Report in relation to the Draft order approving the Catalog of electronic signature and identification systems

The draft order approving the Catalog of identification and electronic signature systems is presented to the Catalan Data Protection Authority.

The draft order is structured in 5 articles, a repealing provision, a final provision and a annex

Having analyzed the Project, which is accompanied by the general report of the disposition and taking into account the current applicable regulations, in accordance with the report of the Legal Counsel, I issue the following report.

Legal foundations

I

(...)

II

The purpose of the draft order is, in accordance with the provisions of article 1, "to approve the catalog of identification and electronic signature systems to carry out the formalities and procedures of the persons interested with the Administration of the Generalitat ".

Article 2 determines the subjective scope of the Order, which applies to the departments of the Administration of the Generalitat of Catalonia, to public bodies and entities under public law linked to or dependent on the Administration of the Generalitat and to consortia attached to the Administration of the Generalitat.

It should be noted that the use of these identification and signature systems in the administrative processing entails the processing, by the subjects subject to the scope of application of the Order, of the personal data of the interested parties who use these systems of 'identification and signature, understanding as personal data, in accordance with article 4.1 of the RGPD, "all information about an identified or identifiable natural person ("the interested party"); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a number, an identification number, location data, an online identifier or one or more elements of identity, shall be considered an identifiable physical person physical, physiological, genetic, psychological, economic, cultural or social of said person".

Article 5.1.a) of the RGPD establishes that the personal data collected must be treated lawfully, loyally and transparently in relation to the interested party. In order for this treatment to be lawful, one of the conditions provided for in article 6.1 RGPD must be met and, in the event that

in the case of special categories of data, the provisions of Article 9 RGPD must also be taken into account.

In general, the processing of personal data by public administrations in the administrative procedure, either face-to-face or by electronic means, can find its legal basis in article 6.1.e) of the RGPD, according to which there is legal authorization for the processing of personal data when "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 person responsible for the treatment".

As can be seen from article 6.3 of the RGPD and expressly included in article 8 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereafter LOPGDD) the treatment of data can only be considered based on the legal basis of article 6.1.e) of the RGPD when this is established by a rule with the rank of law.

A first consequence of this is that the order being analyzed (just like Decree 76/2020, of August 4, of Digital Administration, which it develops) does not constitute an appropriate instrument to enable the existence of new treatments However, this rule can specify the conditions under which treatments are carried out that are already provided for by rules with the rank of law regulating the administrative procedure, as they can be in the case we are dealing with the provisions of articles 9 and 10 of the Law 39/2015, of October 1, of Administrative Procedure
Community of Public Administrations (LPAC).

III

In the statement of reasons for the draft order, it is mentioned that "Decree 76/2020, of August 4, deploys the authority of the administrations to determine their own identification and signature systems, establishing, on the one hand, principles for the creation of new systems, based on the simplicity and ease of use, and on the other hand, the promotion of mechanisms based on biometric elements or on a previous registration (...) "-

Although it does not appear that any of the systems included in the catalog that includes the Annex of the Draft Order is based on "biometric elements", insofar as in accordance with article 3.1.1. and 3.2.1 the recognized systems can be extended to any other non-cryptographic system with prior registration, and that these systems (in accordance with the will expressed in the exposition of motivations for mechanisms based on biometric elements) could involve the processing of biometric data of the interested parties, it is considered appropriate to make considerations regarding the treatment of this data, which must be taken into account
both with regard to the recognition procedure of these systems and the administrations responsible for the treatment of these data of the interested parties.

It should be pointed out that the identification and signature systems may involve the processing of biometric data of the interested parties at the time of provision of the system to the interested party (for example if biometric data is used to identify the interested party for the 'issuance of a certificate or an identification system) but the subsequent use of this mechanism does not entail the processing of this biometric data. There may also be other systems in which the processing of biometric data takes place, in addition to at the time of provision,
every time the data subject uses the identification and signature system (for example a system based on the recognition of the signature on a tablet by dynamic verification with previous registration of the signature or a system based on automated facial recognition).

According to article 4.14 of the RGPD, biometric data are "personal data obtained from a specific technical treatment, relating to the physical, physiological characteristics

or behavioral data of a natural person that allow or confirm the unique identification of said person, such as facial images or fingerprint data;

The RGPD includes biometric data in the category of data that must be subject to special protection. Specifically, article 9.1 of the RGPD establishes that:

> "1. The processing of personal data that reveal ethnic or racial origin, political opinions, religious or philosophical convictions, or trade union affiliation is prohibited, 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 natural person."

Recital 51 of the RGPD specifies that "the treatment of photographs should not be systematically considered treatment of special categories of personal data, because they are only included in the definition of biometric data when the fact of being treated with specific technical means allows the identification or the univocal authentication of a natural person.)".

As we already explained in CNS opinion 21/2020, which can be consulted on the website of this Authority, from the joint reading of these forecasts it is clear that the key element when considering the data relating to the physical, physiological or behavioral characteristics of a natural person as biometric data is that these data are treated with specific technical means in order to uniquely identify or authenticate their identity. When this happens, we are dealing with special categories of personal data.

The prohibition of the processing of special categories of data in Article 9.1 of the RGPD may be the subject of an exception when, in addition to a legal basis provided for in Article 6.1 of the RGPD, there is also some of the exceptions established in article 9.2 of the RGPD, including:

> "(...)
> a) the interested party gives his explicit consent for the treatment of said personal data with 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 section 1 cannot be lifted by the interested party;
> (...)
> g) the treatment 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, essentially respect the right to data protection and establish measures adequate and specific to protect the fundamental interests and rights of the interested party;
>
> (...)"

It can be ruled out at the outset that the treatment of the biometric data of the interested parties for the purpose of identification or signature in the administrative processing can be based on the exception provided for in article 9.2.g) of the RGPD to the extent that it does not seem that the treatment can be based on the existence of an "essential public interest on the basis of the law of the Union or of the Member States" applicable in a general way to any type of procedure, and that, in any case , required the existence of a provision in this respect in the law of the European Union or in a norm with the rank of law.

In the absence of other exceptions to those provided for in article 9.2 RGPD, the consent of the interested parties could be a legitimate basis that enables those responsible for the treatment to use identification and/or electronic signature systems that are based on the use of data biometrics,

provided that this consent meets the requirements established by the data protection regulations.

According to the RGPD, the consent of the interested party is: "any manifestation of free will, specific, informed and unequivocal by which the interested party accepts, (...), the treatment of personal data that concerns him; "(article 4.11 RGPD). In the case of special categories of data, moreover, consent must be explicit.

Recital 42 of the RGPD states that "Consent must not be considered freely given when the interested party does not enjoy true or free choice or cannot refuse or withdraw their consent without suffering any prejudice". And recital 43 adds: "To guarantee that the consent has been given freely, this must not constitute a valid legal basis for the treatment of personal data in a concrete case in which there is a clear imbalance between the interested party and the person responsible of the treatment, in particular when said responsible person is a public authority and it is therefore improbable that consent has been given freely in all the circumstances of said particular situation.". Consequently, given the context of the unequal relationship that occurs between the public administration and citizens, the consent of those interested in the administrative procedure cannot, in general, be considered validly granted.

Only when it is guaranteed that the refusal to give consent does not entail some kind of adverse or discriminatory consequence for the citizen, for example if there are easily accessible alternatives, it could be considered validly granted.

Consequently, in order for the consent of the interested parties for the processing of their biometric data to be considered valid, in the implementation of identification and electronic signature systems that are based on the use of this data, those responsible for the treatment must guarantee that the system is voluntary for the interested party and that they are offered other identification and signature mechanisms for carrying out the procedures that are equally accessible (one of the electronic identification systems provided for in the catalog that is not based on the use of special categories of data) in such a way that the denial of consent does not cause harm or discriminatory situations.

In addition to the principle of legality, any data processing must comply with the other principles established by the RGPD. Among these, the principles of purpose and minimization of data according to which personal data must be collected for specific, explicit and legitimate purposes (Article 5.1.b) RGPD) and must be appropriate, relevant and limited to that necessary in relation to the purposes for which they are treated (article 5.1.c))

As the TC has highlighted in repeated jurisprudence, by all Judgment 39/2016, of March 3, "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 is enough to remember that to check whether a restrictive measure of a fundamental right exceeds the proportionality test, it is necessary to verify whether it meets the following three requirements or conditions: if such a measure is likely to achieve the proposed objective (judgment of suitability); if, in addition, it is necessary, in the sense that there is no other more moderate measure for the achievement of such purpose with equal effectiveness (juicio de necesidad); and, finally, if it is weighted or balanced, more benefits or advantages can be derived from it for the general interest than damages on other goods or values in conflict (proportionality judgment in the strict sense) [SSTC 66/1995, of 8 May, FJ 5; 55/1996, of March 28, FFJJ 6, 7, 8 and 9; 207/1996, of December 16, FJ 4 e), and 37/1998, of February 17, FJ 8]." (FD.5)

The application of the principle of data minimization and the judgment of proportionality that it entails must take into consideration, in each case, the specific procedure in which the system is to be implemented.

Therefore, those responsible for the processing, in this case the administrations subject to the scope of application of the draft order that wish to implement the use of one of the systems recognized in the catalog that involve the processing of biometric data, must analyze its proportionality for each specific procedure in which it is intended to be applied
system, to determine its adequacy to the principle of data minimization.

In this sense, the provision of article 3 of the draft order is positively evaluated according to which:

> "The identification and electronic signature systems to certify the identity of users and signatories by electronic means will be determined depending on the subject and the degree of security of the corresponding procedure."

However, the determination of the identification and signature systems must be carried out depending on the subject and the degree of security required by the corresponding procedure, but in addition, especially in the case that it incorporates special categories of data, the proportionality of the information processed must be taken into account.

For this reason, it is proposed to modify the wording of this article to accommodate this need in such a way that the article would be written as follows:

> "The identification and electronic signature systems to certify the identity of users and signatories by electronic means is determined based on the subject, the degree of security required by the procedure and the result of the proportionality judgment of the system from the point of view of the data protection regulations. "

It should be remembered that, depending on the risks or the concurrence of the requirements provided for in article 35 of the RGPD that may be generated depending on the procedure in question (in this regard, take into account the list of types of data processing that require an impact assessment relating to data protection published by this Authority under Article 35.4 RGPD), it may be necessary to carry out an impact assessment relating to data protection (art. 35 RGPD) and, where applicable, a prior consultation with the Authority (art. 36 RGPD).

On the other hand, the data controller must also take into account, with regard to the collection, storage, treatment and management of biometric data, the obligation to comply with what is established in section 3 of articles 9 and 10 of the LPAC which expressly provides that the technical resources necessary for the collection, storage, processing and management of special categories of data under the terms of the RGPD must be located in Spanish territory, and that they can only be transferred to a third party country or international organization when they have been the subject of an adequacy decision by the European Commission or when compliance with the international obligations assumed by the Kingdom of Spain requires it.

For all this the following are done,

Conclusions

Having examined the Draft order approving the Catalog of identification and electronic signature systems, it is considered adequate to the provisions established in the regulations on personal data protection, as long as the considerations made in this report.

Barcelona, March 3, 2022