CNS 21/2020

Opinion in relation to the consultation of a provincial council on the consideration of certain biometric data as special category data

A letter from a provincial council is presented to the Catalan Data Protection Authority in which it raises whether special category data should be considered:

a) The fingerprint used for biometric verification or authentication in a one-to-one correspondence search system, and not for biometric identification in a one-to-many correspondence search system.

b) The biometric signature obtained on a tablet, measuring the formation of the letters, the direction of the strokes, pressure and other unique dynamic characteristics, registered and admitted without carrying out a verification process by contrast with other signatures.

The Provincial Council states in its consultation that the entity is assessing the use of biometric data.

He points out that Opinion 3/2012 of the Article 29 Working Group, on the evolution of biometric technologies, differentiates the processing of biometric data in identification processes (one-to-many correspondence search) from the processing in processes of verification/authentication (one-to-one correspondence search).

Also that the Spanish Data Protection Agency refers to this differentiation in the report of last May 8 (reference 0036/2020), in which it considers that biometric data would only be considered a special category of data in the cases in which they undergo technical processing aimed at identifying a natural person one by one and not in the case of verifying or authenticating their identity by searching for correspondence
one by one

Having analyzed the request and seen the report of the Legal Counsel, the following is ruled.

I

(...)

II

Article 4.14) of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection Regulation (RGPD), defines biometric data as "personal data obtained from of a specific technical treatment, related 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".

It should be borne in mind that the RGPD includes biometric data in the category of data that must be subject to special protection when regulating the regime applicable to the treatment of this type of data.

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 they are processed by means técnicos específicos allow the unique identification or authentication of a natural person. (...)".

From the joint reading of these provisions, it follows 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 means specific techniques in order to uniquely identify or authenticate their identity. It also seems clear that, when this happens, we will be faced with the processing of personal data that are part of a special category.

Reading Article 4.14 RGPD allows us to conclude, without any doubt, that this special category of data includes both biometric data that allow identification and authentication. The use of the expression "permit or confirm unique identification" is conclusive on this, since the confirmation of identity would be the case of authentication.

However, it is also true that article 9.1 of the RGPD, in prohibiting the processing of biometric data intended to uniquely identify a natural person, does not explicitly refer to authentication, unlike article 4.14) of the GDPR, which, in defining biometric data, refers to both identification and authentication ("allow or confirm unique identification").

This, together with the fact that biometric systems, i.e. systems that extract and process biometric data, have different goals in the case of one-to-many identification and in the case of authentication, could lead to - as pointed out in the query, whether biometric data treated with technical means to authenticate a natural person should really be considered special categories of data.

III

The Article 29 Working Group, in its Opinion 3/2012 on the evolution of biometric technologies, points out, among other issues, that the treatment of biometric data in a biometric system usually consists of different processes , such as the registration of biometric data, biometric storage and biometric correspondence, the latter being understood as "the process of comparing biometric data or templates (captured during registration) with biometric data or templates collected in a new sample for purposes of identification, verification and authentication or categorization."

Biometric identification is defined, that is, the identification of a person by a biometric system as "the process of comparing their biometric data (acquired at the time of identification) with a series of biometric templates stored in a database (that is, a one-to-many correspondence search process).”

And biometric verification or authentication is defined, that is, the verification of a person by a biometric system as "the process of comparing your biometric data (acquired at the time of verification) with a single biometric template stored in a device (that is, a one-to-one correspondence search process).”

However, from this distinction, made at a time when neither one nor the other biometric data was considered a special category of data, the conclusion cannot be drawn that only those whose objective is a special category of data identify from one-to-many correspondence, given that this is clearly opposed to the definition of biometric data contained in Article 4.14) of the RGPD. It could be considered, as it seems to emerge from the query, that despite being biometric data, the use of this data for authentication is not subject to the regime of Article 9 of the RGPD. But the truth is that this possibility must also be ruled out, given that article 9 does not distinguish between one and the other and simply refers to biometric data (and remember that article 4.14 defines what must be understood by biometric data "a effects of this Regulation"). Therefore, the concept given by article 4.14 is for all purposes of this Regulation, that is, when article 9 refers to biometric data, this concept must be understood with the content of the concept provided for in article 4.14.

On the other hand, article 9 only establishes one condition, that is, that the data seek the unequivocal identification of a natural person. And this purpose is fulfilled both in the case of authentication and in the case of the identification of one person among several.

Biometric systems can fulfill two different functions: identifying a person from a set, finally determining who a person is (or at least if there is a match with any of the previously registered persons) and authenticating (or determining that a person really is who says it is). This distinction between the intended objective (if what is intended is to identify or to authenticate) can be said to be relevant with regard to the development of biometric systems, in the understanding that recognition and verification involve using different techniques and that some biometric data might be more appropriate for identification and others for authentication.

In any case, from the data protection aspect, given the ultimate purpose of both cases and the definition contained in article 4.14 of the RGPD, it would not seem pertinent to make this distinction regarding its consideration as to special category of data.

Biometrics, as we have seen, refers to the analysis of a series of distinctive characteristics of each individual, in the sense that they are unique features of each person, non-transferable, unforgettable and that remain unchanged or stable over time .

The inappropriate processing of biometric data, regardless of whether it is for the purposes of identification or authentication, can lead to important, even irreparable, consequences for the rights and fundamental freedoms of the people affected. The most obvious example is that, unlike other identification and authentication systems, once compromised, this data is compromised forever.

A different issue is that, in some cases (for example, a facial recognition system to identify people walking on a public road), the use of biometrics to identify a person from among a set may involve much higher risks by citizens than a system that only aims at authentication (for example, the authentication of a user of a system), but in other cases the risks may be similar.

In any case, it would not seem appropriate to exclude part of the biometric data (those that undergo specific technical treatment in order to verify the identity of a person) from the enhanced protection that the RGPD recognizes for those personal data that , due to their nature and the context in which they are treated, become particularly sensitive, considering the consequences that, for the people affected, may derive from their treatment, which would take place if they were not recognized as special category of data.

It cannot be ignored that identification and authentication, despite responding to different objectives, are concepts closely linked to each other.

Identification aims to determine the identity (recognize) of a person (who are you?) based, in this case, on their physical, physiological or behavioral characteristics. The purpose of authentication is to use this data to confirm or deny the identity of this person (are you who you say you are?) and this action would imply, in any case, having previously identified this person.

When authentication is carried out, for example when a person is identified by fingerprint when entering work, in some cases it leads to a one-to-one identification (for example if a marking card or a code is used in parallel to identify themselves) or it can operate as a one-to-many correspondence system (for example if the fingerprint of the worker who accesses the workplace is compared with that of all the workers in the company to finally determine who the worker is who has accessed).

It must therefore be interpreted that, when the GDPR refers to the unique identification of a natural person in Article 9.1, it is also referring to the authentication of that person's identity (“confirm”).

It is not superfluous to point out that other control authorities in the field of data protection, when they have had the opportunity to examine the implications that biometrics can have for data protection, consider biometric data as a special category of data without distinction .

This would be the case, for example, of the Commission Nationale de l'informatique et des libertés (CNIL) of France, in view of the regulation it makes on the implementation of devices whose purpose is to control access through biometric authentication to facilities, devices and IT applications in the workplace (Délibération n ° 2019-001 of 10 January 2019).

In this regulation, the CNIL mentions the use of biometric data for authentication purposes and states that this type of data is considered sensitive within the meaning of Article 9 of the RGPD (Articles 1 and 5).

This would also be the case with Italy's Garante per la protezione dei dati personali. Both in the Opinion issued by this authority on a bill enabling public administrations to introduce, as a mechanism for controlling working hours, biometric identity verification systems (Web document no. 9051774) , as in the Opinion carried out by this authority

on the draft decree that develops said law (Doc. web no. 9147290), the authority emphasizes the need to justify the proportionality of a measure such as the one proposed, when dealing with biometric data, included in the category of personal data in relations with which greater protection is established.

Also the Information Commissioner's Office (ICO) of the United Kingdom points out, in its Guide on the RGPD (it plans to publish a specific guide on the treatment of biometric data), that biometric data will be special category data in the vast majority of assumptions and warns that, if biometrics is used to, among other purposes, authenticate the identity of an individual, it will be necessary to comply with Article 9 of the RGPD.

All in all, it can be said that biometric data, when subjected to a specific technical treatment in order to uniquely identify (recognize) or authenticate (verify) a natural person, must be considered a special category of personal data and, therefore, that its treatment must be adapted to the specific regime established for this type of data in data protection legislation.

In view of the considerations made so far, and answering the questions raised in the consultation, it could be concluded that:

a) The fingerprint to which a specific technical treatment is applied, when used for the purpose of authenticating the identity of a natural person must be considered as biometric data and, therefore, as a special category data.

b) The biometric signature obtained on a tablet, measuring the formation of the letters, the direction of the strokes, pressure and other unique dynamic characteristics, must also be considered data of a special category, to the extent that it undergoes a technical treatment specific in order to confirm authorship.

This treatment should not be confused with the process of digitizing the traditional handwritten signature. In this case, it cannot be considered a biometric data because, although it seeks to verify the identity of a person, it cannot be said that it is obtained from physical, physiological or behavioral characteristics or, in general, it is subjected to a specific technical treatment for this purpose.

In accordance with the considerations made so far in relation to the query raised, the following are made,

Conclusions

Biometric data subjected to specific technical treatments aimed at biometric recognition purposes, either in the form of biometric identification or biometric authentication, must be considered as a special category of data.

It is, therefore, considered as a special category data, the dactyloscopic print to which a specific technical treatment is applied, when it is used for the purpose of authenticating the identity of a natural person.

Also the biometric signature obtained on a tablet, measuring the formation of the letters, the direction of the strokes, pressure and other unique dynamic characteristics, to the extent that it would undergo a specific technical treatment in order to confirm its authorship.

Barcelona, June 12, 2020