free circulation of these data and by the

repealing Directive 95/46/EC (General Regulation for the protection of

data, RGPD) defines in its article 4.14 biometric data as "data

obtained from a specific technical treatment, related to the

physical, physiological or behavioral characteristics of a natural person who

allow or confirm the unique identification of that person, such as images

facial or fingerprint data.

Article 9 of said rule regulates the treatment of special categories of

data, including biometric data, establishing a

general prohibition of its treatment in the following terms:

“The processing of personal data that reveals the origin

racial or ethnic background, political opinions, religious or philosophical convictions, or

union affiliation, and the processing of genetic data, biometric data

aimed at uniquely identifying a natural person, data relating to

the health or data relating to the sexual life or sexual orientation of a person physical."

In relation to the processing of facial recognition data, in our Report 36/2020, analyzing article 9.1 in relation to Recital 51 of the RGPD, as well as the Protocol of amendment to the Convention for the Protection of Individuals with respect to the processing of personal data, approved by the Committee of Ministers at its 128th session in Elsinore on May 18 of 2018 (Convention 108+) we pointed out that:

"In order to clarify the interpretative doubts that arise regarding the consideration of biometric data as special categories of data

A distinction can be made between biometric identification and biometric verification/authentication established by the Article 29 Group in its Opinion 3/2012 on the evolution of biometric technologies:

Biometric identification: the identification of an individual by a system biometrics is normally the process of comparing your biometrics (acquired at the time of identification) with a series of templates biometrics stored in a database (i.e., a process of one-to-many correspondence search).

Biometric verification/authentication: the verification of an individual by a biometric system is normally the process of comparing your data biometrics (acquired at the time of verification) with a single template biometrics stored on a device (i.e., a search process for one-to-one correspondence).

This same differentiation is reflected in the White Paper on intelligence artificial from the European Commission:

"As far as facial recognition is concerned, 'identification' means that one person's facial image template is compared to many others templates stored in a database to find out if your image is stored in it. "Authentication" (or "verification"), on the other hand, is usually refers to the search for correspondence between two templates concrete. It allows the comparison of two biometric templates that, in principle, they are supposed to belong to the same person; So, the two templates

are compared to determine if the person in the two images is the same. This procedure is used, for example, in control gates automated border controls used in border controls of the airports".

Taking into account the aforementioned distinction, it can be interpreted that, according to the article 4 of the RGPD, the concept of biometric data would include both assumptions, both identification and verification/authentication. However, and with In general, biometric data will only be considered as special category of data in the cases in which they are submitted to treatment technician aimed at biometric identification (one-to-many) and not in the case of biometric verification/authentication (one-to-one)."

In the present case, biometric data is processed for the purposes of identification, that is, to isolate one individual among several, making it a treatment of special categories of data subject to the general rule of prohibition of the same (art. 9.1. RGPD).

However, article 9.2 of the RGPD regulates exceptions to said prohibition.

general by stating that:

“Section 1 shall not apply when one of the circumstances

following:

a)

the interested party gave his explicit consent for the treatment of

such personal data for one or more of the specified purposes, except

when the Law of the Union or of the Member States establishes that the

prohibition mentioned in paragraph 1 cannot be lifted by the

interested.

(…)

F)

the treatment is necessary for the formulation, exercise or defense

of claims or when the courts act in the exercise of their function

judicial;

g)

the processing is necessary for reasons of an essential public interest,

on the basis of the law of the Union or of the Member States, which must be

proportional to the objective pursued, respect essentially the right to

data protection and establish adequate and specific measures to protect

the interests and fundamental rights of the interested party;

(…)

In relation to section g), it highlights that when the treatment is necessary

for reasons of public interest, which must be essential on the basis of law

of the Member States, proportional to the objective pursued, to respect as far as

The right to data protection is essential and establish adequate measures and specific to protect the interests and fundamental rights of the interested party.

Therefore, it will proceed to analyze whether, in the present case, the presuppositions established in article 9.2. to lift the ban on treatment of biometric data.

This Agency has had occasion to pronounce itself, on various occasions, on the necessary requirements to lift the prohibition established in art. 9.1 of the RGPD, especially regarding the requirements established by article 9.2.g) of the RGPD, in order to protect the processing of personal data based on facial recognition, given the proliferation of proposals received in relation with them from different areas, which shows the interest increasing use of these systems and the constant concern of this control authority, as they are very intrusive identification systems for fundamental rights and freedoms of natural persons. Concern which has been shared by the rest of the control authorities for years, such as reveal the Working Document on Biometrics, adopted on 1 August 2003 by the Group of 29, or the subsequent Opinion 3/2012 on the evolution of biometric technologies, adopted on April 27, 2012, and that has led the community legislator to include this data among the special categories of data in the RGPD. In this way, being prohibited treatment in general, any exception to said prohibition will be to be subject to restrictive interpretation.

In this regard, it is worth noting, in addition to the aforementioned report 36/2020, referring to the use of facial recognition techniques in conducting tests of

online evaluation that is commented on later, report 31/2019 on the

Incorporation of facial recognition systems in the services of

video surveillance under article 42 of the Private Security Law or the

Report 97/2020 regarding the Draft Order of the Minister of Foreign Affairs

Economics and Digital Transformation on identification methods not

face-to-face for the issuance of qualified electronic certificates. In all

In these cases, it was concluded that there was no legal norm in the legal system

Spanish that meets the requirements of article 9.2.g) of the RGPD, so the

Treatment could only be based on the consent of those affected

provided that it is guaranteed that it is free.

Analyzing and developing the requirements of article 9.2.g) in our Report

36/2020 we pointed out -FD V-, the following:

<< The next question that arises in the consultation is whether the treatment of

biometric data by facial recognition systems in the processes of

online assessment could rely on the existence of a public interest

essential according to article 9.2.g) of the RGPD:

g) the treatment is necessary for reasons of an essential public interest, especially

the basis of the law of the Union or of the Member States, which must be

proportional to the objective pursued, respect essentially the right to

data protection and establish adequate and specific measures to protect the interests and fundamental rights of the interested party.

As mentioned above, the processing of personal data necessary for the provision of the public service of higher education legitimate, in general, in the existence of a public interest under the of the provisions of article 6.1.e) of the RGPD. However, when it comes to special categories of data, the assumption referred to in letter g) of the article 9.2. does not refer only to the existence of a public interest, as does the RGPD in many other of its precepts, but it is the only precept of the RGPD that requires that it be "essential", an adjective that comes to qualify said public interest, taking into account the importance and necessity of greater protection of the processed data.

Said precept finds its precedent in article 8.4 of the Directive 95/46/CE of the European Parliament and of the Council, of October 24, 1995, on the protection of natural persons with regard to the treatment of personal data and the free circulation of these data: “4. As long as provide adequate safeguards, Member States may, for reasons of important public interest, establish other exceptions, in addition to those provided for in paragraph 2, either through its national legislation, or by decision of the supervisory authority. However, its reading results in a greater rigor in the new regulation by the RGPD, since the adjective “important” for “essential” and the exception is not allowed to be be established by the supervisory authorities.

In relation to what must be understood as essential public interest, it must also take into account the jurisprudence of the European Court of Human Rights, which under article 8 of the European Convention on Human Rights, has been considering that the processing of personal data constitutes a lawful interference in the right to respect for private life and only can be carried out if it is carried out in accordance with the law, serves a purpose legitimate, respects the essence of fundamental rights and freedoms and is necessary and proportionate in a democratic society to achieve an end legitimate (D.L. v. Bulgaria, no. 7472/14, May 19, 2016, Dragojević v. Croatia, no. 68955/11, 15 January 2015, Peck v. United Kingdom, no. 44647/98, 28 January 2003, Leander v. Sweden, No. 9248/81, 26 January March 1987, among others). As stated in the last sentence cited, "the The concept of necessity implies that the interference responds to a need pressing social and, in particular, that is proportionate to the legitimate purpose that pursue."

Likewise, the doctrine of the Constitutional Court must be taken into account regarding restrictions on the fundamental right to data protection, which synthesized in its sentence 292/2000, of November 30, in which after configure the fundamental right to the protection of personal data as a autonomous and independent right that consists of a power of disposition and of control over personal data that empowers the person to decide which of these data to provide to a third party, be it the State or an individual, or which this third party can collect, and that also allows the individual to know who owns that personal data and for what, being able to oppose that possession or use, analyzes its limits, pointing out the following:

More specifically, in the aforementioned Judgments relating to the protection of data, this Court has declared that the right to data protection is not unlimited, and although the Constitution does not expressly impose limits specific, nor refer to the Public Powers for their determination as it has done with other fundamental rights, there is no doubt that they must find them in the remaining fundamental rights and legal goods constitutionally protected, as required by the principle of unity of the Constitution (SSTC 11/1981, of April 8, F. 7; 196/1987, of December 11 [RTC 1987, 196], F. 6; and regarding art. 18, the STC 110/1984, F. 5). Those limits or they can be direct restrictions of the fundamental right itself, which have been alluded to before, or they may be restrictions on the manner, time or place of exercise of the fundamental right. In the first case, regulate those limits is a form of development of the fundamental right. In the second, the limits that are set are to the concrete way in which the beam of light can be exercised. powers that make up the content of the fundamental right in question, constituting a way to regulate their exercise, which can do the ordinary legislator pursuant to the provisions of art. 53.1 CE. The first observation that must be made, which is no less important because it is obvious, is that the Constitution has wanted the Law, and only the Law, to be able to set the limits to a fundamental right. Fundamental rights can give way, of course, before assets, and even constitutionally relevant interests, provided that the cut that they undergo is necessary to achieve the legitimate intended purpose, provided to achieve it and, in any case, be respectful of the content essential of the restricted fundamental right (SSTC 57/1994, of February 28 [RTC 1994, 57], F. 6; 18/1999, of February 22 [RTC 1999, 18], F. 2).

Precisely, if the Law is the only one empowered by the Constitution to set the limits to fundamental rights and, in the present case, to the right fundamental to data protection, and these limits cannot be different from those constitutionally provided for, which in this case are none other than those arising from the coexistence of this fundamental right with other rights and legal goods of constitutional rank, the legal empowerment that allows a Public Power collect, store, treat, use and, where appropriate, transfer data personal, it is only justified if it responds to the protection of other rights fundamental or constitutionally protected assets. Therefore, if those Operations with a person's personal data are not carried out with strict observance of the rules that regulate it, the right to protection is violated of data, since constitutionally illegitimate limits are imposed on it, either to its content or the exercise of the bundle of faculties that compose it. as it will also violate that limiting Law if it regulates the limits in such a way that they make impracticable the fundamental right affected or ineffective the guarantee that the Constitution gives you. And so it will be when the Law, which must regulate the limits to fundamental rights with scrupulous respect for their essential content, is limited to empowering another Public Power to set in each case the restrictions that can be imposed on fundamental rights, whose unique determination and application will be at the mercy of the decisions adopted by that Public Power, who will be able to decide, in what interests us now, on the collection, storage, treatment, use and transfer of personal data in the cases it deems appropriate and wielding, even, interests or assets that are not protected with constitutional rank […]”. (Legal Basis 11)

“On the one hand, because although this Court has declared that the Constitution does not prevents the State from protecting legal rights or assets at the cost of sacrificing others equally recognized and, therefore, that the legislator can impose limitations to the content of fundamental rights or their exercise,

We have also specified that, in such cases, these limitations must be be justified in the protection of other constitutional rights or goods (SSTC 104/2000, of April 13 [RTC 2000, 104], F. 8 and those cited there) and,

In addition, they must be proportionate to the purpose pursued with them (SSTC 11/1981, F. 5, and 196/1987, F. 6). For otherwise they would incur in the arbitrariness proscribed by art. 9.3 EC.

On the other hand, even having a constitutional basis and resulting provided the limitations of the fundamental right established by a Law (STC 178/1985 [RTC 1985, 178]), they can violate the Constitution if suffer from a lack of certainty and predictability in the very limits they impose and its mode of application. Conclusion that is corroborated in the jurisprudence of the European Court of Human Rights that has been cited in F. 8 and that here must be considered reproduced. And it should also be noted that not only would violate the principle of legal certainty (art. 9.3 CE), conceived as certainty about the applicable legal system and reasonably founded expectation of the person on what should be the action of the power applying the Law (STC 104/2000, F. 7, for all), but at the same time said Law would be damaging the essential content of the fundamental right thus restricted, given that the way its boundaries have been set make it unrecognizable and make it impossible, in practice, to exercise it (SSTC 11/1981, F. 15; 142/1993, of 22 of April [RTC 1993, 142] , F. 4, and 341/1993, of November 18 [RTC 1993, 341], F. 7). Luckily, the lack of precision of the Law in the budgets materials of the limitation of a fundamental right is likely to generate

an indeterminacy about the cases to which such a restriction applies. and to produce this result, beyond any reasonable interpretation, the Law already does not fulfill its function of guaranteeing the very fundamental right that it restricts, for he allows instead simply the will of the one who has to operate. enforce it, thus undermining both the effectiveness of the fundamental right and the legal security […]". (FJ15).

“More specifically, in relation to the fundamental right to privacy we have highlighted not only the need for its possible limitations are based on a legal provision that has constitutional justification and that they are proportionate (SSTC 110/1984, F. 3, and 254/1993, F. 7) but that the Law that restricts this right must express precisely each and every one of the material budgets of the limiting measure. If not, it's bad understand that the judicial resolution or the administrative act that applies it is founded on the Law, since what the Law has done, abandoning its functions, is to empower other Public Powers so that they are the ones set the limits to the fundamental right (SSTC 37/1989, of February 15 [RTC 1989, 37], and 49/1999, of April 5 [RTC 1999, 49]).

Similarly, regarding the right to personal data protection, it is consider that the constitutional legitimacy of the restriction of this right does not

it can be based, by itself, on the activity of the Public Administration. Neither

it is enough that the Law empowers it to specify in each case its

limits, limiting itself to indicating that it must make such precision when it concurs

some constitutionally protected right or asset. It is the legislator who must

determine when that good or right concurs that justifies the restriction of the

right to personal data protection and under what circumstances you can

limit himself and, moreover, it is he who must do so by means of precise rules that

make the imposition of such limitation and its consequences foreseeable for the interested party.

impact. For otherwise the legislator would have transferred to the

Administration the performance of a function that only he/she is responsible for in terms of

of fundamental rights by virtue of the reservation of Law of art. 53.1 CE, this

is, to clearly establish the limit and its regulation. […] (FJ 16)”.

Likewise, our Constitutional Court has already had the opportunity to

pronounce specifically on article 9.2.g) of the RGPD, as

consequence of the challenge of article 58 bis of the Organic Law 5/1985,

of June 19, of the General Electoral Regime, introduced by the provision

final third of Organic Law 3/2018, of December 5, on the Protection of

Personal data and guarantee of digital rights, regarding the legitimacy

of the collection of personal data related to the political opinions of the

persons carried out by political parties in the framework of their activities

elections, a precept that was declared unconstitutional by Judgment no.

76/2019 of May 22.

Said sentence analyzes, in the first place, the legal regime to which

is subject to the treatment of special categories of data in the

GDPR:

In accordance with section 1 of art. 9 RGPD, the treatment of

personal data that reveal political opinions, in the same way as

is the processing of personal data that reveals ethnic or racial origin,

religious or philosophical convictions or trade union membership and the treatment of

genetic data, biometric data aimed at uniquely identifying

a natural person, data relating to health or data relating to sexual life or

the sexual orientation of a natural person. However, section 2 of

The same precept authorizes the processing of all such data when it concurs

any of the ten circumstances provided therein [letters a) to j)]. some of those

circumstances have a limited scope of application (labour, social, associative,

health, judicial, etc.) or respond to a specific purpose, so, in

themselves, define the specific treatments that they authorize as an exception

to the general rule. Furthermore, the enabling efficacy of several of the assumptions there

foreseen is conditioned to the fact that the Law of the Union or that of the States

members the circumstances set out in letters a), b), g), h), i) and j).

The processing of special categories of personal data is one of the

areas in which expressly the General Regulation of Protection of

Data has given the Member States "room for manoeuvre" when it comes to

"specify its standards", as recital 10 qualifies it. This margin

of legislative configuration extends both to the determination of the causes

Enabling for the processing of specially protected personal data

-that is, to the identification of the purposes of essential public interest and the appreciation of the proportionality of the treatment to the end pursued, respecting essentially the right to data protection - such as the establishment of "appropriate and specific measures to protect the interests and rights of the interested party" [art. 9.2 g) RGPD]. The Regulation contains, by Therefore, a specific obligation of the Member States to establish such guarantees, in the event that they enable the processing of personal data specially protected.

In relation to the first of the requirements demanded by article 9.2.g), the invocation of an essential public interest and the necessary specification of the Likewise, the High Court recalls what was stated in its judgment 292/2000 in which it was rejected that the identification of the legitimate purposes of the restriction could be carried out through generic concepts or vague formulas, considering that the restriction of the fundamental right to the protection of personal data can be based, by itself, on the generic invocation of an indeterminate "public interest" :

In the aforementioned STC 292/2000 (RTC 2000, 292), in which it was also prosecuted a legislative interference in the right to the protection of personal data, We reject that the identification of the legitimate purposes of the restriction could done through generic concepts or vague formulas:

"16. [...] Similarly, regarding the right to protection of personal data

It can be estimated that the constitutional legitimacy of the restriction of this right

it cannot be based, by itself, on the activity of the Public Administration.

Nor is it enough that the Law empowers it to specify in each case its

limits, limiting itself to indicating that it must make such precision when it concurs

some constitutionally protected right or asset. It is the legislator who must

determine when that good or right concurs that justifies the restriction of the

right to personal data protection and under what circumstances you can

limit himself and, moreover, it is he who must do so by means of precise rules that

make the imposition of such limitation and its consequences foreseeable for the interested party.

impact. For otherwise the legislator would have transferred to the

Administration the performance of a function that only he/she is responsible for in terms of

of fundamental rights by virtue of the reservation of Law of art. 53.1 CE, this

is, to clearly establish the limit and its regulation.

17. In the present case, the use by the LOPD (RCL 2018, 1629) in its art.

24.1 of the expression "control and verification functions", opens a space of

uncertainty so wide that it provokes a double and perverse consequence. Of a

hand, by enabling the LOPD to the Administration to restrict rights

fundamental principles by invoking such an expression is renouncing fixing it

limits itself, empowering the Administration to do so. and in a way

such that, as the Ombudsman points out, it allows the same

practically all administrative activity, since all administrative activity

that implies establishing a legal relationship with a company, which will be

practically in all cases in which the Administration needs data

personal property of someone, will ordinarily entail the power of the Administration

to verify and control that the administrator has acted in accordance with the regime

administrative law of the legal relationship established with the Administration. It that, in view of the reason for restriction of the right to be informed of art. 5

LOPD, leaves the citizen in the most absolute uncertainty about in which cases

that circumstance will concur (if not in all) and add to the inefficiency any

jurisdictional protection mechanism that should prosecute such a case of

restriction of fundamental rights without any other complementary criterion

come to the aid of your control of administrative action in this matter.

The same reproaches also deserve the use in art. 24.2 LOPD of the

expression "public interest" as a basis for the imposition of limits on

fundamental rights of art. 18.1 and 4 CE, since it contains a degree of

even greater uncertainty. It is enough to note that all administrative activity, in

Ultimately, it pursues the safeguarding of general interests, whose

attainment constitutes the purpose that must be objectively served by the

Administration pursuant to art. 103.1 CE."

This argument is fully transferable to the present trial. Of

Likewise, therefore, we must conclude that the constitutional legitimacy of the

restriction of the fundamental right to the protection of personal data

can be based, by itself, on the generic invocation of an indeterminate

"public interest". Well, in another case, the legislator would have transferred the political parties

politicians - whom the challenged provision empowers to collect data

relating to the political opinions of people within the framework of their

electoral activities - the performance of a function that only falls to him in matter of fundamental rights by virtue of the reservation of Law of art. 53.1 CE, that is, clearly establish its limits and regulation.

Neither can the purpose adduced by the State attorney, which refers to the functioning of the democratic system, because it also entails a high degree of uncertainty and can suppose a circular reasoning. On the one hand, political parties are in themselves "channels necessary for the functioning of the democratic system" (by all, STC 48/2003, of March 12 (RTC 2003, 48), FJ 5); and, on the other hand, all functioning of the democratic system ultimately pursues the safeguarding of constitutional purposes, values and goods, but this is not enough to identify the reason why the fundamental right should be restricted affected.

Finally, it should be specified that it is not necessary to suspect, with greater or lesser foundation, that the restriction pursues a purpose unconstitutional, or that the data collected and processed will be harmful for the private sphere and the exercise of the rights of individuals. It is It is enough to note that, since it is not possible to identify with sufficient precision the purpose of data processing, nor can the character constitutionally legitimate of that purpose, nor, where appropriate, the proportionality of the planned measure in accordance with the principles of suitability, necessity and proportionality in the strict sense.

On the other hand, regarding the guarantees that the legislator must adopt, the aforementioned ruling no. 76/2019 of May 22, after recalling that “In view of the potential intrusive effects on the affected fundamental right that result of the processing of personal data, the jurisprudence of this Court requires the legislator who, in addition to meeting the aforementioned requirements, also establish adequate guarantees of a technical, organizational and

procedural, that prevent risks of different probability and severity and

mitigate their effects, because only in this way can we ensure respect for the content

essence of the fundamental right itself", analyzes what is the norm that must

contain the aforementioned guarantees:

"Therefore, the resolution of this challenge requires that we clarify a

doubt raised with respect to the scope of our doctrine on the guarantees

adequate, which consists in determining if the adequate guarantees against the use

information technology must be contained in the law itself that authorizes and regulates that

use or can also be found in other normative sources.

The question can only have a constitutional answer. The forecast of

adequate guarantees cannot be deferred to a time subsequent to the regulation

law of the processing of personal data in question. guarantees

adequate must be incorporated into the legal regulation of the treatment,

either directly or by express and perfectly delimited reference to

external sources that have the appropriate regulatory status. Only that

understanding is compatible with the double requirement arising from art. 53.1 EC

(RCL 1978, 2836) for the legislator of fundamental rights: the reservation

of law for the regulation of the exercise of fundamental rights

recognized in the second chapter of the first title of the Constitution and the

respect for the essential content of these fundamental rights.

According to reiterated constitutional doctrine, the reservation of law is not limited to requiring that a law enables the restrictive measure of fundamental rights, but rather It is also necessary, according to both requirements called -sometimes- of normative predetermination and -others- of quality of the law as well as respect for essential content of the right, that in that regulation the legislator, who comes primarily obliged to weigh the conflicting rights or interests, predetermine the assumptions, the conditions and the guarantees in which the adoption of restrictive measures of fundamental rights. That mandate of predetermination with respect to essential elements, also linked in last term to the judgment of proportionality of the limitation of the right fundamental, cannot be deferred to a later legal development or regulation, nor can it be left in the hands of the individuals themselves" (FJ 8).

Consequently, the processing of biometric data under article 9.2.g) requires that it be provided for in a regulation of European or national law, In the latter case, it must have said rule, according to the constitutional doctrine cited and the provisions of article 9.2 of the LOPDGDD, range of law. said law must also specify the essential public interest that justifies the restriction of the right to the protection of personal data and in what circumstances can be limited, establishing the precise rules that make the interested party foreseeable the imposition of such limitation and its consequences, without it being sufficient, to these effects, the generic invocation of a public interest. And this law must establish, in addition, the adequate guarantees of a technical, organizational and procedural, that prevent risks of different probability and severity and mitigate their effects.

In addition, said law must respect in all cases the principle of proportionality, as recalled by the Constitutional Court Judgment 14/2003, of 28 January:

“In other words, in accordance with a settled doctrine of this Court, the constitutionality of any restrictive measure of fundamental rights is determined by strict observance of the principle of proportionality. For the purposes that matter here, it suffices to remember that, to check whether a restrictive measure of a fundamental right exceeds the judgment of proportionality, it is necessary to verify whether it meets the three requirements or following conditions: if the measure is likely to achieve the objective proposed (judgment of suitability); if, in addition, it is necessary, in the sense that There is no other more moderate measure to achieve this purpose with equal efficacy (judgment of necessity); and, finally, if it is weighted or balanced, because it derives more benefits or advantages for the interest general than damages on other goods or values in conflict (judgment of proportionality in the strict sense; SSTC 66/1995, of May 8 [RTC 1995, 66], F. 5; 55/1996, of March 28 [RTC 1996, 55], FF. 7, 8 and 9; 270/1996, of December 16 [RTC 1996, 270], F. 4.e; 37/1998, of February 17 [RTC 1998, 37], F. 8; 186/2000, of July 10 [RTC 2000, 186], F. 6).”

Of the transcribed regulation, which is a transposition of community regulations, it can easily be inferred that it does not meet the requirements established in article 9.2.g), since the legislator has not foreseen the use of biometric data as a proportional measure for the identification of

natural persons, establishing the specific and adequate guarantees that are

derive from the greater risks involved in the processing of said data.

Therefore, intending in the project the processing of data

personal information included in the special categories of data referred to in the

article 9.1. of the RGPD, since it is biometric data aimed at the

identification of natural persons, it is a prerequisite that one of the

the circumstances contemplated in its section 2 that lifts the prohibition of

treatment of said data, established in general in section 1,

requiring article 9.2. of the LOPDGDD that "Data processing

referred to in letters g), h) and i) of article 9.2 of the Regulation (EU)

2016/679 founded on Spanish law must be covered by a

norm with the force of law, which may establish additional requirements related to

its security and confidentiality. not existing, as has been indicated, norm

legal that enables said treatment under article 9.2.g) of the RGPD.

Therefore, said prohibition may only be lifted in those cases in which

that the affected party gives his express consent, under letter a) of the

article 9.2. of the RGPD, and all other requirements must be met to

grant a valid consent that is included in the definition of article 4.11

of the RGPD: "any manifestation of free will, specific, informed and

unequivocal by which the interested party accepts, either by means of a declaration or a clear affirmative action, the treatment of personal data that concern”.

Although the absence of cause that lifts the prohibition of the treatment of special categories of data determines, by itself, the prohibition of the treatment carried out by Mercadona, and it should be noted that neither does it concur a legal basis that would legitimize, where appropriate, the same under article 6.1. of the GDPR on the basis of public interest.

The concept of public interest, or the general interest, which is more frequently used by our constitutional text, is a legal concept indeterminate with a double function: to give legitimizing coverage to the action of the Administration and, on the other hand, constitutes one of the ways of limiting the administrative powers. In this way, the public interest which, as pointed out by Parejo Alfonso, has a clear directive function of the normative development (parliamentary or not) of the constitutional order, acts as a delimiting criterion of the action of the public authorities, so it must, first of all, be identified by the legislator, in order to identify the area in which the develop the performance of the Administration, subject to the principle of legality and to which it corresponds to objectively serve the general interests (article 103.CE) and, in any case, under the control of the courts, since as you remember the Judgment of the Constitutional Court of June 11, 1984, "There is no unaware that the power attributed by the Constitution to the State to define the general interest, an open and indeterminate concept called to be applied to respective matters, can be controlled, against possible abuses and posteriori, by this Court…”.

In the first place, it must be assumed that the existence of a public interest does not legitimizes any type of processing of personal data, but must be, in the first place, to the conditions that may have been established by the legislator, as provided for in article 6 of the RGPD, in its sections 2 and 3, and article 8 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (LOPDGDD) that regulates the data processing based on a legal obligation and on a mission carried out in the public interest or exercises of public interests in its article 8, in the following terms:

"1. The processing of personal data can only be considered based on the compliance with a legal obligation required of the person in charge, in the terms provided for in article 6.1.c) of Regulation (EU) 2016/679, when so foresees a rule of European Union Law or a rule with the rank of law, which may determine the general conditions of the treatment and the types of data object of the same as well as the transfers that proceed as consequence of the fulfillment of the legal obligation. This rule may also impose special conditions to the treatment, such as the

adoption of additional security measures or others established in the Chapter IV of Regulation (EU) 2016/679.

2. The processing of personal data can only be considered based on the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the controller, under the terms provided in the Article 6.1 e) of Regulation (EU) 2016/679, when derived from a

competence attributed by a norm with the force of law.”

Therefore, the public interest requires, in the first place, its realization by part of the legislator, taking into account all the interests affected, purpose of determining the restrictions that private interests may suffer as a consequence of the presence of said general interests, which must be done through a standard with the force of law.

On the other hand, the other principles of article 5 of the RGPD should be respected, especially those of purpose limitation and data minimization.

Especially, in relation to the principle of data minimization, which requires that they be “adequate, relevant and limited to what is necessary in relation to for the purposes for which they are processed” (article 5.1.c) of the RGPD) it is necessary to point out that the processing of facial recognition data will involve the large-scale processing of special categories of data subject to a reinforced guarantee regime. This is so due to the high volume of affected and clients of the company, as well as because such treatment could be generalized to all merchants in the same or another commercial sector.

Finally, apart from the ostensible lack of legitimacy for the treatment of personal data consisting of facial recognition, the system implanted by the company would not meet the proportionality requirements required by the Constitutional Court, since within the triple trial of proportionality, if may well be considered suitable for the proposed purpose, it is not necessary, since there are less intrusive alternative measures, nor is it strictly proportional, to the extent that more benefits are derived for the interest public than damages on other assets or values in conflict, taking into account account that its massive and indiscriminate application is intended for all customers and other affected parties, and that if it were to become widespread it would imply a mass treatment of special categories of data that would reach the almost the entire population, regardless of the level of risk represent becoming the exception of the possibility of data processing biometrics in the general rule, contrary to what is intended by the RGPD.

Precisely, the inadmissibility of using these techniques with a generalized, as well as the absence of connection between the security measure with the public interest, persecuting, on the contrary, private interests or

of the mercantile, is collected in the Order of the Provincial Court of Barcelona, dated 02/15/2021:

Having stated what precedes in the preceding paragraphs, this Chamber considers that the measure requested by the commercial entity, MERCADONA S.A, in In no way is it proportional, necessary or even suitable. the convicts in this execution, Messrs. A.A.A. and B.B.B. a ban was imposed of access to a specific supermarket of the Mercadona entity, specifically located on Frederic Mompou s/n street in the town of San Boi de Llobregat; there has been no record, or at least of the testimony of individuals referred to this section, there is no evidence that they violated the corresponding prohibition of access to the shopping center nor that they are repeat offenders of such conduct. But what is more, this Chamber cannot share that the interested measure is protecting the public interest, but rather, the private or particular interests of the company in question, because as has already been explained in the previous paragraphs, they would be violating the adequate guarantees in order to protect the rights and freedoms of the interested parties, not only of those who have been sentenced and whose prohibition of access is incumbent on them, but on the rest of the people who access the aforementioned supermarket.

In the allegations made to the initial agreement, Mercadona alleges an interest underlying public in the judicial resolutions in which the decisions are adopted. security measures consisting of facial recognition of the sentenced person.

The respondent affirms that “Consequently, in view of the fixation as security measure in criminal sentences of recognition methods face by judges and courts, the public interest put forward and accepted as a legal basis for the convicted, and courts, the public interest put forward and accepted as a legal basis for the convicted, would logically extend to these effects to unconvicted persons”.

Well, it is one thing that the adoption of a security measure can have beneficial effects on society and that a judge or criminal court values proportionally what the adoption of the security measure entails (between the restriction of the rights of the condemned and the public interest, that benefit social, which is obtained from the imposition of the security measure). And another thing is that the preponderance of the public interest (which is why the security measure) legitimizes the processing of personal data of the rest of the citizens, in such a way that all citizens are treated as sentenced, being subjected to the same treatment as the subject to whom has imposed the security measure.

In any case, the existence of that public interest is not a peaceful matter. The aforementioned Order of the Provincial Court of Barcelona, examining specifically the security measure consisting of facial recognition,

considers that there is no public interest, but that, as we have already pointed out, they strictly pursue particular and private interests of the company.

Consequently, and in response to the allegations made at this time procedure by Mercadona, we must definitively conclude that the processing of data based on facial recognition for the purposes of identification is not authorized in accordance with article 9.2.g) of the RGPD and, furthermore, it lacks a legal basis under article 6.1 of the itself and is contrary to the principles of necessity, proportionality and minimization.

IV

On the other hand, and as has already been pointed out, it is appropriate to bring up a summary of the content of the recent Order of the Provincial Court of Barcelona dated 02/15/2021, Appeal No. 840/2020, and Resolution No. 72/2021, in which the mercantile (MERCADONA) has been an interested party in the order of which it brings cause for facts referring to the treatment now under analysis. It reproduces at effects of the references to it appear in this Proposal of Resolution.

The aforementioned Order states the following (the underlining is from the AEPD):

<< LEGAL REASONING

FIRST.- The mercantile MERCADONA requests the adoption of the measure, understanding that biometric data is obtained through security cameras security when a subject enters the premises. To do this, set as regulations to follow the Regulation of the European Union 2016/679 of the Parliament European and Council of April 27, 2016 on the protection of persons physical with regard to the processing of personal data and the free circulation of these data. The appellant understands the fact that, the category of biometric data is recognized in said Regulation as data of special protection, does not exclude its use, provided that it is carried out with all the relevant security measures. It is understood by said company that with the security measures proposed is not injured in any moment the protection of data of the subjects, since, although they are processed the biometric data of every user who enters one of the establishments, the system instantly detects (in 0.3 seconds) those individuals who have been sentenced with a ban on entry to the aforementioned establishment through the final judgment in a judicial process; consequently, not will not remain in the system any biometric data of a person who has not been condemned and will be immediately deleted and never used.

The appellant advocates considering that the purpose of the Legislator in the development of the General Data Protection Regulation is not only to protect

the rights of natural persons but also the free movement of data taking into account the progress of technology. That is why, it would be absolutely ineffective to try to solve a problem such as the control of those

individuals who have been sentenced in a final sentence with a prohibition of

entrance, trying to show the image of said individuals to dozens of

employees of establishments so that they could identify them and

denounce them. It is argued that not taking advantage of the advantages that progress brings us

offers, being able to do so while ensuring the protection of natural persons, it is

condemn the human being, as well as the Spanish legislative development of the last

decades.

The appellant invokes the suitability, necessity and proportionality of the

requested measure. First, it is effective, because it addresses the problem at hand.

presents, in order to achieve its objective, which is to identify all those

individual who, despite having a final judgment that prevents him from entering

one of its establishments, may violate the decision of the judicial body and

also the rights of the company itself. It is necessary, because it is the only

as it confronts the problem and solves it, given that the previous measures

that have been taken, have been completely ineffective due to the

impossibility of exercising control in all establishments by

all the employees; and finally, it is proportional, since it provides more

benefits to the general interest than harm to the particular individual in

so much so that it does not imply any treatment of the biometric data of the subjects

in general terms, implying a treatment only of those individuals

who have been sentenced by a final judgment...

SECOND.- Well, delving into the substance of the request made,

It is true that it is an issue that raises many doubts at the legal level.

We must remember that after the approval and entry into force of the Regulation

general data protection - directly applicable from May 2018 - the treatment will only be lawful if at least one of the following is met

conditions:

* the interested party gave their consent for the processing of their data

personal for one or more specific purposes;

* the treatment is necessary for the execution of a contract in which the

interested party is a party or for the application at the request of the latter of measures

pre-contractual;

* the treatment is necessary for the fulfillment of a legal obligation

applicable to the data controller

* the treatment is necessary to protect the vital interests of the interested party or of

another natural person;

* the treatment is necessary for the fulfillment of a mission carried out in

public interest or in the exercise of public powers vested in the controller

of the treatment;

* the treatment is necessary for the satisfaction of legitimate interests

pursued by the data controller or by a third party, provided that

over said interests do not prevail the interests or the rights and freedoms

fundamental data of the interested party that require the protection of personal data,

in particular when the interested party is a child.

In other words, the Regulation contemplates the obligation that the user

of your consent to process your personal data. When we talk about facial recognition, we must understand the reference to data biometrics The regulation defines them as "personal data obtained from of a specific technical treatment, related to the physical characteristics, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as facial images or data data". In case there was any doubt, section 1 of art.9 of the aforementioned The legal text provides that "The processing of personal data that reveal ethnic or racial origin, political opinions, convictions religious or philosophical beliefs, or trade union affiliation, and data processing genetic, biometric data aimed at uniquely identifying a person natural person, data relating to health or data relating to sexual life or sexual orientation of a natural person.

According to the mercantile MERCADONA S.A, the system "detects, unique and exclusively, the entry of people with final judgments and a precautionary measure restraining order in force against Mercadona or against any of its workers or workers. But, it should be asked before the measure invoked, where do they take images for facial recognition, with what consent, but it is more certain that people with a final judgment have a right to privacy or why they maintain a database of pictures of people

The system used "carries out the identification in real time and erases immediately all the information, only using the results positive to contact the authorities in case of detection.

Mercadona alleges that there is no data processing and that is why it refers to 0.3 seconds. It is, however, surprising to say the least amparen in the "speed". No matter how fast, there is a violation of the privacy. Both the speed argument and the non-processing of data They fall under their own weight.

We are clearly facing what the European Union has called "authentication". In the White Paper on artificial intelligence of the European Commission of 19 February 2020 it is established that "as far as facial recognition is concerned,

by "identification" it is meant that the facial image template of a person is compared with many other templates stored in a database data to find out if your image is stored in it. The "authentication" (or "verification"), on the other hand, usually refers to the search for correspondences between two specific templates. Allows comparison of two biometric templates that, in principle, are supposed to belong to the same person; thus, the two templates are compared to determine if the person in the two images is the same. This procedure is used, for example, in automated border control gates used in checks airport borders.

This is a complex issue. In the words of the AEPD itself in its report 36/2020, "according to the aforementioned distinction, it can be interpreted that, according to with article 4 of the RGPD, the concept of biometric data would include both assumptions, both identification and verification/authentication. Without However, and in general, the biometric data will only have the consideration of a special category of data in the cases in which undergo technical treatment aimed at biometric identification (one-to-one several) and not in the case of biometric verification/authentication (one-to-one). Nope However, this Agency considers that this is a complex issue, subject to interpretation, from which no conclusions can be drawn general, having to attend to the specific case according to the data processed, the techniques used for its treatment and the consequent interference in the right to data protection, and must, as long as it is not pronounced in this regard the European Committee for Data Protection or the bodies jurisdictions, adopt, in case of doubt, the most favorable interpretation for the protection of the rights of those affected." In the present case, it is There is no doubt that the use of facial recognition in information systems video surveillance used in the field of private security would imply the processing of biometric data aimed at uniquely identifying a natural person, in a one-to-one matching process several, constituting the treatment a special category of data whose treatment, in principle, is prohibited by article 9.1 of the RGPD

The Spanish Agency for Data Protection in a report dated May 28, 2020 made the matter quite clear, concluding that

* Facial recognition techniques for biometric identification purposes involve a treatment of special categories of data for which the Regulation requires reinforced guarantees

* To treat special categories of data for these purposes, the regulations requires that there be an "essential public interest" contained in a standard with range of law that does not currently exist in the legal system.

* The Agency rejects that the legitimacy recognized for the systems of

video surveillance that only capture and record images and sounds can cover

technologies such as facial, gait or voice recognition.

As rightly ruled by the Spanish Data Protection Agency in

the aforementioned report, so that facial recognition could have a better

legal protection would require a specific law. Today there is no rule

in our legal system regarding facial recognition.

The existence of a public interest does not legitimize any type of data processing.

personal data, but must be, in the first place, to the conditions

that the legislator may have established, as provided for in article 6 of the

RGPD, in its sections 2 and 3, as well as the aforementioned principles of article 5

of the RGPD, especially those of limitation of the purpose and minimization of

data. And in the event that they are going to be the object of treatment of one or more

of the personal data included in the special categories of data to those

referred to in article 9.1. of the RGPD, that any of the

circumstances contemplated in its section 2 that lifts the prohibition of

treatment of said data, established in general in section 1.

Therefore, the use of facial recognition technologies in

video surveillance systems involves the processing of biometric data, as

as defined in article 4.14 of the RGPD and supposes the treatment of categories

special data regulated in article 9 of the RGPD, as it is "data

biometrics aimed at uniquely identifying a natural person".

we are facing a simple authentication, but rather an identification, so requires a double legitimation.

Although article 48 of the Penal Code establishes "the deprivation of the right to residing in certain places or going to them prevents the convict from residing or going to the place where the crime was committed" and that "the judge or court may agree that the control of these measures be carried out through those means that allow it"; this would occur by ensuring the rights of the sentenced person, that is, provided that he had given his consent. We must remember that the condemned enjoy all the fundamental rights recognized in the Constitution, with the exception of those are expressly limited by the content of the conviction, the sense of punishment and penitentiary law.

THIRD.- Beyond data protection, you could enter into other restraining order issues. Behind the formalism of a restraining order, there are many issues to consider for the crime to be committed, such as notification and prior request and expressed to the sentenced person, and the validity at that time of the order of remoteness. These are issues that can be very complex for a third for sure.

Not everything goes in terms of Fundamental Rights. These technologies can be really intrusive and require a calm ethical and legal debate, all time they can have very adverse effects on core values and the human integrity.

This analysis is necessary to be able to determine the legality or not of this treatment, especially considering the particularities of the category of data being processed, biometric data and therefore especially protected. This is so by making possible the images of the faces of the interested parties the direct, unique and unequivocal identification of all the people being recorded. Collecting images for later recognition must meet the criteria and standards contained in the General Data Protection Regulation, in accordance with which we are faced with an intensive treatment of biometric data, which thus poses situations of high incursion in the private sphere and in the fundamental right of protection of personal data of the interested parties. So much so that in order to be authorized and confirm the legality of this type of treatment, the correct appreciation of aspects such as the nature and origin of the data, the mode of development of the same and, above all, the purpose. These items must be studied together with the informative principles of the regulations in question, in order to determine whether the measures implemented are proportional to the intrusion into the private sphere of the interested parties they suppose.

In accordance with the personal data protection regulations, the processing must always respect a minimum level of proportionality between the intrusion that these treatments can entail in the private sphere of people and the conditions and guarantees that accompany this to be able to correct the possible adverse effects that they entail. Thus, it is established that for those treatments that require data from special categories, as is the case biometric data, the explicit consent of the user must be obtained.

interested as a basis for the legitimacy of the uses and actions that are to develop with your information. In the case at hand, and for the moment,

the express consent of the interested parties is not being obtained, giving

also a situation in which hardly the two parties, company and client,

may be considered with the same capacity to negotiate the effects of granting

consent or not, as this translates directly into the impossibility by

part of the direct customer to continue making their purchases in that supermarket.

The level of intrusion into the private life of the interested parties must enter into the

aforementioned judgment of proportionality, which according to the regulations therefore requires

the expression of the explicit consent of the interested parties. if this

consent is not explicitly collected and is not collected by methods of

test as it can be a written support, as is the case in this

facial recognition treatment, this must be remedied with the support of

another basis of legitimacy strong enough to justify itself

the need for this treatment to obtain the desired purposes, such as

be the maintenance of the proper functioning of the business and the prevention

against robberies, thefts and situations of insecurity for the workers of the

business. This basis of legitimation, assures Mercadona, through its

petition, is the "public interest" that is collected in the same way as legitimation

exceptional in the personal data protection regulations. Nevertheless,

This creates doubts when interpreting its validity or lack of it in this

case, since the implantation of this technology really serves in a greater way to a private purpose of the company, such as guaranteeing the safety of its

installations.

Regarding the implementation of facial recognition technologies and their use

appropriate for the guarantee and maintenance of the security of physical places,

the AEPD ruled in response to a query by a company of

private security, within Report 010308/2019, which remains to date

Today, the regulatory framework dedicated to regulating this type of treatment is insufficient.

and considering that it will be necessary to approve "a standard with a range of

law that specifically justified to what extent and in what circumstances, the use

of said systems would respond to an essential public interest" for the correct

definition of the legality requirements for this type of treatment.

… But what is more, this Chamber cannot share that with the interested measure

is protecting the public interest, but rather, private interests or

of the company in question, because as has already been explained in the

previous paragraphs, the adequate guarantees would be violated in order

to the protection of the rights and freedoms of the interested parties, not only of the

who have been punished and whose prohibition of access concerns them, but of the rest

of people who access the aforementioned supermarket.

(…) >>

v

Once the legal doctrine to be applied in the present case has been exposed, it is appropriate to enter into the

procedural issues.

From the previous investigative actions, it is concluded that Mercadona carries out

a treatment of personal data of biometric data (art. 4.14 of the RGPD)

in order to uniquely identify a specific person among several

(hereinafter one-to-several) being subject to the guarantees of the provisions of the art. 9 of the GDPR.

The treatment does not only occur in relation to the identification of convicted criminals with the imposition of a security measure, as a result of restraining order imposed on those in a criminal sentence, but rather affects anyone who enters one of its supermarkets (including minors) and its employees.

The data processing implemented by Mercadona includes capturing, collating, conservation and destruction -in case of negative identification- (after 0.3 seconds of its collection) of the biometric image captured from any person that enters the supermarket (collection, collation, conservation and destruction are four forms of treatment according to the definition of art 4 of the RGPD).

Mercadona expressly recognizes that there is processing of personal data of biometric character, and thus, for example, in the provided EIPD it states the following:

“The data will be kept:

• Relating to the sentence and the image provided: During the validity period of the the final sentence that imposes the restraining order.

• Related to camera negatives: The treatment will be 0.3 seconds (time between capture and deletion after comparison).

• Relative to the positives of the camera: Duration necessary for its implementation. available to the State Security Forces and Bodies”.

It should be noted that the preservation of facial images for the brief time lapse of 0.3 seconds constitutes a processing of personal data biometrics for "one-to-many" identification purposes, without stating accredited any of the exceptions for the treatment indicated in article 9.2 of the RGPD, so it is not even appropriate to apply the legal bases indicated in article 6 of the RGPD.

The data that is processed is biometric data, whose definition is inherent in article 4.14 of the RGPD: “personal data obtained from a specific technical treatment, related to the physical, physiological and or behavioral of a natural person that allow or confirm the identification unique to that person, such as facial images or fingerprint data”.

In this specific case, it involves the treatment of special categories of data regulated in article 9 of the RGPD, as it is "biometric data aimed at uniquely identify a natural person. Similarly, the recital 51 of the RGPD also reasons that "there are only included in the definition of biometric data when the fact of being treated with specific technical means allows the identification or unequivocal authentication of a natural person.

Report 36/2020 of the Legal Office of the AEPD asserts, without prejudice to address the complexity of the issue and the impossibility of extracting general conclusions, that “biometric data will only have the consideration of a special category of data in the cases in which undergo technical treatment aimed at biometric identification (one-to-one

several) and not in the case of biometric verification/authentication (one-to-one)",

as in the present case.

In the same sense, the European Committee for Data Protection (hereinafter

CEPD) considers the use of video surveillance with facial recognition as

special category of data of article 9 of the RGPD in its "Guidelines 3/2019 on

processing of personal data through video devices".

SAW

According to Mercadona, the purpose of the facial treatment and

One-to-many remote control is to monitor compliance with a security measure.

security imposed by a sentence on a convicted person in a criminal proceeding in

which Mercadona has been a part.

It links the establishment of this surveillance system with facial recognition to the

dictation of several sentences in which a security measure is imposed

referring to the removal of a person convicted of a minor crime.

Said security measure consists of the removal of the sentenced person to a

supermarket or various specific Mercadona or stores of a

certain territory for a period specified in the judgment that

in no case exceeds six months (art. 57.3 of the CP).

Likewise, as a result of the express request for this security measure by

part of Mercadona in the criminal procedure, the judicial resolution allows

establishment of electronic means to control such measures of

security as provided in art. 48.4 of the PC.

In some judgments it is made explicit that such electronic means may be

facial recognition, processing biometric data (one-to-many). that happens

because Mercadona, if asked about the security measure in the process to which it is a party, requests that the security measure be executed

through electronic means, specifying it in electronic means

consisting of facial recognition.

From the sample of Judgments previously provided by Mercadona in relation to

with security measures and the use of electronic means, what is extracted is

Next:

(…)

In view of the sample of Judgments that we have, we have to

conclude that:

The security measure agreed upon by the judicial body affects

□

only the convicted person and his legal sphere of rights.

The security measure comprises electronic means with

□

facial recognition. But not all sentences authorize Mercadona to

install that system "one-to-many" (identification), but some do

generic mention of electronic means that allow the control of this measure

of security without specifying that it is facial recognition and, as has already been

commented previously, the electronic means of facial recognition do not

they have to be of the “massive and remote” type.

The use of remote biometric identification systems massively, indiscriminately and remotely in spaces of public access to effects of the application of a judicial resolution must take into account the nature of the situation giving rise to the possible use, in particular the severity, probability and magnitude of harm caused in the absence of use of the system and also the consequences of using the system for the rights, guarantees and freedoms of all affected persons, including those convicted.

In addition to the existence of a cause for lifting the general prohibition that indicates Article 9.1 of the RGPD, the use of biometric identification systems in a massive (“one-to-many”), indiscriminate and remotely in access spaces public for the purposes of the application of a judicial resolution should comply, In addition, the necessary and proportionate safeguards and conditions in in relation to the use, also with regard to temporary limitations, geographical and personal of those affected.

In the present case, the judicial resolutions previously provided by Mercadona do not specify how to carry out access control to supermarkets, and the guarantees, rights and freedoms of those affected cannot remain at the mercy of unilateral interpretation and decision on the scope of judicial resolutions on the impact on those affected (convicted, employees and clients, including minors) of such treatment by the responsible company (Mercadona).

Regarding massive and remote facial recognition (“one-to-many”), the book White on Artificial Intelligence indicates what biometric identification is remote, under the following terms:

“Remote biometric identification should be distinguished from authentication biometrics (the latter is a security procedure based on the unique biological characteristics of a person to verify that it is

who he claims to be). Remote biometric identification consists of determining the

identity of several people with the help of biometric identifiers

(fingerprints, facial images, irises, vascular patterns, etc.) at a distance,

in a public space and in a continuous or sustained manner, contrasting them with

data stored in a database.

The treatment now analyzed is characterized by:

Use biometric data, which are special categories of data from art.

□

9 of the RGPD (one-to-many) on which a general prohibition of

use, except as provided in the standard itself. This treatment is

therefore exceptional.

□

It is produced remotely in a space accessible to the general public.

It is a continuous treatment that contrasts the data collected with other

□

stored in a database.

□

It is an automatic treatment.

It is of extremely high risk (unacceptable) as it can lead to

□

massive and indiscriminate surveillance.

How can we verify the processing of data using

□

remote biometric identification is automatic, and the biometric data is captured deals) automatically; therefore it is considered extremely high risk (unacceptable) this data processing.

Furthermore, we cannot ignore that the implementation of remote biometric “identification” of the “one-to-many” type (special category of personal data, art 9 RGPD) collects much more information than other types of treatment and, moreover, involuntarily and without knowledge or consent, by establishing guidelines and using preset algorithms that determine the elaboration of a certain pattern (matrix) characteristic of the image treated for each affected person.

In the treatment now analyzed, a system of indiscriminate and massive facial recognition since “depending on the data biometrics collected, subject data such as race or gender may be derived (including fingerprints), their emotional state, illnesses, defects and genetic characteristics, substance use, etc. Being implicit, the The user cannot prevent the collection of said supplementary information” -Note of the AEPD on the "14 misunderstandings in relation to the identification and biometric authentication”. This excess of processed data also violates the minimization principle provided in art. 5.1.c) of the GDPR.

It is Mercadona (as data controller) who has decided to implement a system of these characteristics that was not previously available, consequence of his participation in a criminal judicial proceeding in which he has been party and has requested that the specific security measure be authorized consisting of the use of a facial recognition system.

This shows us that Mercadona has requested in the judicial process the security measure linked to facial recognition, before carrying out a EIPD, before assessing whether it could carry out the treatment in accordance with the data protection regulations and before evaluating the risks of such treatment of data. In this sense, it is insisted, there is no evidence in this AEPD that there carried out the prior consultation referred to in art. 36 of the RGPD, whenever implanted treatment not only carries an extremely high risk (unacceptable) undermining the rights and freedoms of customers and Mercadona workers, but it is prohibited by art. 9.1 of the GDPR. In this sense, it should also be noted that in the risk analysis carried out treatment should previously have been found to be an unacceptable risk and, in consequently be avoided.

Mercadona has requested the adoption of the security measure in the criminal procedure and, once agreed, asserts it to justify the exception of art. 9.2 of the GDPR; that is, it has preconstituted the legitimation necessary to carry out the treatment of biometric data in a massive way and remote “one-to-many”. Let us remember that this security measure is dictated solely with respect to the sentenced person and that only affects the limitation of their rights in the terms of the judicial resolution without affecting third parties, such as Mercadona's customers and workers. It has to be done proportionality trial before requesting this measure before the judicial body,

as will be seen later.

7th

We begin by examining whether Mercadona has legal standing to carry out this

treatment type in the mentioned conditions.

Mercadona asserts that it has legitimacy based on public interest (art.

6.1.e) of the RGPD) for video surveillance purposes and that the

exception of art. 9.2.f) of the RGPD that allows you to process data

special category biometrics, that is, the circumstance that the treatment

it is necessary for the formulation, exercise or defense of claims.

The legal basis for the treatment alleged by the company is based on the previous

lifting of the general prohibition imposed by art. 9.1 of the GDPR through

of the application of art. 9.2.f) of the RGPD and, subsequently, reference to art.

6.1.e) GDPR. First, the exception of art. 9.2.f) of the RGPD does not concur

for the potential clients in the treatment now analyzed (nor for the

workers) according to the AEPD report 010308/2019 already mentioned and, in

second, the legal basis provided in art. 6.1.b) RGPD is also not valid

for the employees since it is a treatment outside the

video surveillance system.

As we have pointed out before, we can observe in terms of legitimation,

that in the treatment examined there are three types of interested parties affected

for this one. On the one hand, the processing of biometric data of a convicted

for the imposition of a security measure of restraint in a sentence

penal; on the other, the processing of biometric data of potential clients of Mercadona; lastly, the treatment of the biometric data of the users themselves

Mercadona employees.

□

Legitimation regarding the data of a convicted person.

Mercadona bases the treatment on the exception provided for in art. 9.2.f)

of the RGPD to consider that they are legitimated to carry out the

biometric data processing. The art. 9.2.f) of the GDPR lifts the ban

general provided for in art. 9.1 of the RGPD when “the treatment is necessary

for the formulation, exercise or defense of claims or when the

courts act in the exercise of their judicial function.

According to the Report of this AEPD reference 0098/2020, it is concluded that:

(Yo)

the RGPD mentions separately the out-of-court claims of

diverse nature and the administrative ones, and on the other hand, those claims

that are promoted through the judicial bodies.

(iii)

should be understood the lifting of the prohibition of treatment of

special categories of data such as exceptional, subsidiary and the interpretation of

its application must be restrictive, in accordance with the special protection of the

who are creditors of this type of data derived from its legal nature.

the national or European Union law that regulates these treatments

(iii)

it must offer sufficient guarantees to protect the rights of those affected.

(iii)

is that although the RGPD establishes assumptions that exempt the prohibition of treatment of special categories of data, through the right In many Member States, ad hoc regulations can be introduced in order to to adapt the reality of the sectors involved to guarantee protection effective protection of the rights of citizens of the union.

The aforementioned report adds that, in general, the assumptions that raise the general prohibition of treatment provided for in article 9.2 RGPD, only serve this purpose, that is, they act as exceptions to the provisions of section 1, which does not mean that whenever any of them occurs, the treatment can given or must be carried out, since the remaining obligations must be fulfilled. they derive from the GDPR itself. That is, the mere existence of a claim to the protection of article 9.2 f) RGPD, does not legitimize by itself, the treatment of categories special data categories, but must be accompanied by other elements, that do not appear, that make the treatment in accordance with the RGPD.

The treatment of biometric data (“one-to-many”), in this case, could occur if necessary for the formulation or exercise or defense of claims or when the courts act in the exercise of their judicial function.

However, strictly speaking, in accordance with the literal nature of the legal norm, and for the assumption now examined, the formulation, exercise or defense of Claims have already been made, since the complaint made by Mercadona derives the situation in which we now find ourselves.

But, we could understand that the imposition in a final judgment of a security measure is consequence and continuation of the claim filed, thus being able to include this measure derived from the claim in the framework of the transcribed precept. However, in any case, the treatment of biometric data for the formulation, exercise or defense of claims would be restricted to the biometric data of the defendant and in the strict terms and scope of the judicial resolution and not of third parties totally outside the procedure and even less from the free unilateral interpretation by the of the scope of the judicial resolution.

Recital 52 of the RGPD, regarding the prohibition of the treatment of special categories of personal data, authorizes the exceptions “always that adequate guarantees are given”, indicating that “It must also be authorized exceptionally, the processing of said personal data when it is necessary for the formulation, exercise or defense of claims, whether by a judicial procedure or an administrative or extrajudicial procedure”.

As it is an exceptional authorization, which requires adults -in case of be able to be applied-the establishment of adequate guarantees, the interpretation granted must be restrictive. This is provided for in recital 51 of the RGPD that includes the restrictive character with which the treatment of these data, when it states that "Such personal data should not be processed, unless unless their treatment is allowed in specific situations contemplated in this Regulation, taking into account that Member States may establish specific provisions on data protection in order to adapt the application of the rules of this Regulation to comply with a legal obligation or the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the data controller.

In addition to the specific requirements of that treatment, the

general principles and other rules of this Regulation, especially as regards

which refers to the conditions of legality of the treatment"; this interpretation is

collected systematically by the AEPD in its resolutions -for all of them, the

PS/00145/2019-.

Let us bring up the art. 10 GDPR. This precept allows the treatment

of personal data related to convictions and criminal offenses or measures of

security, in relation to the personal data concerned in such convictions,

violations or security measures. In our case, and with the diction of the

article would only affect the personal data of the convicted person. And in

In relation to the exception of art. 9 of the RGPD, to the biometric data of the

condemned.

In addition, it requires, or that it be executed under the supervision of the authorities

public or authorized by the Law of the Union or of the Member States

that establishes adequate guarantees for the rights and freedoms of

interested.

In this case, the supervision of the Judicial Authority occurs if the

condemned violent security measures. The Judicial Authority neither reviews nor

has reviewed the facial recognition system implemented in general,

nor the impact of the implementation of such a system on the rights and freedoms of the rest of the citizens (customers and Mercadona workers).

In fact, if the security measure were applied directly by the body

court could not extend it to other subjects than the convicted or

third parties summoned in the procedure and directly affected by the measure

of security. Consequently, what a judge cannot do in compliance

of their own measures, much less an individual who collaborates.

Regarding the treatment of biometric data in a massive and remote way “one-to-

several” of a person convicted of imposing a security measure of

removal in a criminal sentence, the company states that the legal basis

of treatment would be that of art. 6.1.e) of the RGPD, thus forgetting the need for

prior lifting of the general prohibition imposed by art. 9.1 of the GDPR.

Mercadona asserts about the security measure that "This legitimation, although

does not require legal authorization or a specific determination at the

normative, it must be framed within the Spanish procedural system”.

However, in the face of such an affirmation, the truth is that art. 8 of the LOPDGDD is

exhaustive in the sense that "The processing of personal data may only be

be considered founded on the fulfillment of a mission carried out in the interest

public or in the exercise of public powers conferred on the controller, in the

terms provided for in article 6.1 e) of Regulation (EU) 2016/679, when

derives from a competence attributed by a norm with the force of law”. In

Consequently, it is mandatory legal authorization for such legal basis to arise

effects.

Well, in reality it is that the legal basis contained in art. 6.1.e) of the

RGPD could legitimize the processing of data of the sentenced person with respect to a

specific security measure (provided you have an authorization

between those of art. 9.2 of the RGPD), understanding that they carry out a mission in public interest, by order of the judicial body that has been assigned for the sake of the Law empowered to do so (art 17 of the Organic Law 6/1985, of July 1, of the Power Judicial). However, as has already been pointed out, there is also no evidence that the measure of security is an essential public interest since what it would protect would be a private interest of the business.

In this sense, the GT29 in its Opinion 06/2014 on the concept of interest public of the data controller pursuant to art. 7 of the Directive 95/46/EC, examines what is meant by mission in the public interest, stating that "Article 7, letter e), covers two situations and is relevant for both the public and private sectors. First, includes situations in which the data controller himself has

a public power or a mission of public interest (but not necessarily a legal obligation to process the data) and the processing is necessary for the exercise of said power or for the execution of said mission".

“However, the treatment must be “necessary for the fulfillment of a public interest mission. Alternatively, a power must have been conferred official either to the person in charge of the treatment or to the third party to which this communicates the data and the data processing must be necessary for the exercise of said power. It is also important to emphasize that this power official or mission of public interest should be conferred or attributed normally through ordinary laws or other legal regulations. If the treatment involves an invasion of privacy or if this is otherwise required under the national legislation to ensure the protection of affected persons, the The legal basis must be sufficiently specific and precise when define the type of data processing that can be allowed”.

In endorsement of the affirmed, we only have to examine the art. 10 GDPR quoted by the company: “The processing of personal data related to convictions and criminal offenses or related security measures based on the Article 6, paragraph 1, may only be carried out under the supervision of the public authorities or when authorized by the Law of the Union or of the Member States that establish adequate guarantees for the rights and freedoms of the interested parties. A complete record can only be kept criminal convictions under the control of public authorities”.

In our case, that legitimation that we now find based on the mission in the public interest and collaboration with justice, would be different from the interest public employee by the mercantile that legitimizes, via art. 6.1.e) of the RGPD and the art. 22 of the LOPDGDD video surveillance, especially because, as already we have indicated, in some of the judgments examined there is generically of the use of electronic means to control the measurement of security, without specifying in a "specific and precise way when defining the type of data processing that can be allowed”.

Legitimation regarding the data of potential clients of

□

Mercadona.

The company wields the exception provided for in art. 9.2.f) of the GDPR cited above to proceed with the treatment of biometric data "one-to-many" of the Mercadona customers.

As we have indicated previously, the exception provided for in art. 9.2.f) of the RGPD, regarding the formulation, exercise or defense of claims, must be interpreted restrictively and in its own terms, by its exceptionality in view of the prohibition contained in the first section of art. 9 of the GDPR.

We have also meant that the proper understanding of art. 9.2.f) of the RGPD limits, according to a literal, systematic and teleological interpretation of the standard, the use of special categories of personal data in cases in which the treatment of such data is necessary for the formulation, the exercise or defense of claims. Thus, we could understand that the concept "formulation", "exercise" and "defense" could not only accommodate the formulation, exercise or defense of a claim, but that could extend to the execution of the resolution obtained after the formulation, exercise or defense of the claim, within the framework of guardianship effective court.

Let's transfer it to domestic law and to the specific "claim" process, since that the exception is not indifferent to the functioning of the procedural system Spanish.

In the case examined, the treatment consisting of the recognition face, which, let us remember, has been chosen by the merchant, derives from the imposition of a security measure to a specific person, in accordance with a judgment favorable court ruling obtained by Mercadona. Being, in our case, a criminal judicial procedure and constraining it to the characteristics and elements definitions of the same established in the legal system, would only affect the parties to the procedure (including, where appropriate, a third party when there is summoned by the judicial body so that it can defend what in its incumbent right), without being able to extend its effects to third parties outside the same.

When adopting the security measure, the judicial body weighs, as it can only being, the affectation of the security measure in the Fundamental Rights of the condemned. The judicial body does not examine the affectation of the measure of safety in third parties unrelated to the procedure nor does it value or weigh what incidence produces such a measure of security in the Fundamental Rights of the latter (intimacy and protection of personal data, among others).

And this because such a decision does not concern them at all.

A criminal sentence between parties does not per se enable data processing biometrics massively "one-to-many", remote and indiscriminate, affecting to an important and undetermined group of the population, including minors.

In addition to the total disproportion implied by the implementation of this system, which we will talk about later. Extrapolating it, we would arrive at the absurdity that, by imposing a security measure for a subject or subjects specific in a judicial sentence, or even in an administrative resolution, the establishment of a facial recognition treatment could be enabled massive, which would violate the letter and spirit of the RGPD.

The exception provided for in art. 9.2.f) of the RGPD, due to the effect on the categories of sensitive data and the risks inherent to the treatment, you must extreme care in its restrictive interpretation when it affects a

indeterminate and massive plurality of people, and who are totally alien to the

court decision issued.

It only enables the parties to the claim to use the biometric data

precise to exercise the claim itself, restricting it to the affectation

specific number of people referred to in the process and the subsequent resolution

judicial. The biometric data of any potential Mercadona customer is not

have been necessary to formulate the complaint. However, this treatment

facial recognition implanted by Mercadona, seen as a whole

directly affects all of Mercadona's potential customers, being

strictly unrelated to the claim itself.

In conclusion, art. 9.2.f) of the RGPD could lift the prohibition, but

restricting such legitimation to a specific sentence and with express scope in

the same and in relation to the specific security measures imposed,

with respect to the persons mentioned in it, and for a territorial scope (a

territory, or one or more supermarkets) and limited time. This is only

regarding the condemned.

However, the facial recognition system implemented by Mercadona,

that lacks legitimacy based on art. 9.1 of the RGPD, it is highly

intrusive, indiscriminately affecting an indeterminate number of

citizens. They are indirectly imposed a security measure of

criminal nature.

It generates a perverse effect, because finally with those ***NUM.2 processes courts that they say they file annually throughout the Spanish territory, practically in all supermarkets they would have activated a system of facial recognition, monitoring all Mercadona customers, usual or not. It would result in practice in the establishment on a large scale of a highly intrusive facial recognition system in the rights and freedoms of those affected. It carries an extremely high risk acceptable.

In this sense, in the "Guidelines on Facial Recognition" of January 2021 of the “Consultative Committee of the Convention for the protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108”, it is stated that private entities cannot develop recognition systems facial in uncontrolled environments such as shopping malls, especially for identify persons of interest for security purposes: “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”.

(“Private entities shall not use facial recognition technologies in uncontrolled environments such as shopping malls, especially for identify persons of interest, for marketing purposes or for the purpose of Private security". The translation is from the AEPD).

Regarding rights, the aforementioned Guide clarifies that they can be restricted only when a law establishes it, that is, that now, in our assumption, the The rights of the interested parties cannot be restricted: “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+”.

(“These rights may be restricted but only when that restriction is provided by law, respects the essence of the rights and freedoms fundamental and constitutes a necessary and proportionate measure in a democratic society for specific legitimate purposes (such as enforcement purposes) of the law), in accordance with article 11 of the Convention 108+”. (The translation is from the AEPD).

On the other hand, we must examine whether the company has legitimacy for the treatment of biometric data of a special nature (“one-to-many”) of the Potential Mercadona customers.

Apart from the general prohibition imposed in art. 9.1 of the RGPD that affects biometric data of a special nature, let's go back to the art. 6.1.e) of the RGPD cited by the company. The legal basis -if they were not data biometrics of a special nature - would be the same, the public interest, but in this case is not based on the competence of a judicial body that for the execution of a security measure allows one of the parties in the process the processing of personal data of the convicted person (mission in the interest public). It is obvious that citizens, in general, potential clients of Mercadona have not been part of the procedure, they are not cited in the sentence, nor have been considered for the purpose of implementing any electronic means, nor are affected by it.

The public interest could apparently be found in this case inherent in a treatment in video surveillance. Article 22 of the LOPDGDD regulates the treatments for video surveillance purposes whose legitimacy is found, as As stated in the Statement of Motives of the referenced legal text, in the existence of a purpose of public interest incardinable in article 6.1.e) of the RGPD, having the purpose of "preserving the security of people and goods, as well as its facilities", an objective that goes beyond the mere interests legitimate of an individual.

In the field of private security, said regulation must be completed with the provided in its specific regulations, this is the Private Security Law (LSP), in which article 42 regulates video surveillance services. states that

“Video surveillance services consist of the exercise of surveillance through camera or video camera systems, fixed or mobile, capable of capturing and recording images and sounds, including any technical means or system that allow the same treatments as these.

When the purpose of these services is to prevent infractions and avoid damage to persons or goods object of protection or prevent unauthorized access, They will necessarily be provided by security guards or, where appropriate, by rural guards.

In the case examined, the video surveillance will be carried out by a

private security company.

However, as reasoned in Report 31/2019 of the Legal Cabinet

(entry: 010308/2019) of the AEPD "video surveillance processing

regulated in the LOPDGDD and in the LSP, refer exclusively to the

treatments aimed at capturing and recording images and sounds, but do not include

facial recognition treatments, which is a radically

different when incorporating a biometric data, as the RGPD itself recalls in its

Considering 51 when stating that "The treatment of photographs should not

systematically consider treatment of special categories of data

personal, since they are only included in the definition of

biometric data when the fact of being treated with technical means

allows the unique identification or authentication of a person

physical.

Therefore, the incorporation into video surveillance systems, aimed at

the capturing and recording of images and sounds, of applications of

facial recognition will involve the processing of biometric data, regarding

of which the data protection authorities had been warning of the

risks that they imply for the rights of the people".

The aforementioned report includes various documents of the Working Group of the article

29, such as Opinion 4/2004 regarding the processing of personal data

through video surveillance, the working document on biometrics,

adopted on August 1, 2003 or Opinion 3/2012 on the evolution of the

biometric technologies, adopted on April 27, 2012, in which it is exposed

the difference between conventional video surveillance systems and the

facial recognition, also indicating a diverse set of risks important and significant such as discrimination, such as the fact that the treatment can be carried out without the knowledge of the interested party, the possible widespread use and errors that may occur.

In accordance with the foregoing, the legal basis included in art. 6.1.e) of the RGPD in relation to art. 22 of the LOPDGDD would be enough to carry carry out an ordinary video surveillance treatment (not of a special nature). But would not be enough for a facial recognition system in the terms

exposed, that is, a radically different treatment when using data biometrics in a massive and remote way of the "one-to-many" type, without previously lifted the prohibition established in art. 9.1 of GDPR. For the Therefore, it would be necessary to determine what is the precise legal basis to carry out carry out a facial recognition treatment (“one-to-many”), as well as the precise legal requirements for it.

Report 31/2019 of the Legal Office (entry: 010308/2019) considers that “The current regulation is considered insufficient to allow the use of facial recognition techniques in video surveillance systems used by private security (...) being necessary that a norm be approved with range of law that would specifically justify to what extent and in what cases, the use of such systems would respond to an essential public interest, defining said legal norm, after weighting by the legislator of the conflicting interests in accordance with the principle of proportionality, each and every one of the material budgets of the limiting measure through rules

precise, that make the imposition of such limitation and its consequences foreseeable for the interested party.

consequences, and establishing the technical, organizational and

adequate procedural measures, which prevent risks of different probability

and severity and mitigate their effects.

The report concludes that the use of facial recognition systems of

video surveillance systems used by private security is

disproportionate, in attention to the intrusion and the unacceptable high risks

that it implies for the fundamental rights of citizens. At least

when it comes to configuring the exception of art. 9.2.g) of the RGPD as a

essential public interest, specifying the need for specific legal regulation

(art 8.2 LOPDGDD). The Legal Report 010308/2019 of the AEPD indicates "...

In the case of special categories of data, the assumption contemplated in the

letter g) of article 9.2. does not refer only to the existence of a public interest, such

and as the RGPD does in many other of its precepts, but it is the only

RGPD precept that requires that it be "essential", an adjective that comes

to qualify said public interest, taking into account the importance and necessity of

greater protection of the processed data.”

For all these reasons, we can consequently glimpse that, in attention to the

special characteristics of the data processing that is carried out (with risk

extremely high unacceptable), we are not faced with what

we could define it as a current, ordinary video surveillance system; East

implanted system that incorporates facial recognition applications has its

own entity and virtuality, since it deals with biometric data aimed at identifying

a unique way to a natural person through facial recognition, in

a “one-to-many” matching process (the condemned and the other people who access supermarkets, whether they are potential customers or employees) and massively and remotely. This has been stated by the CEPD.

□

Legitimation regarding the data of Mercadona workers.

Furthermore, we have to mean that there is another group affected by establishing facial recognition. We refer to the workers of the merchant, who are also biometrically identified when entering the supermarkets.

Well then, the processing of the biometric data of the employees of Mercadona through a facial recognition system like the one analyzed It is also not covered by the exception of art. 9.2.f) of the GDPR.

The art. 20.3 of the Workers' Statute and the exceptions of art. 9.2.f) and 9.2.h) of the RGPD do not support the legitimacy of the treatment for the purpose intended, which is to make effective a security measure derived from a legal proceedings between Mercadona and a person who has stolen products or damage to its facilities (Mercadona does not hold the legitimacy to defend aggressions and personal and property damages suffered by their employees, which corresponds to the latter).

It is fully applicable to Mercadona employees, what we have indicated in the previous section on the use of the legal basis of art. 6.1.e) of the GDPR. This legal basis, without complying with the exception of art. 9.2.f), it is not possible to legitimize the processing of biometric data of employees

of Mercadona.

We have to mean that the group of supermarket workers has not

been considered by the data controller when assessing and choosing

treatment consisting of a facial recognition system that respects and

weigh the risks in the violation of rights and freedoms of this group.

This can be verified from the examination of the administrative file, since,

in the EIPD, the categories of interested parties are “Subjects who access the

MERCADONA centers; Subjects with final conviction”, page 6.

You may also notice that the DPIA examines the threat of

that “A treatment is carried out that implies a systematic monitoring of the

holders without them being aware of the activity and/or scope of the

same […] The facial recognition system can systematically assess

(although always with human intervention) the images of the people who

access MERCADONA centers”, page 16.

Employees do not appear as differentiated subjects, they are not taken into account

as a specific group affected by their own risks. However, they are

being detected by the facial recognition system every time they enter and

they go out the door of the supermarket, either to go to work or in the

performance of their duties.

Of course, employees cannot be included among the "subjects that access the MERCADONA centers"; the latter are all potential clients and it is obvious because their risks, together with the eventual risks to the sentenced person, are the only ones that are examined throughout the EIPD. Nope the specific and singular risks of the workers are examined. In this sense, it should be noted that the DPIA provided is incorrect. In this sense, it brings up the provisions of opinion WP248 on impact assessment of WG29: "…Under the GDPR, non-compliance with the requirements of the DPIA may lead to the imposition of fines by the supervisory authority competent. Failure to carry out an DPIA when the treatment requires a evaluation of this type (article 35, paragraphs 1, 3 and 4), carry out an DPIA incorrectly (article 35, sections 2, 7, 8 and 9) or not consulting the competent supervisory authority when necessary [article 36, paragraph 3, letter e)] may lead to an administrative fine of up to EUR 10 million or, in the case of a company, an amount equivalent to a maximum of 2% of the global total annual turnover of the previous financial year, opting for for the highest amount…)".

Thus, Opinion 2/2017 on the processing of data in the work of the GT29 (adopted June 8, 2017) states that "although the use of these technologies can be useful in detecting or preventing property loss intellectual and material of the company, improving the productivity of the workers and protecting the personal data that is in charge of the responsible for the treatment, also poses important challenges in terms of privacy and data protection. Therefore, a new assessment of the balance between the legitimate interest of the employer to protect his company and the reasonable expectation of privacy of the interested parties: the workers".

Therefore, "Regardless of the legal basis for such treatment, before

its beginning, a proportionality test must be carried out in order to

determine if the treatment is necessary to achieve a legitimate purpose, as well as the

measures to be taken to ensure that violations of the

rights to private life and secrecy of communications are limited to

minimum. This may form part of an impact assessment relating to the

data protection (EIPD)”.

In the case examined, no proportionality test has been carried out.

in relation to the risks and the affectation of the rights and freedoms of the

employees. This follows clearly from the undoubted fact that not so

They are not even cited in the EIPD that appears in the administrative file as

a specific group to assess.

As stated by the WG29 in the aforementioned Opinion "The processing of data in

The work must be a proportionate response to the risks to which it is

faces an entrepreneur. In the case examined, it is not proportionate

from the moment that not even the collective has been considered at the

time to determine the risks.

It is unavoidable to consider whether the treatment (of the biometric data of the

employees) is proportionate, what the risks are and consider them in all

case in the EIPD. Opinion 2/2017 on data processing at work

of WG29 highlights the need for its implementation "particularly if it uses new technologies, due to their nature, scope, context or purposes, entail a high risk to the rights and freedoms of natural persons. And this because "The Modern technologies allow workers to be subject to follow-up over time, at workplaces and in their homes, to across many different devices such as smartphones, desktop computers, tablets, vehicles and wearable technology. If the treatment has no limits and is not transparent, there is a high risk that the interest legitimate interest of entrepreneurs in improving efficiency and protecting the company assets becomes an unwarranted and intrusive control.

In any case, the processing of biometric data of the employees of the supermarket supposes an indirect control of these (in the sense that the The purpose of the treatment is aimed at unequivocally identifying the convict). Control at all points.

If you have to comply with the provisions of art. 89 of the LOPDGDD for the purposes of respect the privacy of workers against the use of communication devices video surveillance, much more if we are faced with a differentiated treatment of video surveillance, more invasive, with more specific and greater risks, than involves the use of biometric data. If such precept imposes the measure of prior information to employees and their representatives, you must also proceed in the case examined for the sake of transparency. The information must be supplied, in any case, to the representatives of the workers and the latter by virtue of art. 13 of the GDPR.

In the case of Mercadona, considering the number of workers that have, the representative body will be the Company Committee, given that the art. 63 of the Workers' Statute establishes that "The works council is the representative and collegiate body of all the workers in the company or workplace for the defense of their interests, constituting in each work center whose census is fifty or more workers.

It should be noted, for information purposes, the recent modification of article 64.4.d) of the Workers' Statute Law, approved by Royal Decree Legislative 2/2015, of October 23 (Statute of Workers), which remains worded as follows in accordance with article 13.2.f) of the GDPR:

<<d) Be informed by the company of the parameters, rules and instructions in which the algorithms or artificial intelligence systems that affect making decisions that may affect working conditions, the access and maintenance of employment, including profiling.>>

In addition to the obligations of information and transparency derived from the data protection, employee representatives have the right to be informed and consulted in certain cases provided for by law.

The art. 64 of the Workers' Statute (at the date of the events), on this In particular, it indicates that “The works council shall have the right to be informed and consulted by the employer on those issues that may affect workers, as well as on the situation of the company and the evolution of the employment in the same, in the terms provided in this article.

Information is understood as the transmission of data by the employer to the committee company, so that it has knowledge of a specific issue

and you can proceed to your examination. Consultation means the exchange of
opinions and the opening of a dialogue between the employer and the works council
on a specific issue, including, where appropriate, the issuance of a report
advance by him”.

The same continues, indicating that the works council will also carry out a
of, art. 64.7.a) “1st Surveillance in compliance with the regulations in force in
labor, social security and employment matters, as well as the rest of the
agreements, conditions and uses of the company in force, formulating, where appropriate, the
timely legal actions before the employer and the agencies or courts
authorities”, for which you will need information on the actions
business.

We can connect this last precept with art. 5.1.a) and arts. 12, 13 and 14 of the
GDPR and art. 89 of the LOPDGDD.

In the administrative file there is a communication to the Intercenter Committee of
Mercadona on this particular.

The inter-centre committee is a body
representative of the second level, established by collective agreement and with the
functions provided for in it (art. 63 of the ET) that cannot assume the
functions of the Company Committee, which is the one to which, for the reasons stated,
should be communicated these issues of implementation of a system of
facial recognition. However, according to the allegation presented by the
mercantile, it should be noted that, indeed, in the present case there is
legally assumed the competence of the Company Committee in the Committee
Intercenters.

In any case, the communication made shows that, considering this group by the company as affected by the treatment of facial recognition, however, there is no reference to the risks on the workers' rights in the EIPD. (art 35 RGPD and list of types of data processing that requires protection impact assessment of data). In this sense, as has already been pointed out, the incorrect evaluation of impact is grounds for sanction in accordance with the provisions of the CEPD guideline reference WP248, rev.01, section I in fine.

That control of the facial recognition system in the terms set forth also produces coercive pressure on workers and can lead to an extremely high unacceptable risk that restricts the freedom of employees, personally and professionally. It's a risk to track your activities without evidence of sufficiently justified cause and, above all, that it has not been taken into account in the elaboration of the EIPD.

As well determined by Opinion 2/2017 on the processing of data in the WG29 work, “Systems that allow employers to control who can enter your facilities, and/or certain areas of your facilities, they can also allow the monitoring of the activities of the workers”.

In relation to video surveillance, he continues to point out that “Video surveillance continues to presenting the same issues for worker privacy as before: the ability to continuously record the behavior of the employee".

We must not ignore other risks that are inferred from all of this, since indicating the aforementioned Opinion that “Although these systems exist since years ago, new technologies designed to track the use of time and the presence of workers are becoming widespread, including those that process biometric data and others such as the tracking of mobile devices” and that “Although these systems may constitute a important component of the follow-up carried out by the employer, also pose the risk of providing an invasive level of knowledge and control on the activities of the worker in the workplace.

Thus we run into the highly plausible risk of combining data obtained from the video surveillance and biometric system, that of “following” continued behavior of the worker, although the treatment of facial recognition was not originally established for it.

As the WG29 ends by indicating, "Therefore, businessmen must refrain to use facial recognition technologies. there may be some marginal exceptions to this rule, but such scenarios cannot be used to invoke a general legitimation of the use of this technology”.

Paraphrasing WG29, compliance with a security measure intended to a single specific person cannot be used to invoke legal standing

general use of this technology in the terms set forth, nor with respect to the employees or any other citizen.

For all the above, we can conclude that the treatment as a whole does not has legitimacy to carry it out, for which it violates the provisions of the arts. 9 and 6 of the RGPD, infractions typified in article 83.5.a) of said regulation and considered very serious for prescription purposes in art. 72.1.e) and a), respectively, of the LOPDGDD.

viii

It is necessary to carry out the proportionality judgment before starting any treatment.

In this sense, the Constitutional Court has indicated, for all the Judgment of the Constitutional Court 14/2003, of January 28, that “in order to verify if a restrictive measure of a fundamental right exceeds the judgment of proportionality, it is necessary to verify whether it meets the three requirements or following conditions: if such a measure is likely to achieve the objective proposed (judgment of suitability); if, in addition, it is necessary, in the sense that There is no other more moderate measure to achieve this purpose with equal efficacy (judgment of necessity); and, finally, if it is weighted or balanced, because it derives more benefits or advantages for the interest general than damages on other goods or values in conflict (judgment of proportionality in the strict sense).

And this based on the jurisprudence established by the European Court of Human Rights Humans, that is, overcoming a triple trial, in the sense of determining if the interference produced in the holder of the right object of restriction by the measure is the minimum in order to achieve the legitimate aim pursued with it.

The first thing we must indicate is that, regarding the treatment of Mercadona's facial recognition -which affects data processing not only of the condemned, but of all the potential clients and employees-, the judgment of proportionality in a broad sense must be carried out in a timely manner.

Notwithstanding the foregoing, authorized by the judicial body an electronic means generic or a specific one such as facial recognition without indicating the form or way to carry it out (see judgments), it is still necessary to carry out the trial of proportionality before starting treatment to assess which medium is most suitable, if necessary to fulfill the purpose permitted by the sentence and examine the proportionality of the measure.

Second, that the judgment of proportionality when it covers the treatment of biometric data requires especially careful examination and detailed.

The GT29 in its Opinion 3/2012 on the evolution of biometric technologies indicates that “When analyzing the proportionality of a proposed biometric system, It is necessary to consider beforehand if the system is necessary to respond to the identified need, that is, whether it is essential to satisfy that need, and not just the most suitable or profitable. A second factor that must be taken into account account is the probability that the system will be effective in responding to the need in question in light of the specific characteristics of the technology biometric to be used. A third aspect to ponder is whether the loss of resulting intimacy is proportional to the expected benefits. If the benefit is relatively minor, such as increased comfort or slight savings, then the loss of intimacy is not appropriate. The fourth aspect to evaluate adequacy of a biometric system is to consider whether a means less invasion of privacy would achieve the desired end.

Third, and now entering the examination of the proportionality trial, with respect to suitability, yes the facial recognition system may be suitable for comply with the restraining order with respect to the sentenced person, but it is not necessary, since there are less intrusive alternative measures, nor is it strictly proportional, to the extent that more benefits are derived for the interest public than damages on other assets or values in conflict, taking into account account that its massive and indiscriminate application is intended for all potential clients, regardless of the level of risk they represent and becoming the exception of the possibility of processing biometric data in the general rule, contrary to what is intended by the RGPD.

In this way, in the aforementioned judgments it is considered that the security measure requested by the company, it is possible to apply it without rule on the guarantees on the rights and freedoms of affected that should be associated with its implementation, nor does it justify the application of none of the exemptions of art. 9.2 of the GDPR. Now, of course, the judicial body does not express itself regarding the restriction of rights neither for the condemned nor for the rest of the citizens with the implementation of the generalized facial recognition system, since it exceeds the scope of its competence. And in this sense it has already been pointed out, and it will be insisted later, that said treatment is prohibited in application of art. 9.1 of the GDPR.

Let us take as an example the aforementioned Sentence of Santander in which it is indicated that “It is also requested that the establishment be authorized to control this measured through the electronic means available to the entity Mercadona in order to facial recognition, in accordance with art. 58.4 CP, which provides: “The judge or court may agree that the control of these measures be carried out through those electronic means that allow it”. There is not absolutely no inconvenience in granting what is requested, since that the affectation to the sphere of rights or interests of the sentenced person is minimum, being only a means or instrument available to the establishment to enforce what has been agreed more effectively”.

Thus, it authorizes, with respect to the sentenced person, the implementation of the security measure valuing the conflicting interests, without even examining the impact on the Mercadona customers and workers (because none of them is a party to the Penal procedure). It can be, therefore, an ideal measure with respect to the condemned, but it is not with respect to the rest of the citizens, specifically customers and workers of Mercadona, who are affected in a way indiscriminate.

For this reason, the facial recognition treatment as a whole, integrating the treatment of biometric data of potential clients and employees of Mercadona is not suitable. Other systems or way of carry it out in a way that does not affect their rights and public freedoms.

Let us remember that even understanding that this treatment of biometric data implemented by Mercadona is the one authorized by the judicial body, it would only be for the purpose of adopting a security measure in relation to the sentenced and, even so, respecting their fundamental rights, except resolution court against.

In any case, there are less invasive means in the rights and freedoms of potential customers and supermarket employees to get the intended purpose; some of which could fall directly on the sentenced (such as and together with the prohibition of going to certain places, impose on the convict a light criminal of permanent location or impose a location system, which would be assessed by the judicial body at the request of the party concerned) without affecting in any way and at any time the rights and freedoms of no one else; others, could be the traditional used to hang the condemned person's photograph in the place -of restricted access and controlled - where ordinary video surveillance images are displayed, or although the photograph of the sentenced person included in an electronic device is compared manually "one-to-one" at the entrance of the establishment.

Fourth, and once the decision to install the system has been made, it must be necessary “in the sense that there is no other more moderate measure for the achievement of such purpose with equal effectiveness.

It should be examined whether to carry out the treatment it is necessary to carry it out a certain pre-established way or if, among all the options available should be chosen the most moderate and with less incidence in the rights and freedoms of the citizens concerned and in accordance with the RGPD and LOPDGDD regulations.

We will start from the concept of need for treatment, which should not be confused with its utility. A facial recognition system can be useful, but does not have to be objectively necessary (the latter being what really must be present). As established by GT29 - Opinion 3/2012 on the evolution of biometric technologies - should be examined "if it is essential to satisfy that need, and not just the most suitable or profitable”.

In this sense, the AEPD, analyzing the need for treatment, concludes that, "Whether it is necessary or not, in the sense that there is no other measure moderate for the attainment of such purpose with equal efficacy by power manually carry out the activity. The term need should not confused with useful but if the treatment is objectively necessary for the purpose” -by all, PS/00052/2020-.

If there is no objective need for the treatment now under analysis, if it is not essential to satisfy that need, the treatment is neither proportional nor lawful. Consequently, it is prohibited.

In the case examined, the facial recognition system can be useful, but not necessary, since not being the only one with which the intended purpose when there are multiple alternatives, it is the only one that can cause devastating interference with the rights and freedoms of citizens. Consequently, it is insisted, it is prohibited.

The SEPD expresses itself in this same sense, in an article on October 28, 2019 entitled “Facial Recognition: A solution in search of a problem?” boarding these types of treatments. Thus, it requires that treatment by facial recognition is "demonstrably necessary", that is, objectively necessary and that there are no other less intrusive alternative means through which the same objective is obtained and expressly states that "the efficiency and convenience are not sufficient justification.

(Retrieved on February 22, 2020 from https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en.)

But it is that, in addition, to greater abundance and, for the purposes merely illustrative, we cannot avoid the fact that the condemned can circumvent easily the facial recognition system with a simple mask -like explained in the note from the AEPD on the "14 misunderstandings in relation to the identification and biometric authentication", with which, it could happen that implemented the system it was not, moreover, neither useful nor effective for the purpose claimed by the supermarket.

Here, the principle of minimum intervention comes into play (art. 5.1.c) and art. 25.1 RGPD), because, in addition, it has to be proven that there is no other measure moderate for the achievement of the intended purpose with equal efficiency, in the framework of the proactive responsibility of the data controller.

Although the court generically authorizes the facial recognition system, does not force you to install it or make it impossible to establish another with which you can

The same purpose can be achieved by other less intrusive systems. this is nothing What would happen if, instead of installing this facial recognition system like the analyzed now, Mercadona opted for another that would allow it to carry out the security measure (e.g. ordinary surveillance system with or without security guard) security, i.e. not remotely “one-on-one”).

Furthermore, the authorization of the judicial body is by no means a carte blanche, nor does it confer an unlimited right to Mercadona, but must comply with the data protection regulations. Especially since the establishment of this facial recognition system may de facto involve the implantation undue security measure for all customers and employees of Mercadona, as it has happened.

In this same sense, Report 36/2020 of the Legal Office of the AEPD, regarding the use of facial recognition techniques in carrying out online evaluation tests, pointed out that “the existence of a public interest does not legitimize any type of personal data processing, but must be, in the first place, to the conditions that may have been established by the legislator, as provided for in article 6 of the RGPD, in its sections 2 and 3, as well as the aforementioned principles of article 5 of the RGPD, especially the purpose limitation and data minimization. And in case they go to be subject to treatment any or some of the personal data included in the special categories of data referred to in article 9.1. of RGPD, that any of the circumstances contemplated in its section 2 to lift the ban on the processing of said data, established with general character in section 1”.

Fourthly, and as regards proportionality in the strict sense, we must to examine how many convictions they have obtained, what is the measure agreed in each of them, regarding how many people, how many supermarkets affect such sentences and if all this is proportional in relation with the number of customers who enter their centers each day and the number of global supermarkets that they have in the Spanish territory.

Thus, we must consider whether the adoption of such a treatment is considered, balanced, deriving from it more benefits or advantages for the general interest than damages to other goods or values in conflict. Against the interest of Mercadona to enforce a restraining order (regarding who has committed a minor crime on its premises), the rights to privacy and data protection of all customers and their employees.

At a glance, it turns out that the treatment is excessive. well to do Effective a security measure for an average of ***NUMBER 3 people per year throughout the territory of the Spanish State -according to their calculations, on an average of ***NUMBER 2 judicial processes- for a limited period and established in sentence -which can be a maximum of six months as it is a minor crime- is

could manage to monitor once implemented in all shopping centers to an average of ***NUMBER 7 customers per year (...). This measure would also affect the group of its workers, numbering more than 100,000 workers.

Mercadona has 1,624 establishments in Spanish territory.

Or, put another way, to control access to Mercadona from a single person will be controlled at an average ***NUMBER 1 potential customers daily per store (which will have to be multiplied by the number of establishments affected by the security measure).

Mercadona alleges that the system has only been installed in ***NO.8 centers, and in consequently the above numbers are incorrect. In this sense, it must note that the aforementioned ***NUMBER 8 establishments refer to "test" mode and the highly plausible intention is its extension to the totality of commercial establishments.

If, in order to adopt a security measure for a citizen, it has to be massively and indiscriminately the personal data of the rest of the citizens, the treatment is clearly disproportionate. Let's add now that we we find the processing of biometric data intended to identify uniquely to a person. A system would be installed in the private sector that is not being used by the State Security Forces and Bodies that pursue the achievement of purposes of general interest.

Regarding the immense amount of data collected, it should be added, in addition, that there is no evidence that adequate technical measures have been taken to avoid a possible transfer of that data to third parties, including third countries outside the EEA. The measure taken is limited to a contractual prohibition of the type agreement between the company and the entity in charge and owner of the applied software (*** COMPANY.2), based on prior authorization from the person in charge, without previous studies that reliably prove the technical impossibility of carry out the aforementioned transfer to third countries given the extremely high (unacceptable) that would lead to a reduction in the rights, guarantees and freedoms of those affected.

We must point out regarding the disproportion of the treatment, which are treated personal data of any person who enters the supermarket, buy or not, including unaccountable minors. Unaccountable minors in no case can they be affected by a conviction.

The company argues that it is not possible to detect the age of people affected, so all the more reason not to carry out this type of treatment. The extremely high risk assumed in treatment is unacceptable.

Also for these reasons there would be a violation of the principle

of data minimization (art. 5.1.c) RGPD).

This can be verified from the simple examination of the administrative file, since

than in the EIPD and about the threat that “Data is processed

inadequate, irrelevant, excessive or unnecessary for the intended purpose”

no mention is made of these data, which are completely excessive,

page 13. They are limited to considering only the data of the convicted person regarding

of the principle of minimization, since they point out that “Only the

data derived from final judgments, in which MERCADONA is a party and

have provided images in the course of the procedure as evidence, which

determine the restraining order becoming effective through the possible

use of new technologies”.

The principle of minimization that is mandatory in all data processing

article 5.1.c) of the RGPD, in view of the documentation sent and

to the description of the treatment carried out, we can consider that the system

of facial recognition implemented by Mercadona in forty (***NO.8)

of its shopping centers processes biometric data aimed at "identifying" a

univocally to a natural person, in a process of searching for

“one-to-many” correspondences subject to the provisions of article 9 of the

RGPD, treatment also called by the doctrine "massive and in a

remote”, in order to differentiate it from other automated facial treatments also comparative "one-to-one" biometrics aimed at "authenticating"

a person with a database (could also be facial images)

automated or with human intervention in each of the checks,

less intrusive features. It is the case of having in a team

electronically the database of images to be compared (undoubted persons) and

manually limited to performing the “one-to-one” comparison to

“authenticate”, what the doctrine calls “massive non-remote” treatment. There is not

doubt that the latter type of treatment would considerably minimize the

risks of violating the rights, guarantees and freedoms of the people who

enter the establishment by limiting themselves to what is necessary and pertinent (principle of

minimization, art. 5.1.c) GDPR).

Consequently, this treatment operation in the terms set forth

violates the provisions of art. 5.1.c) of the RGPD, infringement typified in art.

83.5.a) of said rule, considered very serious for prescription purposes in the

art. 72.1.a) of the LOPDGDD, when treating excessive personal data for the

purpose to which it is directed.

IX

It is necessary to carry out an impact assessment before starting any

high-risk treatment in order to be able to detect, where appropriate, those

unacceptable that would preclude treatment.

In the case analyzed, in addition, an EIPD must be carried out. In this sense

is accurate when “it is likely that processing operations entail a high risk for the rights and freedoms of natural persons.

considering 84 RGPD, "before treatment", considering 90 RGPD, and

will perform under the terms of art. 35 of the GDPR. The intended treatment for

Mercadona is included in the list of types of data processing

that require impact assessment related to data protection (art 35.4). The

EIPD must inherently entail the indicated proportionality judgment.

Before implementing a one-to-many facial recognition system, the

responsible must first assess whether there is another less intrusive system with which

to obtain the same purpose. Section 72 of CEPD Guide 3/2019

“on processing of personal data through video devices”, clarifies in this sense

that “The use of biometric data and in particular facial recognition

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, proportionality and data minimization as set forth in the 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”.

(“The use of biometric data and, in particular, facial recognition

entails greater risks for the rights of the interested parties. It's fundamental

that the use of such technologies takes place respecting the principles of

legality, necessity, proportionality and minimization of the established data

in the GDPR. Considering that the use of these technologies can be perceived

as particularly effective, those responsible should first evaluate

the impact on fundamental rights and freedoms and consider means less intrusive to achieve their legitimate goal of transformation.” The

translation is from the AEPD).

However, Mercadona has requested the adoption of a security measure in

courts consisting of facial recognition processing before

assess the concurrence of risks and the need to carry out an EIPD, which does not

It appears in the administrative file - as evidenced in the fact

that the DPIA is subsequent to the request for such a security measure in a

plurality of criminal procedures. Even when the DPIA is prior to the

execution of the treatment, the adequate understanding of the responsibility

proactive and privacy by design imply valuing from the moment

original of the outline of a treatment of personal data if this can

carried out. Thus, the first moment in which the idea of requesting the

security measure consisting of a facial recognition treatment before

the courts and tribunals, should have been the occasion to assess and detect the risks

on the rights and freedoms of citizens.

It must be added that the risks derived from such automation are high in themselves.

themselves and, in fact, unacceptable as they cannot reduce the initial inherent risk

at adequate levels (residual irrigation) as there is a legal prohibition in accordance with

points out article 9.1 of the RGPD. Such treatment occurs without intervention

as soon as the corresponding system is installed and activated, in such a way

that the person concerned cannot prevent the processing of their data personal in its aspect of the exercise of the right of suppression and opposition, which which may imply a violation of art. 35 of the RGPD, typified in article 83.4.a) of said rule and considered serious for the purposes of prescription in art. 73.t) of the LOPDGDD (in this sense, see GT29 248 already mentioned).

X

In this approach, they ignore and do not consider the possibility that the data of all potential customers entering the supermarket are being treated inappropriate, irrelevant, excessive or unnecessary for the purpose planned. They have not considered for a moment that this is the situation of the unaccountable minors.

Although in principle the personal data of minors is not are especially safeguarded in attention simply to the age of these, it is also true that the legal system protects them especially, because of their particular vulnerability. This protection is specifically deployed in protection of personal data from Convention 108 of the Council of Europe –"specific attention shall be given to the data protection rights of children and other vulnerable individuals"-, going through the RGPD and the LOPDGDD, up to the Organic Law 1/1996, of January 15, on the Legal Protection of Minors, of partial modification of the Civil Code and the Law of Civil Procedure.

The latter establishes in its article 2 that "Every minor has the right to have his or her best interest is valued and considered paramount in all actions and decisions that concern him, both in the public sphere and private", specifying in its art. 4 regarding their right to honor, privacy personal and family and in his own image and in his art. 22 quater regarding the Treatment of personal data.

The art. 28.2 of the LOPDGDD prevents as one of the greatest risks to that the person in charge and the person in charge of the treatment must attend to that the “e) When the data processing of affected groups is carried out in situation of special vulnerability and, in particular, of minors and People with disabilities".

In this sense, we will highlight recital 38 of the GDPR, which establishes that “Children deserve specific protection of their personal data, since may be less aware of the risks, consequences, guarantees and rights concerning the processing of personal data. Said protection Specific information should apply in particular to the use of personal data of children for marketing or personality profiling purposes or user, and the collection of personal data relating to children when used

services offered directly to a child. The consent of the owner of the Parental authority or guardianship should not be necessary in the context of services preventive or advisory services offered directly to children”.

For this reason, the AEPD has clarified in its guides the special recommendations of protection of minors, as is the case with regard to video surveillance in relation to image capture in school settings.

eleventh

In terms of transparency, in relation to the information provided to those interested, there are several aspects to review.

Previously, in the present case, it should be noted that the treatment analyzed does not comply with the GDPR regulations as indicated above,

so it is a prohibited treatment. However, it is analyzed

succinctly the informative signage.

First, regarding the posters, they indicate that it is “to detect

only those people with a restraining order or judicial measure

analogous, in force that may pose a risk to your security.

These sentenced persons generate risk to the assets and facilities of the

supermarket, which is what they have been convicted of. The security risk

of customers is clearly indirect and very tangential. And it would be covered

customer safety by ordinary video surveillance system. There is not

information transparency.

In the administrative file, in the EIPD, it is established in a context -

literally copy- “Facial recognition system to identify agents

outsiders with a current restraining order issued within the framework of a judgment

firm, enabling the use of technological means for its effectiveness,

harmful to MERCADONA employees and centers”, page 4.

In the same way we find it when in the aforementioned document they determine the

purpose of the treatment, which again restrict the security of your

employees and their assets (Mercadona centers): “System of recognition

face to identify external agents with a current restraining order

issued within the framework of a final judgment, making it possible to use

technological means for its effectiveness, harmful to employees and

MERCADONA centers”, page 6 (private interests).

They do not mention the customers of the supermarket chain as potential

"your safety" goals. Surprisingly, they do so on the aforementioned billboard

above and in the information they show their employees for them to give explanations to potential customers.

The information provided is not correct, nor does it fit the purpose (make a security measure), since the system does not start up to protect customers, but Mercadona, as a result of obtaining a judgment favorable to their interests (which contains a penalty for the condemned). In any case, the ordinary security system is enough to guarantee the safety of clients (art. 22.1 of the LOPDGDD). not accurate establish facial recognition system like the one now analyzed for guarantee the safety of customers, because if necessary for such purposes, it would be the one that would ordinarily be established in all types of installations. Without However, this facial recognition system is a security system extraordinary when processing biometric data in order to identify uniquely to a person "one-to-many" and remotely meet included in the special category of personal data (art. 9 of the RGPD).

As we have pointed out before, the information provided on the signage of the supermarkets is the same, without specifically indicating in which of them it is activated the system or if by the simple fact of hanging the poster it is found activated, nor for how long it is activated (duration of the measurement of security), nor is the specific purpose made explicit.

Customers are given the impression that in all supermarkets there is installed the system and permanently. Potential customers are stolen the possibility of not entering the specific supermarket and choosing another in which facial recognition system is installed. It is de facto limiting the right to self-determination, freedom and privacy. The derived risks of this incorrect information are clear, the impairment of their freedoms and Fundamental rights.

The information should indicate whether or not the system is installed. Especially if so As Mercadona states, it will only use the system "in the event that it is part of a judicial proceeding in which, through a final resolution, determine the use of facial recognition to make effective the orders of remoteness".

Second, that in the case of such invasive technologies and, based on the reasoning set forth above regarding minors and other vulnerable groups that deserve special protection, the information provided should be specific to them.

Recital 58 RGPD, on the principle of transparency (information) "…

Since children deserve specific protection, any information and communication whose treatment affects them must be provided in clear language and simple that is easy to understand". And article 12 RGPD states that "The responsible for the treatment will take the appropriate measures to facilitate the interested all information indicated in articles 13 and 14, as well as any communication under articles 15 to 22 and 34 relating to processing, in concise, transparent, intelligible and easily accessible form, with clear language and simple, in particular any information directed specifically at a little boy…".

Although the EIPD indicates that "The use of innovative technologies such as easy recognition poses a risk to the subjects due to the novelty that present the same and the lack of knowledge about their operation. MEASURES; Clear and transparent information about treatment and technology used", page 17, no additional measure is established, specific to transmit the information appropriately to minors and other groups vulnerable. The information provided is the same for everyone.

Third, in terms of transparency and possible transfers international, which assert that they will not occur, the truth is that in the treatment manager contract means that there is the possibility of international transfer in certain cases: "8.2. In case of transfer of personal data to a third country outside the Union Union, a country that does not have an adequate level of protection, or a international organization, the Data Processor must obtain the prior written authorization of the Data Controller and cooperate to guarantee an adequate protection framework under current regulations, through the application of binding corporate rules, the formalization of standard contractual clauses adopted by the European Commission or, in its case, obtaining the authorization of the transfer by the authority competent". They do not inform customers of such a possibility or establish how would report if this scenario finally occurred. Previously it has been pointed out the absence of technical measures to avoid possible transfers improper international

The lack of transparency in the information that prevents those affected from being warned that the implanted treatment is not possible, rather, it is prohibited, constitutes another of the volitional elements of responsibility.

Consequently, the information provided by the company both to the public in general as to the employees violates the provisions of art. 12 of the GDPR to Failure to comply with the requirements cited in arts. 13 of said rule, infraction typified in art 83.5.b) and considered very serious for the purposes of prescription in the art. 72.1.h) of the LOPDGDD.

XII

The foregoing is extensible to the information provided in the "privacy policy", in which it is limited to informing in a generic way -regarding the treatment of facial recognition system or early detection system-, the following:

Data categories: biometric (in those stores in Spain where you are early detection system implemented).

Purpose: “Carry out the necessary actions to protect the interests vital of the clients when it is necessary, or the fulfillment of the judicial resolutions and the measures agreed upon therein”.

Time of maintenance of the data: "In relation to the protection of the vital interest of the people and the execution of the sentences or resolutions that entail restraining orders on work centers and/or people,

Data will be processed and guarded for the time necessary to give compliance with the judicial measures of those persons sentenced to

said restraining order (in those stores in Spain where it is

The early detection system has been implemented.

However, the data collected incidentally to comply with said

purpose will remain on the server only in the process of

check (this check lasts tenths of a second). One time

Once this verification has been carried out, it will proceed to be definitively destroyed (in

those stores in Spain where the detection system is implemented

advance)".

International transfers: "In those cases in which Mercadona

has service providers or suppliers that are outside the

European Union, international transfers made with them are

fully guaranteed in accordance with the standards established by the

Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27

of 2016, and criteria of the Spanish Agency for Data Protection".

Legitimation: "In the case of the treatment of sensitive data

will be processed for reasons of public interest with the consequent

considerations provided by the data protection regulations, which must be

proportional to the objective pursued, which is to enforce the law, respecting the

remaining principles of data protection regulations and establishing the

adequate and specific measures to protect the interests and rights of the

interested, on the basis of the Law of the Union or of the member states

(in those stores in Spain where the detection system is implemented

advance)".

Data communication: "The State Security Forces and Bodies in

under the provisions of the law".

Other data: “In the same way, we inform you that, in order to improve the customer and employee safety, Mercadona, based on the public interest, can process your image or your biometric facial profile to identify subjects with a restraining order 8th analogous judicial measure) in force against Mercadona or against any of its workers (in those stores in Spain where early detection system is in place).

These images will only be processed internally by Mercadona, being exclusively communicated to the Security Forces and Corps for protect the safety of Mercadona's customers and workers and the compliance with the measures decreed judicially (in those stores of Spain where the early detection system is implemented).

Rights: (...) regarding the opposition, "In certain circumstances and for reasons related to your particular situation to the processing of your data, the Interested parties may oppose the processing of their data. Mercadona will stop process the data, except for compelling legitimate reasons, or the exercise or defense of possible claims.

XIII

On the other hand, the risks arising from misidentification of a person who is not prohibited from access by the security measure, bound by form intrinsic to the default design indicated in art. 25.1 of the GDPR.

In these facial recognition systems, a pattern is used to create the facial recognition - the result of an initial treatment of personal data for which which also constitutes personal data prepared and contained within the scope of the right of access that may be exercised, but it is known that "the stored biometric information (e.g. pattern) allows to reconstruct partially the original biometric information (eg face). Bliss partial reconstruction is sometimes fidelity enough for another biometric system recognizes it as the original” -14 misunderstandings in relation to the identification and biometric authentication of the AEPD-. And this links us to the need to implement regular evaluations that allow verifying the relevance and sufficiency of the guarantees granted (section 4 of Guidelines3/2019 on processing of personal data through video devices, of the CEPD).

There are several studies in the framework of facial recognition, both of the type “one-to-one” (biometric data) as well as “one-to-many” (category biometric data) special), which refer to the high error rates in certain own assumptions of the incipient technology and scarce datafication of the applied artificial intelligence systems. In this sense, the great demand of "data" to feed this type of software, makes it necessary to take measures, at least technical, to avoid undue transfers and, in particular, possible international transfers that make possible in the future the identification of the affected party in environments and purposes very different from those initials.

For such purposes, the studies carried out by C.C.C. are important, who puts showed that the high rates of error in the identification of individuals by facial recognition occur when it comes to individuals of color and women (in the latter case, whatever the color of their skin).

In this second assumption, the misunderstandings originate from the minimum amount of images of women that contain the training sets and the test sets (using mostly images of white men).

It also considers that facial recognition does not work well in children and older adults. C.C.C. perceives the existence of what they call the algorithmic bias.

(***URL.1)

***URL.2

In addition, we must bring up the error in the identification that can be produce today due to the pandemic situation that requires us to carry Mandatory masks to all people. The National Institute of United States Standards and Technology (NIST) has conducted since 2002 various independent evaluations of TRF's commercial systems. This is the Face Recognition Vendor Test. One of his evaluations focuses on the massive use of masks, concluding that the error rate in the facial recognition algorithms most used today soars between 5% and 50%.

(Retrieved February 22, 2021 from 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)

Misidentifications also occur in relation to relatives and

brothers, as stated by the AEDP in its note on the "14 misunderstandings with

relation to biometric identification and authentication.

It is true that issues relating to the predictable error rate from the

design is a controversial issue, since the greatest technological development in the

more or less near future will improve the accuracy rate.

(Recovered

https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-

facial-recognition-algorithms)

february

2021

22

of

of

the

of

But, today, it is one more risk that we cannot afford, because the

inaccuracy is predictable from the very moment of designing this type of

information systems when identifying the sentenced person and their confusion with

another person may generate a risk of discrimination and social exclusion

unacceptable. And this in excess of all considerations

put forward about the lack of regulations that legitimize it (prohibited treatment) and guarantees the appropriate level of proportionality with respect to the rights and freedoms for those affected.

The violation of data protection by design violates article 25.1 of the RGPD, typified in article 83.4.a) and considered serious for the purposes of prescription in art. 73.d) of the LOPDGDD.

fourteenth

Regarding the risks derived from the treatment, it must be taken into account that facial recognition is configured as a method involuntary identification through the use of biometric data, as established in the Ethical Guidelines for Trustworthy AI, a document presented at 2019, produced by the High Level Expert Group on Artificial Intelligence under the auspices of the European Commission.

The risks derived from such automatism are very high by themselves, since a person cannot prevent the processing of their personal data, because such processing (the capture and subsequent processing of your biometric data from your face in the case of facial recognition) occurs automatically, without human intervention as soon as the corresponding system is installed and activated.

In fact, in the cited document it is included as one of the first and major concerns the identification and tracking of individuals through artificial intelligence techniques and, as far as what interests us, that “the automatic identification raises serious concerns both from the point of legal and ethical view, since it can have unexpected effects on many psychological and sociocultural levels”; therefore, they differentiate "between the identification of a person versus tracking and tracing, and between a selective or mass surveillance.

They also assert that the application of this type of technology must be clearly justified in existing legislation, which is not the case.

Furthermore, we cannot ignore that the implementation of a system facial recognition such as the one analyzed now collects much more information of the subject than other types of treatment, not being able to be prevented by the affected person, consequence of automation and algorithms applied, since "depending on the biometric data collected, they can derive data from the subject such as their race or gender (including fingerprints fingerprints), their emotional state, diseases, defects and characteristics genetics, substance use, etc. Being implicit, the user cannot prevent the collection of said supplementary information” -Note from the AEPD on the "14 mistakes in relation to biometric identification and authentication"-.

Regarding the risks of social exclusion, discriminatory risks and the principle of accuracy, it should be noted that we can perceive two important risks of

social exclusion derived from a possible malfunction of the system established by the merchant.

In this sense, it is included in the Guidelines 3/2019 on processing of personal data through video devices (Version for public consultation. Adopted on 10 July 2019), that “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's why, date 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".

("In addition to privacy concerns, there are also risks related to possible malfunctions of these devices and the biases that can induce. The researchers report that the software used for the facial identification, recognition or analysis is performed in a different depending on the age, gender and ethnicity of the person who is identifying. The algorithms would be performed on the basis of different demographics, therefore bias in facial recognition threatens to reinforce the prejudices of society. Therefore, those responsible for the treatment of data must also ensure that the processing of biometric data adopted in 5 derived from video surveillance undergoes an evaluation periodic review of the relevance and sufficiency of the guarantees provided". The translation is from the AEPD).

On the one hand, we find ourselves with a long-term risk of discrimination of a criminally convicted person (even after he or she has served conviction and the criminal record is canceled) that continues to be identified as in a situation away from supermarkets.

In the EIPD, all those issues related to the accuracy principle; of the one carried out by the company, there is no evidence that valued and specifically consider these risks indicated previously, which has led to carry out treatment operations

undue undermining the guarantees, rights and freedoms for

affected. To which we must add that it is not contemplated in the EIPD either

provided by the company any impact assessment on minors who

access the premises and their employees, and leaves content empty in the exercise

of certain rights collected in articles 12 and 13 and 15 to 22 of the RGPD.

These deficiencies in the elaboration of the EIPD with the consequences mentioned

must be considered a substantial defect that de facto invalidates the DPIA

done. Consequently, the lack of knowledge of the possible impacts of the

data processing implemented on the freedoms and rights of those affected

and, consequently, the absence of corrective measures that minimize it or, as

is the case, that they invalidate it, supposes a violation of the provisions of article

35 of the RGPD, infringement typified in article 83.4.a) of said regulation and considered

serious for the purposes of prescription in art. 73.t) of the LOPDGDD.

For mere illustrative purposes, we will mean that some companies have

abandoned their businesses and facial recognition programs for

invasions of privacy and clear risks of racial discrimination.

There is also a general risk of using biometric data of

facial recognition by converting all people who enter the

supermarket into possible suspects, subject to biometric surveillance

indiscriminate (it does not discriminate either by group, or by age, or by vulnerability, etc.) which supposes an abuse of the use of biometric data and a clear interference in the fundamental rights and public liberties of citizens. This has been understood by the European Citizens' Initiative (ICE) entitled "Initiative of the civil society for the prohibition of the practices of mass biometric surveillance” (Civil society initiative for a ban on biometric mass surveillance practices) submitted to the European Commission in January 2021.

Regarding the specific risks of vulnerable subjects, the European Agency of Fundamental Rights (European Union Agency for Fundamental Rights, known by its acronym UEFRA) has produced in 2019 a document entitled “Facial recognition technology: fundamental rights considerations in the context of law enforcement”. In it, he examines, in addition to the risks to privacy, protection of personal data and discrimination concerned for a treatment with a facial recognition system, other rights, freedoms and legal rights affected.

It makes specific mention of certain more vulnerable groups, which are minors, the elderly or the disabled.

Regarding minors, it states that “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 individual 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”.

(“Facial recognition systems affect the rights of children of different ways. [...] The best interests of the child must also receive a primary consideration in the context of the use of information technology. facial recognition for law enforcement and border management. [...]

Due to the particular vulnerability of children, the processing of their data biometrics, including facial images, must be subject to proof of identity. necessity and stricter proportionality, compared to adults. [...] Software tests clearly indicate that images of people younger results in considerably more false negatives (misses) in Compared to other age groups, it is most likely due to the rapid growth and change in facial appearance. The translation is from the AEPD).

Therefore, given the special protection that the legal system provides to the childhood, the evaluation regarding the proportionality of data treatment information of minors by biometric systems must be subject to a judgment of necessity proportionality much stricter than the one that would refer to grown ups. This is not reflected in the EIPD carried out by Mercadona. The exam is absolutely general and omits groups at high risk, a circumstance that, had it been taken into account, would have reported a risk result extremely high unacceptable and therefore prohibited.

Regarding the risks to the rights and freedoms of the employees of Mercadona have not even been considered in the EIPD presented.

Previously we mentioned the right to self-determination. attached to same, along with the right to privacy, there is a certain risk of loss of freedom and privacy. Judgment 600/2019 of the First Civil Chamber of the Supreme Court, of November 7, 2019 (Rec. 5187/2017) examined the that the right to privacy implied the establishment of a fictitious chamber; thus, the right not to have to endure a permanent uncertainty in relation to a camera that can or not be activated, real or fictitious. It is true that it refers to a camera oriented to a private estate and not to a public space, but it serves to illustrate the impact it has on privacy. The indubitable fact is that no one behaves the same if it is being recorded or so it thinks; if a fake camera can produce a more than significant impact on privacy, is located in a private or public space, imagine the impact of a camera fully operational and, beyond, the shock of the use of techniques of massive and indiscriminate facial recognition of the “one-to-many” type. The risk is increased by the lack of adequate information on the posters, as as we have stated in previous sections.

Opinion 3/2012 on the evolution of biometric technologies of the GT29 considers that “However, these systems used on a large scale can produce serious side effects. In the case of facial recognition, where biometric data can be easily captured without knowledge of the interested, a wide use could end anonymity in spaces and allow continuous monitoring of people.

It should be added, regarding the risks arising from the exercise of rights,

we can see how in the EIPD presented by the company, page 17, it is

understood as one of the threats to the group of people who

access supermarkets that “No means have been made available

or the interested party has not been informed about their option to oppose the taking of

automated decisions”, explaining that “Although the

information to the subjects of the possibility of exercising their right of

opposition (based on the legitimacy of article 6 of the RGPD), this can

present certain risks.

Subsequently, among the measures to be adopted, they indicate that “based on article

21.1 MERCADONA must stop processing the data unless it proves

compelling legitimate reasons for the treatment that prevail over the

interests, rights and freedoms of the interested party, or for the formulation, the

exercise or defense of claims.

Since the data processing of the facial recognition system is

automatic, massive and remote and the image is captured and treated automatically,

this measure is impossible to carry out (make effective the right of

opposition/deletion) safe from uninstalling the established system in all

supermarkets. If an interested party exercises their right of opposition/deletion and

You have the right to it, your opposition affects the processing of data by the

supermarket from

facial,

regardless of the location of the supermarket to which

access the interested party.

the same uptake

image

the

In the documentation provided by the merchant (doc 7.1 and Doc. 7.2) it is not justified

the denial of the exercised right of opposition, with a generic basis in the

existence of "…a compelling public interest…". Recital 69 of the GDPR

states: "(69) In cases where personal data may be processed

lawfully because the treatment is necessary for the fulfillment of a

mission carried out in the public interest or in the exercise of public powers

conferred on the controller or for reasons of legitimate interests

of the person in charge or of a third party, the interested party must, however, have the right

to object to the processing of any personal data relating to your situation

particular. It must be the person in charge who demonstrates that his legitimate interests

overriding interests or rights and freedoms

fundamental of the interested party". In the same sense, it is indicated in article 21.1 of the

RGPD: "… The controller will stop processing the personal data,

unless it proves compelling legitimate reasons for the treatment that

prevail over the interests, rights and freedoms of the interested party, or

for the formulation, exercise or defense of claims..."

It would be leaving without content and de facto the right of opposition or suppression,

remembering that a limitation to these rights can only be established by

pursuant to legislative provisions of the EU or of the Member States, in which terms of recital 73 and articles 23 and 89 of the RGPD.

fifteenth

In addition, this approach is not unique at European level, since other control authorities follow him.

In this sense, the Control Authority of the Netherlands (Netherlands) issued a formal warning to a supermarket for the use of technology facial recognition.

The system in place, the purpose of its establishment, the issue of its lack of legitimacy in relation to facial recognition processing used by a Dutch supermarket chain is almost identical to the Mercadona course.

Thus, this treatment is implemented to prevent certain people from being able to access supermarkets, in response to a ban issued for this purpose. The supermarket wields that the facial recognition system had been implemented in order to protect its customers and staff and prevent theft in the shops. The cameras were also located at the entrance of stores and, in the same way as Mercadona, proceeds to scan all the people entering the store, comparing it with the database of people with entry ban and, if discarded, deleting the data processed after several seconds.

The vice president of the Control Authority of the Netherlands, has stated that “It is unacceptable that this supermarket, or any other store of the Netherlands, start using facial recognition technology”, stating that the use of this technology is prohibited in almost all cases.

He goes on to explain that “Facial recognition makes us all walk barcodes”, and that “Your face is scanned every time you walk into a store, a stadium or a sports arena that uses this technology. and it's done without your consent. By putting your face through a search engine, there is the possibility that your face could be linked to your name and other data personal. This could be done by matching your face to your social media profile, for instance".

The Netherlands Control Authority also considers that with the implantation of facial recognition cameras we can be monitored continually. And that there is an extremely high (unacceptable) risk of subsequent use of the information that qualifies us as suspicious or interest or profile us.

The aforementioned Control Authority continues to indicate that there are two cases of use allowed to use facial recognition. The first is based on the explicit consent of the client to process their data; not constituting

explicit consent the informative warning to the client of the use of the technology in stores. Entering a supermarket can not be understood how to give consent

In our case examined, Mercadona intends to process the data biometrics of potential customers without asking for their consent, based on One of the exceptions indicated in art. 9.2 of the RGPD that, as we have explained, it is not applicable.

And the second exception is if facial recognition technology is necessary for security purposes, but only insofar as it is in the public interest substantial. The supermarket claims that this is the case. But the said Authority of Control does not consider it so. The vice president of the Control Authority of the Netherlands indicates that the only example in his country is that of security in a nuclear power plant.

(Retrieved on February 19, 2021 from https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en)

For its part, the European Data Protection Supervisor, as we have noted above, published an article on October 28, 2019 titled "Facial Recognition: A solution in search of a problem?" dealing with this kind of treatments.

(Retrieved on February 22, 2020 from https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en)

In said article, it is indicated that "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",

("The purposes that triggered the introduction of facial recognition may seem uncontroversial at first glance: It seems unobjectionable to use it to verify the identity of a person against a presented facial image, and at national borders, including in the EU. It's another level of intrusion use it to determine the identity of an unknown person by comparing your image with an extensive database of images of individuals acquaintances”. The translation is from the AEPD)

That is, it raises more than reasonable doubts due to the intrusion that “using it to determine the identity of an unknown person by comparing their image with an extensive database of images of known people” (one-to-many).

And, he adds, that “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”.

(“any interference with fundamental rights under Article 52 of the Letter must be demonstrably necessary. The bar for this test is it becomes higher the deeper the interference. Is there any evidence still that we need technology for everything? Is there really no other less intrusive means to achieve the same goal? Obviously, the "efficiency" and "convenience" could not be enough. The translation is from the AEPD).

Another issue that we highlight from your article is the reference to respect for principles of data minimization and accuracy, when it mentions that "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"

("Facial recognition technology has never been completely accurate, and this has serious consequences for the people identified falsely, whether as criminals or otherwise. The goal of 'accuracy' implies a logic that leads irresistibly to an endless collection of (sensitive) data to refine an algorithm that is ultimately possible. In fact, there will never be enough data to eliminate bias and risk of false positives or false negatives. The translation is from the AEPD).

XVI

In the present case, it must be concluded that the data processing through facial recognition in the terms that the company has implemented in its supermarkets, does not allow the application of the exemption from article 9.2.f) of the RGPD to the general prohibition imposed by the article 9.1 of said rule. Consequently, from that moment it is not possible to legitimize the treatment based on the legality criteria of article 6 of the GDPR. The implanted treatment is prohibited according to the provided in art. 9.1 of the RGPD, regardless of the measures of security and legal conditions set forth in article 6 of the RGPD.

Notwithstanding the foregoing, it would not be lawful to go directly to the provisions in article 6.1.e) since it cannot be shared that with the measure of implanted identification is protecting the public interest, but rather, the private or particular interests of the company in question, public interest

which in any case should be essential. In the same sense, the legal basis

provided in art. 6.1.b) RGPD is also not valid for employees every time

that it is a treatment outside the video surveillance system. Also,

There is no legal regulation that allows it according to the provisions of article 8 of the

LOPDGDD. It must be insisted that the analyzed treatment is

prohibited from its origin as indicated in article 9.1 of the RGPD

On the other hand, the company does not comply with the right to information

required in article 12 and 13 of the RGPD. In this sense, there is no information

significantly on the logic applied in the recognition treatment

facial applied, nor does it allow those affected to exercise their rights given the

immediacy of treatment. It must be insisted that the analyzed treatment be

is prohibited from origin as indicated in article 9.1 of the RGPD

There is also no evidence that the principle of minimization stated in the

article 5.1.c) of the RGPD. The treatments carried out through

facial recognition technology are extremely risky treatments

high (unacceptable), with a high probability of incidence and severity, which

makes the inherent risk very high and very complicated to reduce

acceptable residual risk, which would allow with high probability that

carry out treatments of various kinds (including those affected by article

9.1 of the RGPD) and with great impact outside of what is strictly necessary. In view of

an “unacceptable” level of risk, the provisions of article 36 must be resorted to of the RGPD, prior consultation, which is not recorded. In addition, it is necessary to take into account the incorrect assessment of the impact on the rights and freedoms of those affected when it does not contemplate all the subjects involved. I know must insist that the analyzed treatment is prohibited from origin as stated in article 9.1 of the RGPD

Furthermore, and notwithstanding that the analyzed treatment is is prohibited from origin as indicated in article 9.1 of the RGPD with independence of the security measures implemented, the treatment analyzed does not have the proper security safeguards from the design, every time the implanted system performs a systematic evaluation and comprehensive personal aspects of natural persons on a large scale of data special category. In fact, it is known that the entity in charge of the logic applied to the treatment undertakes to guarantee a level of security appropriate to the risk, which may include, among others: pseudonymization. In Consequently, the design admits the possibility that the treatment of data is carried out on people identified remotely, massively and indiscriminate.

Finally, and taking into account all of the above, especially the high level of risk of the violation of the rights and freedoms of those affected by the treatment object of analysis, the maintenance of the

precautionary measure imposed as it is a treatment prohibited from its origin

In accordance with what is stated on the article. 9.1 of the GDPR.

seventeenth

The facts analyzed could constitute an infringement, attributable to the

claimed, for infringement:

of art. 9 of the RGPD (treatment of special categories of data),

□

typified in article 83.5.a) of said regulation and considered very serious for the purposes of

prescription in art. 72.1.e) of the LOPDGDD, and may be sanctioned with

a fine of up to €20,000,000 or, in the case of a company, of

an amount equivalent to a maximum of 4% of the total annual turnover

of the previous financial year, opting for the highest amount, of

in accordance with article 83.5.a) of the RGPD.

of art. 6 of the RGPD (legality of treatment), typified in article 83.5.a) of

□

said rule and considered very serious for the purposes of prescription in art. 72.1.a)

of the LOPDGDD, and may be sanctioned with a fine of up to €20,000,000

maximum or, in the case of a company, an amount equivalent to 4%

as a maximum of the overall annual total turnover of the financial year

above, opting for the highest amount, in accordance with article 83.5.a)

of the GDPR.

of arts. 12 and 13 of the RGPD (transparency of the information provided to

□

the different groups affected), typified in article 83.5.b) and considered very

serious for the purposes of prescription in art. 72.1.h) of the LOPDGDD, and may be

sanctioned with a maximum fine of €20,000,000 or, in the case of a

company, of an amount equivalent to a maximum of 4% of the volume of total annual global business of the previous financial year, opting for the

greater amount, in accordance with article 83.5.b) of the RGPD.

of art. 5.1.c) (principle of data minimization) and typified in art.

□

83.5.a) and considered very serious for prescription purposes in art. 72.1.a) of the

LOPDGDD, and may be sanctioned with a maximum fine of €20,000,000

or, in the case of a company, an amount equivalent to 4% maximum

of the global total annual turnover of the previous financial year,

opting for the highest amount, in accordance with article 83.5.a) of the RGPD.

of art. 25.1 of the RGPD (data protection by design) typified in

□

art 83.4.a) and considered serious for prescription purposes in art. 73.d) of the

LOPDGDD, and may be sanctioned with a maximum fine of €10,000,000

or, in the case of a company, an amount equivalent to 2% maximum

of the global total annual turnover of the previous financial year,

opting for the highest amount, in accordance with article 83.4.a) of the RGPD.

of art. 35 of the RGPD (impact assessment), typified in art 83.4.a) and

□

considered serious for prescription purposes in art. 73.t) of the LOPDGDD,

being able to be sanctioned with a fine of €10,000,000 maximum or, in the case of

of a company, of an amount equivalent to a maximum of 2% of the volume of total global annual business of the previous financial year, opting for the greater amount, in accordance with article 83.4.a) of the RGPD.

Likewise, it is considered appropriate to graduate the sanctions to be imposed according to the following criteria as indicated in article 83 of the RGPD:

Art 83.1 of the RGPD. effective, proportional and dissuasive (company size)

"1. Each control authority will guarantee that the imposition of fines administrative actions under this article for violations of this Regulation indicated in sections 4, 5 and 6 are in each individual case effective, proportionate and dissuasive”.

The defendant has a turnover in 2019 (latest audit report published) of more than 25,000 million euros and 90,000 employees, so It is a large company, with 1,636 open stores.

Art 83.2 GDPR.

“a) the nature, seriousness and duration of the offence, taking into account the nature, scope or purpose of the processing operation in question as well as the number of interested parties affected and the level of damages who have suffered"

The data subject to treatment are of a special category and the volume of data treated can exceed ***NUMBER 7 per year of facial recognition, including minors and vulnerable people. The treatment is carried out as remote, massive and indiscriminate.

“b) intentionality or negligence in the infringement”

The development of the early detection system has been promoted by the responsible. There is no evidence that the respondent has chosen to consult prior to the AEPD as indicated in art. 36 of the RGPD, even when the implanted treatment constitutes an extremely high risk unacceptable source for the rights and freedoms of customers and employees

of the merchant.

“d) the degree of responsibility of the person in charge or of the person in charge of the treatment,

taking into account the technical or organizational measures that they have applied in

under articles 25 and 32”

The degree of responsibility is fully attributable to the claimed party and is

that the deficiencies and incompatibilities of the treatment are of decision and

own responsibility, specifically purpose and means.

“g) the categories of personal data affected by the infringement”

From the design of the implemented security system, it is clear that it will carry out a

systematic and exhaustive evaluation of personal aspects of natural persons

large-scale special category data.

“h) the way in which the supervisory authority became aware of the infraction, in

particular if the person in charge or the person in charge notified the infringement and, in such case, in

what measure”

It is known that the AEPD was aware of the treatment now analyzed through

of two claims unrelated to the one claimed.

“k) any other aggravating or mitigating factor applicable to the circumstances of the

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement.”

Article 76 of the LOPDGDD. Sanctions and corrective measures.

"1. The penalties provided for in sections 4, 5 and 6 of article 83 of the

Regulation (EU) 2016/679 will be applied taking into account the criteria of

graduation established in section 2 of the aforementioned article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

may also be taken into account:

As aggravating factors:

a) The continuing nature of the offence.

Coast that the treatment is being carried out from July 1, 2020, until the

05/06/2021.

b) The link between the activity of the offender and the performance of treatments

of personal data.

The defendant is a large company in the general distribution sector with

CNAE code 4711, "Retail trade" sector in establishments not

specialized, and carries out treatment of personal data of clients and

workers as usual.

(…)

f) Affectation of the rights of minors.

It is stated that the data processing implemented affects minors and

vulnerable people accessing establishments.

(…)

3. It will be possible, complementary or alternatively, the adoption, when

appropriate, of the remaining corrective measures referred to in article

58.2 of Regulation (EU) 2016/679.

4. It will be published in the Official State Gazette the information that

identify the offender, the offense committed and the amount of the penalty imposed

when the competent authority is the Spanish Agency for the Protection of

Data, the sanction exceeds one million euros and the offender is a

legal person. When the competent authority to impose the sanction is

a regional authority for data protection, it will be subject to its regulations

app."

As mitigating factors:

Art 83.2) GDPR:

e) There is no record of recidivism or reiteration. This mitigation has been of special

relevance to establish the amount of the pecuniary fine now proposed.

From the foregoing, it is considered proportional, effective and dissuasive to impose the

following administrative fines as stated in art. 58.2.i) of the RGPD that

below is indicated:

For the alleged violation of arts. 6 and 9 of the RGPD, typified in art

□

83.5.a) of said rule and considered very serious for prescription purposes in

the art. 72.1.a) and e), respectively, of the LOPDGDD, administrative fine of

amount €2,000,000.

for the alleged violation of art. 5.1.c) of the RGPD, typified in art

□

83.5.a) of said rule and considered very serious for purposes of prescription in the

art. 72.1.a) of the LOPDGDD, an administrative fine of €500,000.

For the alleged violation of arts. 12.13 of the RGPD, typified in art

□

83.5.b) of said rule and considered very serious for purposes of prescription in the

art. 72.1.h) of the LOPDGDD, an administrative fine of €100,000.

For the alleged violation of art. 25.1 of the RGPD, typified in art

□

83.4.a) of said rule and considered serious for the purposes of prescription in art.

73.d) of the LOPDGDD, administrative fine of €500,000.

For the alleged violation of art. 35 of the RGPD, typified in art 83.4.a)

□

of said rule and considered serious for the purposes of prescription in art. 73.t) of

the LOPDGDD, an administrative fine of €50,000.

eighteenth

The art. 69 of the LOPDGDD, states the following:

“Article 69. Provisional measures and guarantee of rights.

1. During the performance of the preliminary investigation actions or initiated

a procedure for the exercise of sanctioning powers, the Agency

Spanish Data Protection Authority may agree to the measures

provisions necessary and proportionate to safeguard the right

fundamental to data protection and, in particular, those provided for in article

66.1 of Regulation (EU) 2016/679, the precautionary blocking of data and the

immediate obligation to attend to the requested right.

2. In cases where the Spanish Data Protection Agency considers that the continuation of the processing of personal data, their communication or international transfer entail a serious impairment of the right to protection of personal data, may order those responsible or in charge of the treatments the blocking of the data and the cessation of its treatment and, in If these mandates are not complied with, proceed to their immobilization.

3. When it had been submitted to the Spanish Agency for the Protection of Data a claim that referred, among other issues, to the lack of attention in term of the rights established in articles 15 to 22 of the Regulation (EU) 2016/679, the Spanish Data Protection Agency may agree at any time, even prior to the start of the procedure for the exercise of the sanctioning power, by resolution reasoned and prior hearing of the data controller, the obligation to address the right requested, continuing the procedure for the rest of the issues that are the subject of the complaint.

Preamble I of the LOPDGDD says: "The protection of natural persons in relation to the processing of personal data is a fundamental right protected by article 18.4 of the Spanish Constitution. In this way, our Constitution was a pioneer in the recognition of the fundamental right to the protection of personal data when it provided that "the law will limit the use information technology to guarantee the honor and personal and family privacy of citizens and the full exercise of their rights. Thus it echoed the work developed since the end of the 1960s in the Council of

Europe and the few legal provisions adopted in countries of our environment. The Constitutional Court indicated in its Judgment 94/1998, of 4 May, that we are faced with a fundamental right to the protection of data by which the person is guaranteed control over their data, any personal data, and about its use and destination, to avoid traffic illicit of the same or harmful to the dignity and rights of those affected; of In this way, the right to data protection is configured as a faculty of the citizen to oppose certain personal data being used for purposes other than that for which it was obtained. For its part, in the Judgment 292/2000, of November 30, considers it as a right autonomous and independent that consists of a power of disposition and control on the personal data that empowers the person to decide which of those data to provide to a third party, be it the State or an individual, or which may this third party collect, and that also allows the individual to know who owns those personal data and for what, being able to oppose that possession or use. (...). By On the other hand, it is also included in article 8 of the Bill of Rights Fundamentals of the European Union and in article 16.1 of the Treaty of Functioning of the European Union. Previously, at European level, there had been adopted Directive 95/46/EC, the purpose of which was to ensure that the guarantee of the right to the protection of personal data does not suppose an obstacle to the free movement of data within the Union, thus establishing a common space of guarantee of the right that, at the same time, would ensure that in case of international transfer of data, its treatment in the country of destination was protected by appropriate safeguards to those provided for in the own directive.

Article 56 of Law 39/2015, of October 1, on the Procedure Common Administrative of Public Administrations (hereinafter, LPACAP), insofar as it is applicable, states the following:

"1. Initiated the procedure, the competent administrative body to resolve, may adopt, ex officio or at the request of a party and in a reasoned manner, the measures provisional measures it deems appropriate to ensure the effectiveness of the resolution that could fall, if there were sufficient elements of judgment for it, of in accordance with the principles of proportionality, effectiveness and least burden.

2. Before the initiation of the administrative procedure, the competent body to initiate or instruct the procedure, ex officio or at the request of a party, in which cases of urgent urgency and for the provisional protection of the interests involved, may adopt, in a reasoned manner, the provisional measures that are necessary and proportionate. Provisional measures must be confirmed, modified or lifted in the agreement to initiate the procedure, which must be carried out within fifteen days following its adoption, which may be subject to the appropriate appeal.

In any case, these measures will be without effect if the procedure within said term or when the initiation agreement does not contain a express statement about them.

3. In accordance with the provisions of the two previous sections, they may agree

the following provisional measures, under the terms provided in Law 1/2000, of January 7, of Civil Procedure:

a) Temporary suspension of activities.

b) Provision of bonds.

c) Withdrawal or intervention of productive assets or temporary suspension of services for health, hygiene or safety reasons, the temporary closure of the establishment for these or other reasons provided for in the regulations applicable.

d) Preventive seizure of assets, income and fungible things computable in cash by application of certain prices.

e) The deposit, retention or immobilization of personal property.

f) The intervention and deposit of income obtained through an activity that is considered illegal and whose prohibition or cessation is intended.

g) Consignment or constitution of a deposit of the amounts that are claim.

h) The withholding of income on account that must be paid by the Administrations Public.

i) Those other measures that, for the protection of the rights of the interested parties, expressly provided by law, or deemed necessary to ensure the effectiveness of the resolution.

4. Provisional measures may not be adopted that may cause damage to difficult or impossible reparation to the interested parties or that imply a violation of rights protected by law.

5. The provisional measures may be lifted or modified during the

processing of the procedure, ex officio or at the request of a party, by virtue of

supervening circumstances or that could not be taken into account in the

time of its adoption.

In any case, they will be extinguished when the resolution takes effect.

administrative order that puts an end to the corresponding procedure”.

In the treatment of data on facial recognition now analyzed and that

It is known that the claimed was carrying out since July 1, 2020

(until 05/06/2021) in various open centers in Spain (at least

forty), is a treatment of personal data expressly prohibited by the

article 9.1 of the RGPD

It is recorded that on 05/06/2021, the respondent carried out the execution of the

precautionary measure imposed by providing reliable documentation that accredits it,

turning off implanted facial recognition systems and removing the

posters.

The adoption of this provisional measure in the Initiation Agreement and its confirmation

and elevation to definitive in this Resolution Proposal, weighs all

the rights and interests in conflict and does not invalidate the security measure

adopted by the judicial bodies, but only the means of recognition

face to carry it out, without prejudice to the fact that the person responsible for the treatment

may adopt other less intrusive systems to achieve such

purpose.

Consequently, the processing of data based on the recognition

for identification purposes implanted by MERCADONA is is prohibited by the provisions of article 9.1, since there is no

no cause that allows to lift the prohibition among those exposed in the

art. 9.2 of the RGPD, so it is not appropriate to rely on the causes of legality

of art. 6.1 of it. Such prohibition cannot be circumvented by

application of proactive security measures, since the prohibition of

treatment indicated in article 9.1 of the RGPD determines that they are

irrelevant, so they are not analyzed.

In view of the foregoing, the following is issued

MOTION FOR A RESOLUTION

That the Director of the Spanish Data Protection Agency sanction

to MERCADONA S.A., with NIF A46103834, for the infraction of the following

articles and sanctions:

art. 6 and 9 of the RGPD, typified in art. 83.5.a), of said rule, a fine

□

administrative amount of €2,000,000 (two million euros).

art. 12 and 13 of the RGPD, typified in art. 83.5.b), of said regulation, a fine

□

administrative amount of €100,000 (one hundred thousand euros).

art. 5.1.c) of the RGPD, typified in art. 83.5.a), of said rule, a fine

□

administrative amount of €500,000 (five hundred thousand euros).

art. 25.1 of the RGPD, typified in art. 83.4.a), of said rule, a fine

□

administrative amount of €500,000 (five hundred thousand euros).

art. 35 of the RGPD, typified in art. 83.4.a), of said rule, a fine

□

administrative amount of €50,000 (fifty thousand euros).

Confirm the provisional measure imposed on MERCADONA in the Agreement

□

of Home on the temporary suspension of all data processing

related to facial recognition in their establishments as it is

said treatment prohibited in accordance with the provisions of the RGPD and regulations

connected and elevated to final.

Likewise, in accordance with the provisions of article 85.2 of the LPACAP,

You are informed that you may, at any time prior to the resolution of the

present procedure, carry out the voluntary payment of the proposed sanction,

which will mean a reduction of 20% of the amount of the same. With the

application of this reduction, the penalty would be established at €2,520,000

(two million five hundred and twenty thousand euros) and its payment will imply the termination of the

process. The effectiveness of this reduction will be conditioned to the

withdrawal or waiver of any administrative action or appeal

against the penalty.

In case you chose to proceed with the voluntary payment of the amount

specified above, in accordance with the provisions of article 85.2 cited,

You must make it effective by depositing it in the restricted account number ES00

0000 0000 0000 0000 0000 opened in the name of the Spanish Agency for

Data Protection in the banking entity CAIXABANK, S.A., indicating in the concept the reference number of the procedure that appears in the heading of this document and the cause, by voluntary payment, of reduction in the amount of the penalty. Also, you must send proof of admission to the Subdirectorate General for Inspection to proceed to close the proceedings.

By virtue thereof, the foregoing is notified, and the procedure so that within TEN DAYS you can allege as much consider in his defense and present the documents and information that consider pertinent, in accordance with article 89.2 of the LPACAP). >>

SECOND: On July 19, 2021, the claimed party has proceeded to pay the sanction in the amount of €2,520,000 making use of the reduction foreseen in the motion for a resolution transcribed above.

THIRD: The payment made entails the waiver of any action or resource in via against the sanction, in relation to the facts referred to in the resolution proposal.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and as established in art. 47 of the Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights (in hereinafter LOPDGDD), the Director of the AEPD is competent to sanction the offenses committed against said Regulation.

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common to Public Administrations (hereinafter LPACAP), under the rubric

“Termination in sanctioning procedures”, provides the following:

II

"1. Started a sanctioning procedure, if the offender acknowledges his responsibility,

the procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction is solely pecuniary in nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature, but the

inadmissibility of the second, the voluntary payment by the alleged perpetrator, in

any time prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the infringement.

3. In both cases, when the sanction is solely pecuniary in nature, the

competent body to resolve the procedure will apply reductions of, at least,

20% of the amount of the proposed sanction, these being cumulative with each other.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or recourse against the sanction.

The reduction percentage provided for in this section may be increased

regulations."

In accordance with the above, the Director of the AEPD,

RESOLVES:

FIRST: DECLARE the completion of the aforementioned sanctioning procedure

PS/00120/2021 in accordance with the provisions of article 85 of the LPACAP, sanctioning MERCADONA, S.A., with NIF A46103834, for violating the

following items:

□

□

□

□

□

art. 6 and 9 of the RGPD, typified in art. 83.5.a), of said rule,

art. 12 and 13 of the RGPD, typified in art. 83.5.b), of said rule,

art. 5.1.c) of the RGPD, typified in art. 83.5.a), of said rule,

art. 25.1 of the RGPD, typified in art. 83.4.a), of said rule,

art. 35 of the RGPD, typified in art. 83.4.a), of said rule,

□ Prohibit all processing of personal data relating to recognition

face mask in its establishments, in accordance with article 58.2.f).

SECOND: NOTIFY this resolution to MERCADONA, S.A., with NIF

A46103834 and with address at Paseo de la Castellana No. 259 C, 28046 Madrid.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of the Public Administrations, the interested parties may file an appeal

contentious-administrative before the Contentious-administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-Administrative Jurisdiction, within a period of two months from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Sea Spain Marti

Director of the Spanish Data Protection Agency

968-160721

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es