Legal cabinet

N/REF: 0047/2021

The project proposes the processing of facial recognition data in

the moment of registration of clients in the branch or through an online channel with the

objective of verifying your identity and thus carry out the appropriate verifications

provided for in Law 10/2010, of April 28, on the prevention of money laundering

capital and the financing of terrorism (PBC / FT), as well as the control of

fraud.

The project presented is limited to:

-

Note that the legal basis for consent to the

processing of the data, since it is biometric data, that is,

special categories of data, cannot be an adequate legal basis for

depend on customers consenting to these treatments. And why can

considered that a compulsory consent would not be lawful when conditioning the

provision of services to the granting of consent with the consequence

that said consent would not be free.

-

The proposed alternative to consent is that of

consider as a legal basis for the processing of data without consent

the fulfillment of a mission of public interest, such as the prevention of

money laundering and the financing of terrorism. Being limited the

application of this legal basis exclusively for the purposes indicated and not to

commercial or any other purpose other than fraud control or

AML/FT.

I

Regulation (EU) 2016/679, of the European Parliament and of the Council of April 27, 2016 regarding the protection of natural persons in what regarding the processing of personal data and the free circulation of these data and repealing Directive 95/46/EC (General Regulation of data protection, RGPD) defines in its article 4.14 the biometric data as “personal data obtained from a specific technical treatment, relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as facial images or fingerprint data”.

Article 9 of said rule regulates the treatment of categories special data, among which are biometric data,

c. George John 6
28001 Madrid

establishing a general prohibition of its treatment in the following terms:

“The processing of personal data that reveals the racial or ethnic origin, political opinions, religious convictions or philosophical, or union affiliation, and the treatment of genetic data, data biometrics aimed at uniquely identifying a natural person, data relating to health or data relating to sexual life or sexual orientation sex of a natural person.

In relation to the processing of facial recognition data, in our Report 36/2020, analyzing article 9.1 in relation to the

Recital 51 of the RGPD, as well as the Protocol of amendment to the Convention for the Protection of Individuals regarding data processing personnel, approved by the Committee of Ministers in its 128th period of sessions in Elsinore on May 18, 2018 (Convention 108+) we pointed out that

“In order to clarify the interpretative doubts that arise regarding the consideration of biometric data as categories special data can be resorted to the distinction between identification biometrics and biometric verification/authentication that established the Article 29 Group in its Opinion 3/2012 on the evolution of the biometric technologies:

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

Biometric verification/authentication: Verification of a biometric individual by a biometric system is normally the process of comparison between your biometric data (acquired at the time of verification) with a single biometric template stored in a device (i.e., a one-to-one mapping process) to-one).

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

“As far as facial recognition is concerned, by “identification” it is understood that the template of a person's facial image is

compares with many other templates stored in a database

to find out if your image is stored on it. The

"authentication" (or "verification"), on the other hand, usually refers to

searching for matches between two specific templates.

It allows the comparison of two biometric templates that, in principle,

they are supposed to belong to the same person; Thus, the two templates

compared to determine if the person in the two images is the

c. George John 6

28001 Madrid

two

Legal cabinet

same. This procedure is used, for example, in the doors of

automated border control used in border controls

of the airports".

Taking into account the aforementioned distinction, it can be interpreted that,

In accordance with article 4 of the RGPD, the concept of biometric data

would include both assumptions, both identification and

verification/authentication. However, in general, the

biometric data will only be considered as a category

special 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).

However, this Agency considers that this is a question

complex, subject to interpretation, with respect to which no

draw general conclusions, 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,
must, as long as the Committee does not rule on the matter
European Data Protection or the jurisdictional bodies,
adopt, in case of doubt, the most favorable interpretation for the
protection of the rights of those affected."

Consequently, in said report this Agency already highlighted the
difficulty in separating the concepts of identification and authentication, which
requires being to the specific case and the particular techniques used in
relation to the purpose pursued by the treatment, as well as the need
to grant maximum protection to the rights of those affected against the use
of techniques that may be more invasive for your privacy and generate greater
risks to their rights and freedoms.

In the project presented, a data processing
biometrics in order to comply with the duty of identification
established in the regulations on the prevention of money laundering and
financing of terrorism, thus avoiding the possible impersonation of
identity. Therefore, it must be concluded that the recognition process
employee facial involves the processing of biometric data for the purpose of
unambiguously identify a natural person, so it is a treatment of
special categories of data subject to the general rule of prohibition of data
themselves (art. 9.1. RGPD).

This same conclusion was reached by the Agency in the aforementioned report 36/2020,
analyzing a case analogous to the present, in which what was intended was
identification through facial recognition of students who
performed the exams in the online modality, in order to verify their

identity and avoid assumptions of impersonation.

c. George John 6

28001 Madrid

However, article 9.2 of the RGPD regulates exceptions to said

general prohibition by establishing that

“Section 1 will not apply when one of the

following circumstances:

to)

the interested party gave his explicit consent for the

processing of such personal data for one or more of the purposes

specified, except when the Law of the Union or of the States

states that the prohibition referred to in paragraph 1 does not

can be raised by the interested party.

processing is necessary for reasons of interest

essential public, on the basis of the Law of the Union or of the States

members, which must be proportional to the objective pursued, respect in

essential the right to data protection and establish measures

adequate and specific to protect the interests and rights

fundamentals of the interested party;

(…)

g)

In relation to section g), it should be noted that when the treatment is

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

of the law of the Member States, proportional to the objective pursued,

essentially respect the right to data protection and establish

adequate and specific measures to protect the interests and rights

fundamentals of the interested party. It is appropriate, therefore, to analyze whether, in the

present case, the budgets established in article 9.2.g) concur.

to lift the ban on the processing of biometric data.

II

This Agency has had occasion to pronounce itself, on various occasions,

Regarding the requirements established by article 9.2.g) of the RGPD to

be able to protect the processing of personal data based on the

facial recognition, given the proliferation of proposals received in relation to

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 the fundamental rights and freedoms of natural persons.

This concern is shared by the rest of the control authorities since

years ago, as the Working Document on

biometrics, adopted on August 1, 2003 by the Group of 29, or the subsequent

Opinion 3/2012 on the evolution of biometric technologies, adopted on

April 27, 2012, and which has led the community legislator himself

include this data among the special categories of data in the GDPR. From

In this way, its treatment being prohibited in general, any

exception to said prohibition shall be subject to a restrictive interpretation.

In this regard, it should be noted, in addition to the aforementioned report 36/2020, referring to the use of facial recognition techniques in carrying out online assessment tests, report 31/2019 on the incorporation of facial recognition systems in video surveillance services under protection of article 42 of the Private Security Law or Report 97/2020 regarding the Draft Order of the Minister of Economic Affairs and Transformation Digital on non-face-to-face identification methods for the issuance of Qualified electronic certificates. In all these cases it was concluded that there was a legal norm in the Spanish legal system that met the requirements of article 9.2.g) of the RGPD, so that the treatment only could rely on the consent of those affected as long as it was guaranteed that it is free.

Analyzing the requirements of article 9.2.g) in our Report 36/2020 we noted the following:

v

The next question that arises in the consultation is whether the treatment of biometric data by facial recognition systems in online evaluation processes could rely on the existence of a Essential public interest in accordance with article 9.2.g) of the RGPD:

g) the processing is necessary for reasons of public interest essential, on the basis of the Law of the Union or of the States members, which must be proportional to the objective pursued, essentially respect the right to data protection and establish adequate and specific measures to protect the

interests and fundamental rights of the interested party.

As we pointed out earlier, the data processing

personnel necessary for the provision of the public service of

higher education is legitimated, in general, in the existence of

a public interest under the provisions of article 6.1.e) of the

GDPR. However, in the case of special categories of data, the

assumption referred to in letter g) of article 9.2. does not refer only to

the existence of a public interest, as it does in many other

its precepts the RGPD, but it is the only precept of the RGPD that

requires that it be "essential", an adjective that comes to qualify

this 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/EC of the European Parliament and of the Council, of October 24,

1995, relative to the protection of natural persons with regard to the

processing of personal data and the free circulation of these data:

"4. Provided they have adequate guarantees, the States

Members may, for reasons of important public interest, establish

other exceptions, in addition to those provided for in section 2, either

through its national legislation, either by decision of the

control". However, its reading results in a greater rigor in the new

regulation by the RGPD, since the adjective "important" is replaced by

“essential” and it is not allowed that the exception can be established by the

control authorities.

In relation to what should be understood as public interest

essential, 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 can only be carried out if

performs in accordance with the law, serves a legitimate purpose, respects the

essence of fundamental rights and freedoms and it is necessary and

proportionate in a democratic society to achieve an end

legitimate (D.L. against Bulgaria, no. 7472/14, May 19, 2016,

Dragojević v. Croatia, #68955/11, 15 January 2015, Peck

v. United Kingdom, No. 44647/98, January 28, 2003, Leander v.

Sweden, No. 9248/81, March 26, 1987, among others). as pointed out

In the last sentence cited, "the concept of necessity implies that the

interference responds to a pressing social need and, in particular,

that it is proportionate to the legitimate aim pursued”.

Likewise, the doctrine of the Constitutional Court must be taken into account

regarding restrictions on the fundamental right to protection of

data, which it synthesizes in its sentence 292/2000, of November 30, in

the one that after configuring the fundamental right to the protection of

personal data as an autonomous and independent right that

consists of a power of disposition and control over data

personal data that empowers the person to decide which of these data

provide to a third party, be it the State or an individual, or which

this third party 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 regarding the

data protection, this Court has declared that the right to

data protection is not unlimited, and although the Constitution does not

expressly impose specific limits, or refer to the

Public Powers for its determination as it has done with

other fundamental rights, there is no doubt that they must

find them in the remaining fundamental rights and goods

constitutionally protected legal rights, as required by the

principle of unity of the Constitution (SSTC 11/1981, of 8

April, F. 7; 196/1987, of December 11 [RTC 1987, 196], F. 6; Y

regarding art. 18, the STC 110/1984, F. 5). Those limits or

may be direct restrictions on the fundamental right

itself, to which it has been alluded before, or they can be

restrictions on the manner, time or place of exercise of the right

fundamental. In the first case, regulating these limits is a way

development of the fundamental right. In the second, the limits

that are fixed are to the concrete form in which it is possible to exercise the

bundle of faculties that make up the content of the right

in question, constituting a way of regulating its

exercise, what the ordinary legislator can do in accordance with what

provided in art. 53.1 CE. The first observation that must

done, which is no less capital 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

they can cede, of course, before goods, and even interests

constitutionally relevant, provided that the cut that

experiment is necessary to achieve the intended legitimate purpose,

proportionate to achieve it and, in any case, be respectful

with the essential content 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 authorized by the Constitution

to set limits on fundamental rights and, in the case

present, to the fundamental right to data protection, and those

limits cannot be different from those constitutionally

foreseen, which in this case are none other than those derived from the

coexistence of this fundamental right with other rights and

legal goods of constitutional rank, legal empowerment

that allows a Public Power to collect, store, treat, use and,

where appropriate, transferring personal data is only justified if

responds to the protection of other fundamental rights or

constitutionally protected assets. Therefore, if those

Operations with a person's personal data are not

carried out in strict compliance with the rules that regulate it,

violates the right to data protection, since they are imposed

constitutionally illegitimate limits, either to its content or to the

exercise of the bundle of faculties that compose it. as it

will also violate that limiting Law if it regulates the limits of

in such a way as to make the fundamental right impracticable

affected or ineffective the guarantee that the Constitution grants. And so

will be when the Law, which must regulate the limits to the rights

principles with scrupulous respect for their essential content,

is limited to empowering another Public Power to set in each case

the restrictions that may be imposed on the rights

fundamental, whose singular determination and application will be at the

albur of the decisions adopted by that Public Power, who

will be able to decide, in what interests us now, on obtaining,

storage, processing, use and transfer of personal data

in the cases it deems convenient and wielding, even,

interests or assets that are not protected with constitutional status

[...]". (Legal Basis 11)

"On the one hand, because although this Court has declared that the

Constitution does not prevent the State from protecting rights or property

legal rights at the cost of the sacrifice of others equally recognized and,

therefore, that the legislator may impose limitations on the

content of fundamental rights or their exercise,

We have also specified that, in such cases, these

limitations must be justified in the protection of other

constitutional rights or assets (SSTC 104/2000, of 13

April [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 the

arbitrariness proscribed by art. 9.3 EC.

On the other hand, even having a constitutional basis and

the limitations of the right being proportionate

established by a Law (STC 178/1985 [RTC

1985, 178]), they can violate the Constitution if they suffer from

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 as reproduced.

And it should also be pointed out that it would not only harm the principle

of legal certainty (art. 9.3 CE), conceived as certainty about

the applicable law 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 by

At the same time, said Law would be injuring the essential content

of the fundamental right thus restricted, given that the way in

that its limits have been set make it unrecognizable and

make it impossible, in practice, to exercise them (SSTC 11/1981, F. 15;

142/1993, of April 22 [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 material budgets of the

limitation of a fundamental right is likely to generate

an indeterminacy about the cases to which such application applies.

restriction. And by producing this result, beyond all

reasonable interpretation, the Law no longer fulfills its function of

guarantee of the very fundamental right that restricts, since it leaves

c. George John 6

28001 Madrid

Legal cabinet

that instead operate simply the will of the one who has to

enforce it, thus undermining both the effectiveness of the right

as fundamental as legal certainty [...]". (FJ15).

"More specifically, in relation to the fundamental right to

privacy we have emphasized not only the need for

its possible limitations are based on a legal provision

that have constitutional justification and that are proportionate

(SSTC 110/1984, F. 3, and 254/1993, F. 7) but the Law that

restrict this right must accurately state each and every

one of the material budgets of the limiting measure. From

If this is not the case, it is difficult to understand that the judicial decision or the act

administrative authority that applies it are founded on the Law, since

what she has done, abandoning her duties, is

empower other Public Powers so that they are the ones

set the limits to the fundamental right (SSTC 37/1989, of 15

February [RTC 1989, 37], and 49/1999, of April 5 [RTC 1999,

49]).

Similarly, regarding the right to data protection

personal it can be estimated that the constitutional legitimacy of the

restriction of this right 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

any constitutionally protected right or asset concurs. Is

the legislator who must determine when that good or

right that justifies the restriction of the right to protection of

personal data and under what circumstances it can be limited and,

furthermore, it is he who must do it by means of precise rules that

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

consequences. For otherwise the legislator would have moved

to the Administration the performance of a function that only he

competent in terms of fundamental rights by virtue of the

Law reservation of art. 53.1 CE, that 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

third final provision of Organic Law 3/2018, of December 5,

Protection of Personal Data and guarantee of digital rights,

regarding the legitimacy of the collection of personal data relating to

to the political opinions of the people who carry out the parties

politicians within the framework of their electoral activities, a precept that was

declared unconstitutional by Judgment no. 76/2019 of May 22.

Legal cabinet

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

that is subject to the treatment of special categories

of data in the RGPD:

In accordance with section 1 of art. 9 GDPR, it is prohibited to

processing of personal data revealing opinions

policies, in the same way that data processing is

revealing racial or ethnic origin, religious convictions

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

genetic data, biometric data aimed at identifying

unambiguously to a natural person, data related to health or

data relating to the sexual life or sexual orientation of a

Physical person. However, section 2 of the same precept

authorizes the treatment of all these data when it concurs

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

Some of those circumstances have a scope

limited (labour, social, associative, health, judicial, etc.) or

respond to a specific purpose, so that, in themselves,

define the specific treatments that they authorize as

exception to the general rule. Furthermore, the enabling efficacy of

several of the assumptions foreseen there is conditioned to the fact that the

The law of the Union or that of the Member States provides for them and

expressly regulate in their field of competence: this is the case

of the circumstances listed in letters a), b), g), h), i) and j).

Treatment of special categories of personal data

is one of the areas in which expressly the

General Data Protection Regulation has recognized the

Member States "room for manoeuvre" when it comes to

"specify its rules", as its recital 10 qualifies it.

This margin of legislative configuration extends both to

the determination of the enabling causes for the

processing of specially protected personal data

-that is, to the identification of public interest purposes

essential and the appreciation of the proportionality of the

treatment to the end pursued, essentially respecting the

right to data protection - such as the establishment of

"appropriate and specific measures to protect the

interests and fundamental rights of the interested party" [art. 9.2

g) GDPR]. The Regulation therefore contains an obligation

of the Member States to establish such

guarantees, in the event that they enable to process the data

specially protected personnel.

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 thereof, the High Court recalls what was stated in its

c. George John 6

28001 Madrid

judgment 292/2000 in which it was rejected that the identification of the

legitimate purposes of the restriction could be carried out through concepts

generic or vague formulas, considering that the restriction of the right

fundamental to the protection of personal data cannot be based,

by itself, in the generic invocation of an indeterminate "interest

public" :

In the aforementioned STC 292/2000 (RTC 2000, 292), in which

legislative interference in the right to

protection of personal data, we reject that the identification

of the legitimate purposes of the restriction could be carried out through

generic concepts or vague formulas:

"16. [...] Similarly, with respect to the right to protection of

personal data it can be estimated that the constitutional legitimacy of

the restriction of this right cannot be based, by itself,

in 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

any constitutionally protected right or asset concurs. Is

the legislator who must determine when that good or

right that justifies the restriction of the right to protection of

personal data and under what circumstances it can be limited and,

furthermore, it is he who must do it by means of precise rules that

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

consequences. For otherwise the legislator would have moved

to the Administration the performance of a function that only he

competent in terms of fundamental rights by virtue of the

Law reservation of art. 53.1 CE, that is, to clearly establish the

limit and its regulation.

17. In the present case, employment by the LOPD (RCL 2018, 1629)

in your art. 24.1 of the expression "control functions and

verification", opens up a space of uncertainty so wide that

provokes a double and perverse consequence. On one side, to

enable the LOPD to the Administration to restrict rights

fundamental principles by invoking such an expression is renouncing

to set the limits itself, empowering the Administration to

do it. And in such a way that, as the Defender of the

Town, allows to redirect to the same practically all

administrative activity, since all administrative activity that

involves establishing a legal relationship with a company, which

This will be the case in practically all cases in which the

Administration needs someone's personal data,

will ordinarily entail the power of the Administration of

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

administrative legal regime of the legal relationship established

with the Administration. What, in view of the reason for restriction

of the right to be informed of art. 5 LOPD, leave in the most

absolute uncertainty to the citizen about in which cases
that circumstance will occur (if not in all) and add to the
inefficiency any jurisdictional protection mechanism that must
prosecute such a case of restriction of rights
without any other complementary criterion that comes in
help of its 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 the basis of the
imposition of limits to the fundamental rights of art. 18.1 and
4 CE, since it contains an even greater degree of uncertainty. Enough
note that all administrative activity, ultimately,
pursues the safeguarding of general interests, whose
achievement constitutes the purpose to which it must serve with
objectivity the Administration in accordance with art. 103.1 CE."

This argument is fully transferable to the present.
prosecution. Likewise, therefore, we must conclude that the
constitutional legitimacy of the restriction of the right
fundamental to the protection of personal data cannot be
based, by itself, on the generic invocation of a

unspecified "public interest". For otherwise the legislator
would have moved the political parties - to whom the provision
challenged authorizes to collect personal data related to the
political views of people within the framework of their
electoral activities - the performance of a function that only
he is responsible for fundamental rights under the
Law reservation of art. 53.1 EC, that is, clearly establish
its limits and regulation.

Nor can we accept, because it is equally imprecise, the purpose
adduced by the State attorney, which refers to the
functioning of the democratic system, since it also contains
a high degree of uncertainty and may involve a
circular reasoning. On the one hand, political parties are
itself "channels necessary for the operation of the system
democratic" (for all, STC 48/2003, of March 12 (RTC
2003, 48), FJ 5); and, on the other hand, the entire operation of the
democratic system ultimately seeks to safeguard
of the purposes, values and constitutional goods, but this does not
manages to identify the reason why the
affected fundamental right.

Finally, it should be specified that it is not necessary to be able to
suspect, with greater or lesser grounds, that the restriction
pursues an unconstitutional purpose, or that the data that is
collect and process will be harmful to the private sphere and the
exercise of the rights of individuals. It is enough with
note that, since it was not possible to identify with sufficient precision

the purpose of the data processing, nor can the

constitutionally legitimate nature of that purpose, nor, in its

case, the proportionality of the planned measure in accordance with

the principles of suitability, necessity and proportionality in

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 right

fundamentally affected resulting from the processing of personal data,

the jurisprudence of this Court requires the legislator that, in addition to

meet the above requirements, also set

adequate guarantees of a technical, organizational and procedural nature, which

prevent risks of varying 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

Let us clarify a doubt that has arisen regarding the scope of our

doctrine of adequate safeguards, which consists of

determine whether adequate safeguards against the use of the

computing must be contained in the law itself that authorizes and

regulates that use or can also be found in other sources

regulations.

The question can only have a constitutional answer. The

Provision of adequate guarantees cannot be deferred to a

time after the legal regulation of data processing

personal in question. Adequate collateral must be

incorporated into the legal regulation of the processing, whether

directly or by express and perfectly delimited reference to

external sources that have the appropriate regulatory status. Only

This understanding is compatible with the double requirement that

stems from art. 53.1 CE (RCL 1978, 2836) for the legislator of

fundamental rights: the reservation of law for regulation

of the exercise of the fundamental rights recognized in the

second chapter of the first title of the Constitution and respect

of the essential content of said fundamental rights.

According to reiterated constitutional doctrine, the reservation of law is not

limits itself to requiring that a law authorizes the restrictive measure of

fundamental rights, but it is also necessary, according to

both to demands called -sometimes- of

normative predetermination and -others- of quality of the law as well as

respect for the essential content of the law, which in this regulation

the legislator, who is primarily obliged to weigh the

conflicting rights or interests, predetermine the assumptions, the

conditions and guarantees in which the adoption of

restrictive measures of fundamental rights. That mandate of predetermination regarding essential elements, linked also ultimately to the judgment of proportionality of the limitation of the fundamental right, cannot be deferred to further legal or regulatory development, nor can it be leave in the hands of the individuals themselves" (FJ 8).

Consequently, the processing of biometric data under the Article 9.2.g) requires that it be provided for in a rule of law European or national, in the latter case having to have said norm, according to the cited constitutional doctrine and the provisions of the Article 9.2 of the LOPDGDD, range of law. This 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 imposition of such limitation foreseeable to the interested party and its consequences, without it being sufficient, for these purposes, the generic invocation of a public interest. And this law must establish, in addition, the adequate guarantees of a technical nature, organizational and procedural, that prevent the risks of different likelihood and severity and mitigate their effects.

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

In other words, in accordance with a long-standing doctrine of this Court, the constitutionality of any restrictive measure of fundamental rights is determined by the 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 if it meets the three following requirements or conditions: if the measure is susceptible to achieve the proposed objective (judgment of suitability); Yes, besides, is necessary, in the sense that there is no other measure moderate for the achievement of such purpose with equal effectiveness (judgment of necessity); and, finally, if it is weighted or balanced, because it derives more benefits or advantages for the general interest that harms 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 28 of March [RTC 1996, 55], FF. 7, 8 and 9; 270/1996, dated 16 December [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).”

c. George John 6

28001 Madrid

Legal cabinet

In the present case, said treatment intends to be covered by the

obligation of identification imposed on obligated subjects by article 3 of Law 10/2010 of April 28, on the prevention of money laundering and the terrorist financing:

Article 3. Formal identification.

1. The regulated entities will identify how many individuals or legal entities intend to establish business relationships or intervene in any operations.

In no case will the obligated subjects maintain relations of business or carry out operations with individuals or legal entities that are not have been properly identified. In particular, it is prohibited opening, hiring or maintenance of accounts, savings books, safe deposit boxes, numbered assets or instruments, encrypted, anonymous or with fictitious names.

2. Prior to the establishment of the relationship of business or the execution of any operations, the subjects obliged will verify the identity of the participants by means of reliable documents. In the event of not being able to verify the identity of the interveners through reliable documents in a first moment, it will be possible to contemplate what is established in article 12, unless there are elements of risk in the operation.

Regulations will establish the documents that must be deemed reliable for identification purposes.

3. In the field of life insurance, verification of the identity of the policyholder must be made prior to the celebration of the contract. Verification of the identity of the beneficiary of the insurance life must be carried out in any case prior to the payment of the

benefit derived from the contract or the exercise of the rights of

redemption, advance or pledge conferred by the policy.

As can be seen, the aforementioned precept establishes an obligation to

identification, also establishing the way in which to proceed to

the same: "through reliable documents", referring to the regulations

regulation in order to determine "the documents that must be considered

irrefutable".

In this regard, Royal Decree 304/2014, of May 5, which

approves the Regulation of Law 10/2010, of April 28, on the prevention of

money laundering and financing of terrorism, determines these

documents in its article 6:

Article 6. Reliable documents for identification purposes

formal.

1. Reliable documents will be considered, for the purposes of

formal identification, the following:

a) For natural persons of Spanish nationality, the

National identity document.

For natural persons of foreign nationality, the Card of

Residence, the Foreigner Identity Card, the Passport or, in the

case of citizens of the European Union or the Economic Area

European, the document, letter or official personal identity card

issued by the authorities of origin. It will also be a document valid for the identification of foreigners the identity document issued by the Ministry of Foreign Affairs and Cooperation for the personnel of the diplomatic and consular representations of third countries in Spain.

Exceptionally, the obligated subjects may accept other personal identity documents issued by an authority provided that they enjoy adequate guarantees of authenticity and include a photograph of the owner.

b) For legal persons, the public documents that prove their existence and contain their company name, form legal entity, domicile, the identity of its administrators, statutes and tax identification number.

In the case of legal entities of Spanish nationality, it will be admissible, for purposes of formal identification, certification of the Registry Provincial commercial, provided by the client or obtained through consultation telematics.

2. In cases of legal or voluntary representation, the identity of the representative and the person or entity represented, will be documented proof. For these purposes, a copy must be obtained of the reliable document referred to in the preceding paragraph corresponding to both the representative and the person or entity represented, as well as the public document accrediting the powers conferred. Verification by certification of the Provincial Mercantile Registry, provided by the client, or obtained by telematic consultation.

3. The regulated entities will identify and verify through
authentic documents the identity of all the participants of the
entities without legal personality. However, in the event of
entities without legal personality that do not carry out activities
In general, it will suffice to identify and
Verification by reliable documents of the identity of the
person acting on behalf of the entity.
In the case of investment funds, the obligation to
identification and verification of the identity of the participants
will be carried out in accordance with the provisions of article 40.3 of Law 35/2003,
of November 4, Collective Investment Institutions.
In Anglo-Saxon trusts ("trusts") or other instruments
analogous legal entities that, despite lacking legal personality,
can act in economic traffic, the obligated subjects will require
the constitutive document, without prejudice to proceeding to the identification and
verification of the identity of the person acting on behalf of the
beneficiaries or in accordance with the terms of the trust, or
legal instrument. For these purposes, the trustees will communicate their
condition to obligated subjects when, as such, they intend to
establish business relationships or intervene in any
operations. In those cases in which a trustee does not declare

his condition as such and this circumstance is determined by the subject

obliged, the business relationship will be terminated, proceeding to carry out

the special examination referred to in article 17 of Law 10/2010, of

28th of April.

4. The identification documents must be in force

at the time of establishing business relationships or executing

occasional operations. In the case of legal persons, the

validity of the data consigned in the documentation provided must

accredited by a responsible declaration of the client.

On the other hand, article 13 provides for other means of identification, without

detriment of the fact that they must also obtain the corresponding

reliable documents:

Article 12. Business relationships and non-face-to-face operations.

1. The regulated entities may establish business relationships

or execute operations through telephone, electronic or

telematics with clients who are not physically present,

provided that any of the following circumstances occur:

a) The identity of the client is accredited by means of the signature

qualified electronic regulated in Regulation (EU) No. 910/2014 of the

European Parliament and of the Council, of July 23, 2014, regarding the

electronic identification and trust services for

electronic transactions in the internal market and repealing

Directive 1999/93/EC. In this case it will not be necessary to obtain

the copy of the document, although the conservation of the

identification data justifying the validity of the procedure.

b) The first income comes from an account in the same name

open client in an entity domiciled in Spain, in the Union

European or equivalent third countries.

c) are verified

regulations.

the requirements determined

In any case, within a period of one month from the establishment of

the business relationship, the regulated entities must obtain from these

clients a copy of the documents necessary to practice the

due dilegence.

When there are discrepancies between the data provided by

the client and other information accessible or in the possession of the obligated subject,

It will be mandatory to proceed to face-to-face identification.

The regulated entities will adopt additional measures of

due diligence when in the course of the business relationship they appreciate

risks higher than the average risk.

2. The regulated entities will establish policies and procedures

to deal with the specific risks associated with relationships of

non-face-to-face business and operations.

However, the use of these means is conditioned to the possible

risk of the operation, as stated in article 3 of the LPBCFT.

Precisely, risk assessment is a central element in the regulations

on prevention of money laundering and financing of terrorism.

Of the transcribed regulation, which is a transposition of the regulations

community, 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 guarantees and

that derive from the greater risks involved in the treatment of

said data.

Therefore, intending in the project the processing of data

personal information included in the special categories of data referred to

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

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

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

of treatment of said data, established in general in its

section 1, requiring article 9.2. of the LOPDGDD that “The treatment of

data 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 can only be lifted in those

cases in which the affected party gives his express consent, under the
letter a) of article 9.2. of the RGPD, and all other parties must attend
requirements to grant a valid consent that are 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 through a
declaration or a clear affirmative action, the processing of personal data
that concern him”.

III

Although the absence of cause that lifts the prohibition of treatment
of special categories of data determines, by itself, the illegality of the
proposed treatment, it should be noted that there is also no legal basis
to legitimize it 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 concept
indeterminate legal system with a dual function: to provide legitimizing cover for the
action of the Administration and, on the other hand, constitutes one of the forms
to limit administrative powers. In this way, the public interest that,
As Parejo Alfonso points out, it has a clear management role in development
normative (parliamentary or not) of the constitutional order, acts as a criterion
delimiter of the action of the public powers, for which it must, in the first place,
term, be identified by the legislator, in order to identify the scope in which
that the action of the Administration will be developed, subject to the
of legality and to which it corresponds to serve objectively the interests
general (article 103.CE) and, in any case, under the control of the courts, since
that, as recalled by the Judgment of the Constitutional Court of June 11,

1984, “It cannot be ignored that the power attributed by the Constitution to the

State to define the general interest, open and indeterminate concept

c. George John 6

www.aepd.es

28001 Madrid

19

called to be applied to the respective subjects, can be controlled, compared to

to possible abuses and a posteriori, by this Court…”.

Legal cabinet

In the first place, it must be assumed that the existence of an interest

public, which undoubtedly exists in the field of money laundering prevention

capital and the financing of terrorism, does not legitimize any type of

treatment of personal data, but must be, in the first place, to

the conditions that the legislator may have established, as provided by the

own article 6 of the RGPD, in its sections 2 and 3, and article 8 of the Law

organic 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights (LOPDGDD) that regulates 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:

"one. The processing of personal data can only be considered founded

in compliance with a legal obligation required of the controller, in

the terms provided in article 6.1.c) of the Regulation (EU)

2016/679, when so provided for by a rule of Union Law

European Union or a standard with the force of law, which may determine the

general conditions of the treatment and the types of data object of the treatment

same as well as the transfers that proceed as a result of the

compliance with the legal obligation. This rule may also

impose special conditions on treatment, such as 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 founded

in the fulfillment of a mission carried out in the public interest 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."

Therefore, the public interest requires, in the first place,

specification by the legislator, taking into account all the

interests affected, in order to determine the restrictions that may be

private interests as a result of the presence of such

general interests, which must be done through a regulation with a range of

law.

In the present case, on the basis of public interest, it would not be

application of the legal basis of article 6.1.e) of the RGPD to the extent that

Law 10/2010 does not attribute powers, which are specific to the

Public Administrations, to financial entities as obligated subjects

to compliance with said rule.

On the other hand, from the analysis of the justifications provided by the

promoter of the project, referring to alleged identity theft, not

it can be inferred that they refer specifically to the public interest

pursued by the regulations on the prevention of money laundering and

financing of terrorism, but rather to cases of fraud to the detriment of

the entity itself, responding to a private interest of the same, which does not

would be admissible, as you recall, in another case of application of

facial recognition, Order 72/2021 of the Ninth Section of the Hearing

Provincial of Barcelona of February 15, 2021:

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

enter into the already mentioned trial of proportionality, which according to the

regulations therefore require the expression of the explicit consent of

the interested. If this consent is not explicitly obtained and

not be collected by test methods such as a support

writing, as is the case in this recognition treatment

facial, this must be corrected with the support of another base of

legitimacy strong enough to justify the

necessity of this treatment to obtain the desired ends, such as

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

prevention against robberies, thefts and situations of insecurity for

company workers. This basis of legitimation ensures

Mercadona, through its request, is the "public interest" that is collected

in the same way as exceptional legitimation in the regulations of

personal data protection. However, this creates doubts when

to interpret its validity or lack thereof in this case, by serving

really the implantation of this technology in a greater way to a

of the company, such as guaranteeing the safety of its

facilities."

IV

What Law 10/2010 does establish, for reasons of public interest, are obligations to said obligated subjects, being the legal basis applicable to the same not the one foreseen in letter e) of article 6.1. of the GDPR, but the referred to in letter c), as indicated in the Report of this Agency 195/2017:

"As is known, Law 10/2010 and its Development Regulation, approved by Royal Decree 304/2014, of May 5, impose on the obligated subjects certain due diligence measures. The A clearer enumeration of such measures appears in the article 13.1 of Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for money laundering or the financing of

terrorism, and amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, repealing the Directive 2005/60/EC of the European Parliament and of the Council and Directive 2006/70/CE of the Commission, when it establishes that:

"Customer due diligence measures shall include the following actions:

a) the identification of the client and the verification of his identity on the

based on documents, data or information obtained from reliable sources

and independent;

b) the identification of the beneficial owner and the adoption of reasonable measures

to verify your identity, so that the obliged entity has the

assurance that you know who the beneficial owner is; also, in what

regarding legal persons, trusts, companies, foundations

and similar legal structures, the adoption of reasonable measures to

in order to understand the ownership and control structure of the client;

c) the evaluation and, where appropriate, the obtaining of information on the

purpose and intended nature of the business relationship;

d) the application of continuous monitoring measures of the relationship of

business, in particular by scrutinizing transactions

carried out throughout said relationship, in order to guarantee that

adjust to the knowledge that the obligated entity has of the client and its

business and risk profile, including, where necessary, the origin

of the funds, and the adoption of measures to guarantee that the

documents, data or information available are

updated.

When the obliged entities adopt the measures mentioned in

letters a) and b) of the first paragraph, will also verify that any

person claiming to act on behalf of the client is authorized to do so and

will identify and verify the identity of said person."

The measures are detailed in Chapter II of Law 10/2010 and in the

Chapter II of its Development Regulation, consisting of the same

the obligation to collect information from the clients themselves or from third parties

sources where such information may be available. sayings

obligations are clearly imposed in the

legal text, specifically providing for in certain cases the

obligation to consult available sources, as in the case of

people with public relevance (article 15). Similarly, the

Article 8 of the Law refers to the application by third parties of these

obligations.

Legal cabinet

In this way, the money laundering prevention legislation

imposes on obligated subjects, in a clear, precise and unconditional manner,

a series of legal obligations to obtain information, either

directly from customers, or from third parties when it is expected. It

would imply that the treatment of the data, as well as the transfer of the

same when it refers to obtaining the information of said

sources, and even obtaining data from other entities

belonging to the same Group, would be protected, provided that

is proportional to compliance with legal obligations

imposed, by article 6.1 c) of the General Protection Regulation

of data, which enables the treatment of the same when it is

necessary for the fulfillment of a legal obligation imposed on the

responsible for the treatment."

Therefore, these legal obligations must be fulfilled in the

terms that the law that imposes them establishes that, for the purposes of this

report, refers to the identification by reliable documents, being said

document, for Spanish citizens, the National Document of

Identity, regarding which article 8 of the Organic Law 4/2015, of 30 of

March, of measures for the protection of citizen security establishes,

under the heading "Obligations and rights of the holder of the National Document of

Identity" the following:

"one. Spaniards have the right to be issued the Document

National Identity.

The National Identity Document is a public and official document and

will have the protection granted to them by law. It's the only one

document with sufficient value by itself for accreditation, to all

the effects, identity and personal data of its owner.

2. In the National Identity Document will appear the photograph and the

signature of its owner, as well as the personal data determined

regulations, which will respect the right to privacy of the

person, without in any case being related to race, ethnicity,

religion, beliefs, opinion, ideology, disability, orientation or

sexual identity, or political or union affiliation. The support card

National Identity Document will incorporate security measures

necessary to achieve quality conditions and

inalterability and maximum guarantees to prevent counterfeiting.

3. The National Identity Document allows older Spaniards

of age who enjoy full capacity to act and minors

emancipated the electronic identification of its holder, as well as the signature

electronic documents, in the terms provided in the legislation

specific. Persons with judicially modified capacity may

c. George John 6

28001 Madrid

exercise these powers when expressly requested by the interested party and does not specify, according to the judicial resolution that complements its capacity, representation or assistance of an institution of protection and support to bind or contract.

The certification service provider will proceed to revoke the electronic signature certificate at the request of the Ministry of the Interior, after receive the communication from the person in charge of the Civil Registry of the registration of the judicial resolution that determines the need for complement of the capacity to bind or contract, of the death or the declaration of absence or death of a person."

Therefore, the DNI proves by itself and for all purposes the identity and the personal data of its owner.

In this way, imposing mandatory identification through facial recognition would not comply with the provisions of current regulations, in addition to being disproportionate, as will be analyzed later.

v

Lastly, and without prejudice to the aforementioned, they should respect the other principles of article 5 of the RGPD, especially to the purpose limitation and data minimization.

Especially, in relation to the data minimization principle,

which requires that they be “adequate, relevant and limited to what is necessary in

relation to the purposes for which they are processed” (article 5.1.c) of the RGPD) there is

It should be noted that in a highly banked society, the proposal of the

processing of facial recognition data provided for in the project will involve

large-scale processing of special categories of data subject to a

reinforced guarantee regime. This is so due to the high volume of customers

of the banking entities that operate in Spain, as well as because

this treatment should be generalized to all financial institutions

or other subjects bound by the PBC/FT Law.

In addition, this massive data processing will mostly affect

customers with respect to which the specific measures of

diligence provided for in said rule, by applying it indiscriminately to all

customers or potential customers regardless of the existing risk.

Likewise, it would be ignoring the provisions of article 8 of the

Organic Law 4/2015, which, as we have seen, highlights the reference that the

DNI is the public and official document with sufficient value by itself for the

accreditation of the identity and personal data of its owner, of what is

It follows that not even the State Security Forces and Bodies

have large-scale data-based identifying information

facial recognition biometrics contemplated in the project.

On the other hand, the proposed system would not meet the requirements of

proportionality required by the Constitutional Court, since, although it may considered suitable for the proposed purpose, it is not necessary, less intrusive alternative measures exist, nor is it strictly proportional, to the extent that more benefits are derived for the public interest than damages on other assets or values in conflict, taking into account that intends its massive and indiscriminate application for all customers of the obligated subject, and that in case of generalization it would imply a treatment mass of special categories of data that would reach practically all of the population, regardless of the level of risk it represents from the perspective of the prevention of money laundering and the financing of terrorism, becoming the exception of the possibility of treatment of biometric data in the general rule, contrary to what is intended by the RGPD.

Precisely, the inadmissibility of using these techniques with a widespread, is collected in the aforementioned Order of the Provincial Court of Barcelona:

Having stated what precedes in the preceding paragraphs, this Chamber considers that the measure requested by the entity, commercial, MERCADONA S.A. is in no way proportional, necessary or also suitable. The convicts in this execution, Messrs. Juan Ignacio Esmeralda were banned from accessing 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 the same violate the corresponding prohibition of access to the center nor that they are repeat offenders in said conduct.

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

interested party 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

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 concerns them, but of the rest of the people who

access the aforementioned supermarket"

Legal cabinet

Consequently, the proposal for data processing based on the

facial recognition for identification purposes under the AML/CFT law

is not authorized in accordance with article 9.2.g) of the RGPD, has no basis

of legitimacy under article 6.1 of the same and is contrary to the

principles of necessity, proportionality and minimization.

Being, therefore, an illegal treatment, said illegality cannot

avoided by applying proactive security measures, since the

illegality of the treatment determines that they are irrelevant, so

they are not analyzed.

According to what has been exposed, the Spanish Protection Agency

of Data issues a report unfavorable to the processing of the project

referenced.