CNS 63/2018

Opinion in relation to the inquiry made by a professional association on the use of control systems based on fingerprints

A letter from a professional association is presented to the Catalan Data Protection Authority in which it is requested that the Authority issue an opinion to assess whether the use of control systems based on fingerprints may constitute a violation of data protection legislation.

Specifically, the inquiry refers to two situations: on the one hand, the use of fingerprinting systems for the purpose of time control of workers; on the other hand, it is also raised in relation to access to certain facilities that the consultation identifies as security facilities of the College (data processing and archive centers).

Having analyzed the query, which is not accompanied by any other documentation, and in accordance with the report of the Legal Counsel, I issue the following opinion:

I

(...)

II

In relation to the first of the issues raised, the installation of an access and time control system based on the collection and processing of an employee's fingerprint pattern entails the processing of their personal data , given that personal data must be understood as "all information about an identified or identifiable natural person ("the interested party")" (art. 4.1 of Regulation 2016/679, of the Parliament and of the Council, of April 27, general protection of data (hereinafter, RGPD)).

With regard to the fingerprint or fingerprint pattern, this is also data that must be qualified as biometric data, given that in accordance with article 4.14 RGPD they have this consideration when they have been "obtained from 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;".

This means that, in accordance with Article 9.1 RGPD, the specific regime provided for the special categories of data provided for both in Article 9 must be applied to data relating to fingerprints. as in other articles of the RGPD.

In this sense, Recital 51 of the RGPD highlights the restrictive nature with which the processing of this data can be admitted:

> **"(51) (...)Such personal data must not be treated, unless its treatment is allowed in specific situations contemplated in this Regulation, given that the Member States may establish specific provisions on data protection with the purpose to adapt the application of the rules of this Regulation to the fulfillment of a legal obligation or to 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. In addition to the specific requirements of that treatment, the general principles and other rules of this Regulation must be applied, especially with regard to the conditions of legality of the treatment. Exceptions to the general prohibition of the treatment of these special categories of personal data must be explicitly established, among other things when the interested party gives his explicit consent or when it comes to specific needs, in particular when the treatment is carried out in the framework of legitimate activities by certain associations or foundations whose objective is to allow the exercise of fundamental freedoms.**
>
> **(52) Likewise, exceptions to the prohibition of processing special categories of personal data must be authorized when established by the Law of the Union or of the Member States and provided that the appropriate guarantees are given, in order to protect personal data and other fundamental rights, when it is in the public interest, in particular the processing of personal data in the field of labor legislation, legislation on social protection, including pensions and security purposes, supervision and health alert, the prevention or control of communicable diseases and others serious threats to health.(...)"**

In accordance with these considerations, the processing of biometric data will require not only the concurrence of one of the legal bases established in article 6 of the RGPD but, in addition, it will have to concur in one of the exceptions provided for in the Article 9.2 of the RGPD.

This Authority has already analysed, in previous opinions (for example, CNS 9/2009, CNS 22/2009 or 22/2011), the adequacy of access and time control systems to the regulations on the protection of personal data of public administration employees using biometric data (such as a fingerprint or a biometric pattern). These opinions, and others, can be consulted on the website www.apd.cat.

In accordance with article 6.2 of Organic Law 15/1999, of December 13, on the protection of personal data (LOPD) and with the principle of data quality (article 4 of the LOPD), applicable by temporary reasons to the cases that were analyzed in those opinions, the Authority considered, in cases similar to the one examined in this opinion, that, to the extent that the collection of personal data of public workers was carried out within a labor or administrative legal relationship and had as its purpose the control, precisely, of its compliance under the provisions of article 20.3 of the Workers' Statute (ET), the person in charge could process and collect the biometric data consisting of the fingerprint or biometric pattern of its workers without requiring their consent.

In this regard, the Judgment of the Supreme Court, of July 2, 2007, was pronounced, seventh basis, emphasizing that the purpose pursued with this system "is fully legitimate: the control of compliance with the working hours to which public employees are obliged . And, as long as that obligation is inherent in the relationship that unites them with the Autonomous Administration, it is not necessary to obtain their consent beforehand since article 6.2 of Organic Law 15/1999 excludes it in these cases. In addition, it does not appear that taking it in the conditions set forth, of an image of the hand, does not comply with the requirements of article 4.1. On the contrary, it can be considered adequate, relevant and not excessive", to which other judgments that judge similar cases are referred, such as the Judgment of the Superior Court of Justice of the Region of Murcia of January 25, 2010 or the Judgment of the National Court of March 4, 2010. In the same sense, the Interlocutory of the Constitutional Court of February 26, 2007 was pointed out, especially with regard to the arguments referred to the doctrine of proportionality.

The approval and full applicability of the RGPD has introduced, however, some additional elements that affect the analysis that can be made of the use of biometric data in the work environment.

III

With the approval of the RGPD, and from the point of view of the legal basis of the treatment, it is not only possible to go to the legal basis provided for in article 6.1.b) of the RGPD (that the treatment is necessary for the execution of a contract to which the interested person is a party), but it is also possible, in the case of subjects to whom it is applicable, to go to the legal basis established in article 6.1.f) (that the treatment is necessary to satisfy the legitimate interest of the employer in the correct execution of the benefits derived from the employment contract), as recognized by Opinion 3/2012 of the Article 29 Working Group, on the evolution of biometric technologies. Either way, the key element will be the determination of the need for treatment. Not because of the need to do some kind of control, but to do it through the proposed technique, that is the use of identification systems based on biometric data.

On the other hand, and as highlighted by recital 51 of the same RGPD, to the extent that biometric data have come to be considered as a special category of data (art. 9.1 RGPD), it will be necessary for one of the exceptions provided for in article 9.2 RGPD to lift the general ban on the processing of these types of data established in article 9.1.

At this point special mention should be made of letter b) of article 9.2 RGPD, according to which the general prohibition of processing biometric data will not apply when "the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the person responsible for the treatment or of the interested party in the field of labor law and security and social protection, to the extent that this is authorized by the Law of the Union of Member States or a collective agreement in accordance with the Law of the Member states that establish adequate guarantees of respect for the fundamental rights and interests of the interested party.

Therefore, in order to apply this exception, two conditions must be met:

a) That the treatment is necessary for the fulfillment of obligations or the exercise of specific rights of the employer or of the interested person in the field of labor law or social security and protection.

b) That it is authorized by the law of the Union or the member states or a collective agreement, which establish adequate guarantees of respect for the fundamental rights and interests of the people affected.

Regarding the possibility that the law of the member states authorizes it, recital 41 of the RGPD provides that "when the present Reglamento makes reference to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament", but adds that this must be understood "without prejudice to the requirements in accordance with the constitutional order of the Member State in question". In the case of the Spanish State, in accordance with the constitutional requirements, the rule that foresees this, as it concerns the development of a fundamental right, must have the status of law (Art

In this sense, article 88 of the RGPD has established that member states can, through legislative provisions or collective agreements, establish more specific rules to guarantee the protection of rights and freedoms in relation to the treatment of personal data of workers in the workplace, in particular, among others, for the purpose of fulfilling the obligations established by law or the collective agreement, the management, planning and organization of work. These rules must include appropriate and specific measures to preserve the human dignity of data subjects, as well as their legitimate interests and fundamental rights, in particular in relation to, among others, supervisory systems in the workplace .

Each member state must notify the Commission of the legal provisions it adopts in accordance with paragraph 1.

In Spanish law, article 20 of the revised text of the Workers' Statute (ET), approved by Royal Legislative Decree 2/2015, of October 23, provides for the possibility that the employer adopts surveillance measures and control to verify the fulfillment of the labor obligations of its workers, but it does not refer at any time to an authorization for the use of special categories of data or, specifically, of biometric data, for this purpose:

"3. The employer may adopt the surveillance and control measures he deems most appropriate to verify the employee's compliance with his obligations and labor duties, keeping in their adoption and application the consideration due to his dignity and taking into account, where appropriate, the real capacity of workers with disabilities."

Articles 87, 89 and 90 of the Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (LOPDGDD), have provided for and regulated the conditions and guarantees with which you can the control of workers by the employer regarding the use of digital devices made available to them by the employer, the use of video surveillance systems in the workplace or the use of geolocation systems in the workplace, but they do not contain any reference to the possibility of using biometric data in control systems in the workplace, as would be the case for time control.

This authorization to implement control systems would be even more necessary in the case of systems based on biometric data, given the special category status of this data, and the imprecise terms with which the current article 20.3 ET is pronounced. The lack of express provision for an authorization in labor law, which is now required by article 9.2.b) of the RGPD means that doubts may arise regarding the admissibility of this type of time control system in the labor field.

On the other hand, and aside from this issue related to the requirement that the use of biometric data be authorized by a rule with the rank of law, it must be taken into account that in any case the treatment must comply with the rest of the principles and obligations derived from data protection regulations, in particular, the principle of minimization (art. 5.1.c) RGPD

This is clear both from the wording of article 9.2.b) of the RGPD, which requires that the treatment be "necessary", and from Recommendation CM/Rec(2015) 5 of the Council of Ministers of the Council of Europe to member states on the processing of personal data in the work context. Specifically, Principle 18 of this Recommendation establishes the following:

> **"18.1. The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if no other less intrusive means are available and only if accompanied by appropriate safeguards foreseen in the beginning 21.**
>
> **18.2. The processing of biometric data must be based on scientifically recognized methods and must be subject to the requirements of strict security and proportionality."**

In this sense, Opinion 3/2012 of the Article 29 Working Group, on the evolution of biometric technologies, stated the following in relation to the analysis of compliance with this principle:

> **"When analyzing the proportionality of a proposed biometric system, it is necessary to consider beforehand if the system is necessary to respond to the identified need, that is, if it is essential to satisfy that need, and not just the most adequate or profitable one. A second factor that must be taken into account is the probability that the system will be effective in responding to the need in question in light of the specific characteristics of the biometric technology that will be used1. A third aspect to consider is whether the resulting loss of privacy is proportional to the expected benefits. If the benefit is relatively minor, such as greater comfort or a slight savings, then the loss of privacy is not appropriate. The fourth aspect to evaluate the adequacy of a biometric system is to consider whether a less invasive means of privacy would reach the desired end."**

The need to admit the installation of time compliance control systems by workers, as this Authority had repeatedly recognized, in accordance with the judicial decisions mentioned above, seems clear. Now, once biometric data have come to be considered as particularly protected data, it does not seem so clear that the use of time control systems based on this type of data should be admitted as a preferred means to carry out the control Rather the opposite. Given the special nature

of this data it seems that it will be necessary to opt first for other control systems that, without using specially protected categories of data, can allow the same purpose to be achieved.

The requirements derived from data protection in design (art. 25.1 RGPD) and, in particular, from the principle of minimization, force you to choose the technology that is least intrusive from the point of view of data protection. The principle of minimization is not only manifested when opting for alternatives that do not involve the processing of personal data, or to carry out data processing in such a way that the minimum indispensable data is used, but also to imply that if a certain purpose can be achieved without having to process data from special categories, this option must prevail over other options that do involve the processing of these types of data.

It should be borne in mind that biometric data, given their personal and unique nature, constitute a reliable means of identification (although there may be a risk of non-identification in certain biometric data). Reliability as an identification system, however, is also conditioned by the extent to which these identification systems can be used. The greater the number of identification systems that are based on biometric data or a template obtained from biometric data, the greater the risk that this data may end up being used inappropriately and leading to a risk of usurpation or impersonation. This risk can be clearly increased depending on the technology used and the treatment given to the raw or original biometric data.

On the one hand, a loss of confidentiality of this data could allow, depending on the technology used, impersonation. However, this data cannot be modified. In other words, unlike a password, in case of loss they cannot be changed.

On the other hand, there are also obvious risks if the technology used does not sufficiently guarantee that the template obtained from the biometric data will not match the one used in other similar systems.

It is undeniable that the use of systems based on biometric data to carry out time control avoids the risk of impersonation that can occur in some cases. However, it does not seem to be the only system that allows to guarantee this. For example, for the purposes of time control, the use of personal cards or other types of objects (token) in a marking system, the use of personal codes, the direct display of the marking point or the use of video surveillance systems where recording the time of entry or exit can constitute, by themselves or in combination with one of the other available systems, effective measures to carry out the control.

By virtue of these considerations, some control authorities in the field of data protection have not allowed the use of control systems based on biometric data as a generalized system of time control of workers by the employer. This would be the case of the Commission Nationale de l'informatique et des libertés (CNIL) of France or the Garante per la protezione dei dati personali of Italy.

In the query formulated, reference is made to the information provided in the AEPD's frequently asked questions section and to a resolution of December 19, 2016 of the Basque Agency Data Protection where the use of a decentralized control system based on

biometric data. It must be said, however, that if reference is made to the approval of the RGPD, in both cases there is a reference to the jurisprudence prior to the RGPD, which had been admitted, as this Authority had also done in the opinions mentioned at the beginning, the use of biometric data for time control systems in the workplace.

Beyond this, the consultation does not set out what are the circumstances that would justify this type of control, nor what reasons would prevent the use of other control systems that do not involve the treatment of special categories of data and that are therefore less intrusive for the right to data protection of the affected persons.

Given these circumstances, it does not seem possible to conclude the proportionality of the use of the fingerprint to establish a time control system in the case described in the consultation.

In any case, prior to the decision on the implementation of a control system of this type, taking into account the technological implications of the technology used, the systematic observation of the habits of the workers and the processing of data 'a special category (biometrics), it would be necessary to carry out an impact assessment relating to the protection of personal data to evaluate both the legitimacy of the treatment and its proportionality, as well as the determination of the existing risks and the measures to mitigate them

IV

The consultation raises yet another assumption, consisting of the use of the fingerprint to control access to certain dependencies that require greater security. Data processing centers or archives are identified as such in the query.

Unlike the previous case, here, if the dependencies in question are accessed, the possible damage that occurs, destruction, alteration, theft or improper access to the information or the information systems contained in these dependencies, will be difficult to repair It would not only be a question of having a record of who accesses these dependencies but also of preventing unauthorized people from accessing them. That being the case, systems such as the installation of video surveillance cameras would not be effective systems, but instead there may be other systems (keys, personal code, token) that can be effective.

As in the previous case, it is essential that the principle of proportionality or minimization of personal data is complied with when determining which control system is applied.

At the outset it seems plausible that the need to apply more robust access control systems for access to certain dependencies that may contain sensitive information may appear more justified than in the case of the purpose of time control. However, it also does not seem that the justification for the measure can be automatically concluded.

In accordance with Opinion 3/2012 of the Article 29 Working Group, on the evolution of biometric technologies, "As a general rule, the use of biometrics for the general security requirements of property and persons cannot be considered a legitimate interest

that prevails over the interests or fundamental rights and freedoms of the interested party. On the contrary, the processing of biometric data can only be justified as a necessary instrument to secure property or people when there is evidence, based on objective and documented circumstances, of the existence of a considerable risk. For this, the person responsible for the treatment must prove that certain circumstances pose a specific considerable risk, which must be evaluated with special care. In order to comply with the principle of proportionality, the person responsible for the treatment, before these high-risk situations, must verify whether possible alternative measures could be equally effective but less intrusive in relation to the objectives pursued, and opt for such alternatives. The existence of the circumstances in question must also be reviewed periodically. On the basis of this review, data processing operations that are not justified must be concluded or suspended."

Therefore, it will be necessary to see, with attention to the nature of the information guarded and the repercussions that improper access to these dependencies could have, what are the risks that must be faced, as well as what are the possible alternatives. Beyond identifying the type of dependencies (processing centers and archives), the consultation does not offer any other information that would allow us to assess the risks or analyze the possible alternatives.

In any case, and for the assumption that, after carrying out the impact assessment to which we referred in the previous legal basis, it can be concluded that the measure is proportionate, in accordance with Opinion 3/2012 of Article 29 Working Group on the evolution of biometric technologies, and without prejudice to the results of the risk analysis carried out, some technical measures should be taken into account in order to minimize the risks:

a) It is advisable to avoid the storage of raw biometric data, and to keep only those templates obtained from that data.
b) The template must be extracted in such a way that it can be foreseen that it cannot be used by other data controllers for similar purposes. c) Preference must be given to decentralized storage systems, avoiding the creation of centralized databases with these types of data. According to the decentralized model that is proposed, the biometric templates would be kept exclusively in the possession of the persons concerned by means of a card or device, so that their loss would have limited effects. d) The data must be kept encrypted.

All this apart from the need to provide transparent information to the affected people about the treatment that is intended to be carried out so that they can understand the scope and consequences that this treatment could have.

In accordance with the considerations made in these legal foundations in relation to the query raised in relation to the use of fingerprint-based control systems, the following are made,

Conclusions

The inclusion of biometric data, including fingerprint data, among the special categories of data provided for by the RGPD does not automatically allow us to conclude that the implementation of a time control system based on the collection of this type of data can be considered proportionate and, therefore, compliant with the minimization principle. An assessment of the impact on data protection must be carried out in view of the specific circumstances in which the treatment is carried out to determine its legitimacy and proportionality, including the analysis of the existence of less alternatives intrusive, and establish approp

In the case of access control to outbuildings or areas that require enhanced security conditions, the use of this type of system may be justified in certain cases, although it is also necessary to carry out a prior evaluation of the impact on data protection.

Barcelona, February 14, 2019