CNS 2/2022

Opinion in relation to the query made by a City Council regarding compliance with data protection regulations for the use of presence control devices in the workplace through facial recognition

A City Council consultation is presented to the Catalan Data Protection Authority in which it states that it intends to install a presence control system in the workplace using facial recognition. The City Council requests to know the compliance with the data protection regulations of the use of these systems, and proposes "[...] what treatment should be given to the facial recognition data necessary for the correct functioning of the application, and what steps should the City Council follow to be able to put it into operation [...]".

Having analyzed the request, which is not accompanied by further information, in view of the current applicable regulations and in accordance with the report of the Legal Counsel, the following is ruled:

I

(...)

II

The City Council states that it intends to install a new presence control device through facial recognition. He explains that the need for this system is due to different reasons: "[...] to follow the health recommendations regarding Covid-19 to prevent possible contagions by replacing the fingerprint control system, and on the other hand, to be able have a tool that collects the data centrally in a central server without the need to go to each work center to collect the data of each worker and then dump the information and be able to do the hourly control individually, which makes it difficult to correctly monitor working days. The fact of having several work centers spread over different buildings [...] means that in the case of using a personal and non-transferable card, there is no way to check that it is used in an appropriate and unique way as it should to be able to (make) a good follow-up".

The City Council considers that the facial recognition system "[...] is a reliable accreditation system for the presence of staff at their workplace, on the days and hours that pertain to their work calendar, and fully satisfies the needs of the municipal entity in this regard."

In relation to the characteristics of this system, and its implementation, the City Council informs that a terminal will be installed in each work center, which will send all the recorded information to a central server, where it will be stored in a database, in text format, for a time which is not defined in the query. The information that will be recorded on these devices will be related to the workers and officials, including a reference image of them for facial reading, as well as the data related to the days. Regarding access to this information, the City Council states that it will be restricted.

The City Council also refers to the fact that the installation company has informed it of the need to request, in writing, all the labor and civil servants of the local body to agree to the transfer of the image exclusively for the purpose of being able to do the time control.

III

Regulation (EU) 2016/679 of the Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data and by which repeals Directive 95/46/CE (General Data Protection Regulation), hereinafter RGPD, provides that its provisions are applicable to the treatments that are carried out on any information *"on 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" (arts.* 2.1 and 4.1).

On the other hand, article 4.2) of the RGPD considers *"treatment": any operation or set of operations carried out on personal data or sets of personal data, either by automated procedures or not, such as collection, registration, organization , structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of enabling access, comparison or interconnection, limitation, deletion or destruction".*

On the basis of these precepts, it is clear that the use of devices for the purpose of time control or presence through facial recognition entails the processing of personal data, which is subject to the principles and obligations established by the 'RGPD.
In addition, it should be borne in mind that to the extent that said devices use facial recognition mechanisms, biometric data will be processed. Article 4.14 of the RGPD defines 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 dactyloscopic data".

This means that, as stated by this Authority in opinion CNS 21/2020 (which can be consulted on the website www.apdcat.cat), the processing of personal data based on automated mechanisms with the aim of confirming the unique identification of a person based on biometric data, such as the facial image, is subject to the provisions of Article 9 of the RGPD.

Recital 51 of the RGPD refers to the treatment derived from the image of a person and highlights the restrictive nature with which the treatment of special categories of data can be admitted:

"[…] 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 unique identification or authentication of a natural person Such personal data must not be processed, unless its treatment is allowed in specific situations contemplated in this Regulation, given that the Member States may establish specific provisions on data protection in order 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."

Recital 52 of the RPGD adds:

"Also, 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 as long as the appropriate guarantees are given, in order to protect personal data and other fundamental rights, when 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 other serious threats for health Such an exception is possible for purposes in the field of health, including public health and the management of health care services, especially in order to guarantee the quality and profitability of the procedures used to resolve claims for benefits and services in the health insurance regime, or for archival purposes in the public interest, scientific and historical research purposes or statistical purposes. The treatment of personal data must also be authorized on an exceptional basis when it is necessary for the formulation, exercise or defense of claims, whether for a judicial procedure or an administrative or extrajudicial procedure".

These considerations are related to the principle of lawfulness (art. 5.1.a) of the RGPD), from which any processing of personal data must be lawful, and requires that one of the legal bases established in the article 6.1 of the GDPR. And, to the extent that they are treated special categories of personal data, as in the case at hand, must also apply any of the exceptions provided for in article 9.2 of the RGPD.

As can be seen from the consultation, the treatment intended by the City Council responds to the need to control the presence of staff in the service of the local body at the workplace. Thus, to the extent

that the processing of your personal data is carried out within a legal employment or administrative relationship, and has as its purpose the control by the staff of their obligations and duties, in particular, the presence or compliance of the day, it would be possible to attend to the legal basis provided for in article 6.1.b) of the RGPD ("the treatment is necessary for the execution of a contract in which the interested party is a party or for the application of pre-contractual measures at his request").

With regard to labor personnel, labor legislation must be taken into account (article 2.4 of Decree 214/1990, of July 30, which approves the Regulations for personnel in the service of local entities). And, in this sense, it is appropriate to bring to analysis the provision of article 20.3 of the Workers' Statute, approved by Royal Legislative Decree 2/2015, of October 23, according to which:

"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, as the case may be, the real capacity of workers with disabilities"

And, in particular, article 34.9 of the Workers' Statute, which provides for the following:

"The company will guarantee the daily register of work, which must include the specific schedule of start and end of the working day of each working person, without prejudice to the flexible hours established in this article.

Through collective bargaining or company agreement or, failing that, the employer's decision prior to consultation with the legal representatives of the workers in the company, this day record will be organized and documented.

The company will keep the records referred to in this provision for four years and they will remain at the disposal of the workers, their legal representatives and the Labor and Social Security Inspectorate."

On the basis of this precept, with regard to the labor staff of the local entity, the treatment relating to the control of the presence or working hours could also be legitimated on the basis of article 6.1.c) of the RGPD , that is to say, when the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment.

Now, as we have advanced, the processing of biometric data for the purpose of uniquely identifying a natural person requires that, in addition to a legal basis in Article 6.1 of the RGPD, one of the exceptions provided for in article 9.2 of the RGPD.

In the case being examined, it is appropriate to analyze the assumption provided for in letter b) of article 9.2 of the RGPD, regarding when the treatment is necessary for the fulfillment of obligations and exercise of specific rights of the person in charge of the treatment or of the interested party in the field of labor law and social security and protection, to the extent authorized by the law of the Union or of the Member States or a collective agreement in accordance with the law of the Member States that establishes adequate guarantees regarding the fundamental rights and interests of the interested party.

In order for this circumstance to occur, however, it will be necessary:

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

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

Regarding the authorization contained in the law of the member states, recital 41 of the RGPD provides that "when the present Regulation refers 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 (Article 53 CE).

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 processing of personal data of workers in the labor field, in particular, among others, for the purpose of compliance with 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 the interested parties, as well as their legitimate interests and rights fundamental, in particular, in relation, among others, to the supervisory systems in place of work

In accordance with what has been advanced, in the case of personnel subject to the labor regime, the Workers' Statute foresees the possibility for the employer to adopt surveillance and control measures to verify compliance with the labor obligations of its workers (art. 20.3), but in the case of the control of the day, establishes the need to draw up a daily record of the days (art. 34.9).

However, it should be borne in mind that the regulations do not determine the mechanism that can be used to record the day, nor does it provide for any authorization to use special categories of data, specifically, biometric data.

In relation to this lack of concreteness of the rule, it is necessary to take into account the sentence of Constitutional Court 76/2019, of May 22, in which the court recalls that the interference state in the field of fundamental rights and public freedoms requires a rule with the status of law and specifies the indispensable requirements that this rule must meet as a guarantee of legal security:

"[…] This double function of the reserve of law translates into a double requirement: on the one hand, the necessary intervention of the law to enable interference; and, on the other hand, that legal norm "must meet all those indispensable characteristics as a guarantee of legal security", that is, "must express each and every one of the presuppositions and conditions of the intervention" (STC 49/1999, FJ 4). In other words, "it does not only exclude powers of attorney in favor of the rules

regulations [...], but also implies other requirements regarding the content of the Law that establishes such limits" (STC 292/2000, FJ 15).

The second requirement mentioned constitutes the qualitative dimension of the reserve of law, and is specified in the requirements of predictability and certainty of restrictive measures in the field of fundamental rights. In STC 292/2000, FJ 15, we point out that, even if they have a constitutional foundation, the limitations of the fundamental right established by law "can violate the Constitution if they suffer from a lack of certainty and predictability in the limits they impose and their manner of application", pues "the lack of precision of the Law in los material presuppositions of the limitation of a fundamental right is likely to generate indeterminacy about the cases to which such restriction is applied"; "when this result occurs, beyond any reasonable interpretation, the Law no longer fulfills its function of guaranteeing the own fundamental right that it restricts, then let the will of the person who has to apply it simply operate instead." In the same sentence and legal foundation we also need the type of violation that entails the lack of certainty and predictability in the limits itself: " it would not only injure the principle of legal security (art. 9.3 EC), conceived as certainty about the applicable order and reasonably founded expectation of the person about what should be the action of the power applying the law (STC 104/2000, FJ 7, por todas), but at the same time said Law would be injuring the essential content of the fundamental right thus restricted, given that the way in which they have been fixed or its limits make it unrecognizable and make its exercise impossible in practice (SSTC 11/1981, FJ 15; 142/1993, of April 22 (RTC 1993, 142), FJ 4, and 341/1993, of November 18 (RTC 1993, 341), FJ 7)".

That is to say, the impact of the right to data protection arising from the rule must be foreseeable. And in a case like the one we are dealing with, the rule cannot be considered foreseeable if it does not specify the possibility of using biometric data for the purpose of time control.

In addition, the judgment also determines that the rule must establish adequate guarantees, especially when dealing with special categories of data. In particular, the Court states the following:

"The requirement for special protection of this category of data is provided for in the Convention for the protection of persons with respect to the automated processing of personal data (RCL 1985, 2704), of January 28, 1981 (instrument of ratification in the Spanish legal system on November 15, 1985), whose article 6 establishes the following: "The data of a personal character that reveal the racial origin, the political opinions, the

religious convictions or other convictions, as well as personal data relating to health or sexual life, may not be processed automatically unless internal law provides for appropriate guarantees. [...]." [...]

Adequate guarantees must ensure that data processing is carried out under conditions that ensure transparency, supervision and effective judicial protection, and must ensure that data are not collected disproportionately and are not used for purposes other than those they justified their obtaining. The nature and scope of the guarantees that are constitutionally enforceable in each case will depend on three factors essentially: the type

of data processing that is intended to be carried out; the nature of the data; and the probability and severity of the risks of abuse and illicit use which, in turn, are linked to the type

of treatment and the category of data in question. Thus, data collection with statistical purposes does not pose the same problems as data collection with a specific purpose.
Nor does the collection and processing of anonymous data involve the same degree of interference as the collection and processing of personal data that are taken individually and are not anonymized, as is the treatment of personal data that reveal ethnic or racial origin , political opinions, health, sex life or sexual orientation of a natural person, than the treatment of other types of data.

The level and nature of the adequate guarantees cannot be determined once and for all, because, on the one hand, they must be revised and updated when necessary and, on the other hand, the principle of proportionality requires verifying whether, with the development of technology, treatment possibilities appear that are less intrusive or potentially less dangerous for fundamental rights."

To the extent that the special categories of data have special protection, superior to other personal data, "An adequate and specific protection against its treatment constitutes, in sum, a constitutional requirement, without prejudice to the fact that, as seen, it also represents a requirement derived from European Union law. Therefore, the legislator is constitutionally obliged to adapt the protection it provides to said personal data, where appropriate, imposing greater requirements so that they can be the object of treatment and providing specific guarantees in their treatment, in addition to those that may be common or general."

Thus, given the lack of predictability of the regulations, it does not seem that the treatment of time control through facial recognition can be based on a rule with the rank of law, in accordance with the provision of letter b) of article 9.2 of the RGPD.

With regard to staff subject to an administrative legal relationship, although the regulations relating to the public function do not contain specific provisions related to the registration of staff hours, equivalent to articles 20.3 and 34.9 of the Workers' Statute, they do we find forecasts related to compliance with the stipulated day (such as article 54.3 of the Royal Legislative Decree 5/2015, of October 30, which approves the revised text of the Basic Statute Law of the 'public employee, or article 108.2.g) of Legislative Decree 1/1997, of 31 October, which approves the recasting in a single text of the precepts of certain legal texts in force in Catalonia in matters of public function), and the disciplinary regime applicable in case of breach of this (such as article 116, section .o) iq) (serious offences) or article 117.d) (minor offences) of the Legislative Decree 1/1997, of October 31.) from which the public administrations can adopt more hours of surveillance and control of the execution of the day by public employees.

However, as it happens in the case of working personnel, the regulations do not provide for the use of biometric data to control the presence or execution of the day.

In the absence of legal provision, it should be remembered that, in accordance with the provisions of article 9.2.b) of the RGPD, the authorization may be provided for in the framework of a collective agreement. Forecast to understand also applicable to agreements on working conditions of civil servants within the framework of collective bargaining. Therefore, in the event that the collective agreement, pact or agreement resulting from the negotiation provides for the use of biometric data for this purpose and establishes adequate guarantees with respect to the fundamental rights and interests of the persons concerned, this instrument would allow concluding the concurrence of the exception provided for in article 9.2.b) of the RGPD.

IV

In the consultation, the City Council refers to the fact that the entity installing the devices has indicated the need to have the consent of the staff for the treatment of their image for the purpose of time control. It is understood that the City Council refers to the legal basis of consent (art. 6.1.a of the RGPD), which must be explicit in the case of treatments on special categories of data (art. 9.2.a) of the RGPD).

Article 4.11) of the RGPD provides that consent constitutes "[...] any manifestation of free will, specific, informed and unequivocal by which the interested party accepts, either through a statement or a clear affirmative action, the processing of personal data concerning you".

At the same time, it should be borne in mind that, to the extent that the intended treatment entails treating special categories of data, the consent must be explicit (art. 9.2.a) RGPD). In relation to this requirement, it is necessary to take into account Directives 5/2020 on consent within the meaning of Regulation (EU) 2016/679 of the European Data Protection Board (EDPB) (https://edpb.europa.eu/ sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf):

"93. The explicit term refers to the way in which the interested party expresses consent. It means that the interested party must make an express declaration of consent. An obvious way to guarantee that consent is explicit would be to expressly confirm said consent in a written statement. When appropriate, the person in charge could ensure that the interested party signs the written statement, in order to eliminate any possible doubt or lack of proof in the future. […]".

Regarding the requirement that consent be free, Recital 43 of the RGPD states the following:

"[…] the consent […] should 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 for the treatment, in particular when said person responsible is a public authority and it is therefore improbable that consent was given freely in all the circumstances of that particular situation."

On this issue, regarding the free nature of consent, you must also take into account Guidelines 5/2020 of the CEPD. Of these Guidelines, the following should be highlighted:

“13. The term "free" implies real choice and control on the part of the interested parties. [...] if the subject is not really free to choose, feels obliged to give his consent or will suffer negative consequences if he does not give it, then the consent cannot be considered valid.
[...] The notion of imbalance between the person responsible for the treatment and the interested party is also taken into account in the RGPD.

14. When assessing whether the consent has been given freely, the specific situations in which the consent is subject to the execution of contracts or the provision of a service must also be considered. In general terms, the consent will be invalidated by any inappropriate influence or pressure exerted on the interested party (which can manifest itself in many different ways) that prevents him from exercising his free will.

[...]

16. Recital 43 clearly indicates that it is not likely that the public authorities can rely on the consent to carry out the data treatment since when the person responsible for the treatment is a public authority, there is always a clear imbalance of power in the relationship between the responsible for the treatment and the interested party. It is also clear in most cases that the interested party will not have realistic alternatives to accept the treatment (the treatment conditions) of said responsible.

The ECPD considers that there are other legal bases that are, in principle, more suitable for the processing of data by public authorities.

17. Without prejudice to these general considerations, the use of consent as a legal basis for data processing by public authorities is not totally excluded under the legal framework of the RGPD. [...]

21. An imbalance of power also occurs in the context of employment. Given the dependence that results from the relationship between the employer and the employee, it is not likely that the interested party can deny his employer consent to data processing without experiencing real fear or risk that his refusal will have harmful effects. It seems unlikely that an employee could respond freely to a request for consent from his employer to, for example, activate camera surveillance systems in the workplace or to fill out evaluation forms, without feeling pressured to give his consent.
[…] In the case of most of these data treatments at work, the legal basis cannot and should not be the consent of the workers […] due to the nature of the relationship between employer and employee.

22. However, this does not mean that employers can never rely on consent as a legal basis for data processing. There may be situations in which the employer can demonstrate that consent has been given freely. Given the imbalance of power between an employer and his staff members, workers can only give their free consent in exceptional circumstances, when the fact that they give said consent or not does not have adverse consequences”.

On the basis of what has been presented, and other issues that are also included in Guidelines 5/2020 of the CEPD, to which we refer, it does not seem that the legal basis of consent is suitable to legitimize the processing of the data of the staff for the purpose of time control of the staff, given that it cannot be considered that in the case raised there could be truly free consent. In this sense, it could be considered that free consent exists if the interested party has an alternative to comply with the time control or control his presence or execution of the schedule, and it is he who chooses and gives his consent to processing of their biometric data through facial recognition systems, but this does not appear to be the case in a case such as the one described in the inquiry.

In short, the data protection regulations do not generally accept consent as a legitimizing legal basis for the treatments carried out by the
public administrations or employers for control in the work environment, given the imbalance of power that tends to occur between those relationships with the interested parties, which prevents consent from being considered free.

To this end, it must be taken into account that, in accordance with the principle of proactive responsibility (art. 5.2 of the RGPD), the data controller, in the case that we are dealing with the City Council, must be able to demonstrate that the consent is valid and that the treatment is lawful.

v

Apart from the principle of lawfulness, any treatment must also comply with the rest of the principles and obligations derived from data protection regulations, such as the principle of minimization (art. 5.1.c) RGPD).

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 the minimization 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 used. 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 support the installation of time compliance control systems seems clear
by the staff, as this Authority has repeatedly recognized. However, it does not seem so clear that the use of time control systems based on biometric data should be accepted as a preferred means of carrying out the control. Rather the opposite.
Given the special nature of this data, it will be necessary to opt, in the first place, for other systems

control that, without using specially protected categories of data, they can allow achieve the same purpose.

The requirements derived from data protection in the design (art. 25.1 RGPD) and, in particular, of 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 noted that biometric data, given their personal and unique nature, constitute a reliable means of identification (although in certain biometric data it may there is a risk of non-identification). 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. But, in addition, 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.

In order to determine the existing risks and the measures to mitigate them, Guidelines 3/2019 on the processing of personal data using video devices of the ECPD may be of help, in particular section 5.2 relating to the measures suggested to minimize risks at the consultable link https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_es.pdf.

treat data biometrics, Next

It is undeniable that the use of systems based on biometric data to carry out the hourly control avoids the risk of impersonation that can occur in some cases, as the query points out. 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.

The consultation, apart from referring to the need to avoid the risk of spoofing that other marking mechanisms may have, such as the use of individual cards, also refers to what one of the reasons for installing these systems is to follow the health recommendations regarding Covid-19 to prevent possible contagions by replacing the fingerprint control system.

Although the query does not specify which recommendation it refers to, it is understood that it refers to the recommendations of public authorities in the context of the Covid-19 pandemic, such as the Ministry of Health, which in different Orders (such as Order SND/388/2020, of May 3; Order SND/399/2020, of May 9, or Order SND/458 /2020, of May 30) has foreseen, collected in different articles respectively, the following:

"Fingerprint logging will be replaced by any other time control system that guarantees adequate hygiene measures to protect the health and safety of workers, or the logging device must be disinfected before and after each use, warning the workers of this measure."

At the outset, this recommendation can in no case constitute an exception for the treatment of special categories of data for the purposes provided for in article 9.2.b). But beyond this, there are other possible alternatives of simple application, without having to change the control system, such as disinfecting the marking device before and after each use, or having the worker have a dispenser of antiseptic gel near the marking system to be used once the signing is done with the finger, both entry and exit. Therefore, replacing the dialing system does not seem to have to be the only option.

It should be borne in mind that the processing of fingerprints also constitutes processing of biometric data, given the provisions of article 4.11 of the RGPD. This means that in the same way that the treatment through facial recognition requires, in addition to a legal basis in accordance with what is provided for in article 6.1 of the RGPD, that one of the assumptions provided for in article 9.2 is met of the RGPD, according to what has been analyzed, the processing of the fingerprint for this purpose also requires it to the extent that it is a special category of data. In any case, if there is a legal basis for processing the fingerprint for the purpose of time control, but not for using facial recognition mechanisms, while this situation lasts, it would be necessary to resort to another system that does not involve the processing of special categories of data

Finally, remember that, prior to the decision on the implementation of a control system of this type, it must be taken into account that article 35 of the RGPD foresees the need to carry out an evaluation of the impact related to data protection (AIPD) in those treatments, especially if they use new technologies, which entail a high risk for the rights and freedoms of people. For these purposes, and in accordance with article 35.4 of the RGPD, this Authority has published a List of types of data processing that require a data protection impact assessment (https://apdcat.gencat.cat/web/.content/02-rights_and_obligations/obligations/documents/List-DPIA-CAT.pdf), in which it is determined that it will be necessary to make an AIPD in most cases where the treatment meets two or more criteria in the list. Among these criteria, the following may apply in the case under analysis:

"[...] 3. Treatments that involve the observation, monitoring, supervision, geolocation or control of the interested party in a systematic and exhaustive manner, including the collection of data and metadata through networks, applications or in public access areas, as well as the processing of unique identifiers that allow the identification of users of services of the information society such as web services, interactive TV, applications cell phones, etc.

[...]

5. Treatments that involve the use of biometric data for the purpose of identifying unique way to a natural person.

[...]

10. Treatments that involve the use of new technologies or an innovative use of consolidated technologies, including the use of technologies on a new scale, with a new objective or combined with others, so that it involves new forms of collection and use of data with risk to people's rights and freedoms.[...]"

Consequently, it is necessary to carry out an assessment of the impact relating to data protection, in which it is necessary 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 (art. 35 GDPR).

In accordance with the considerations made in these legal bases in relation to the consultation raised in relation to the use of control systems based on facial recognition mechanisms, the following are made,

Conclusions

The consent of the affected staff cannot be considered an adequate legal basis for the implementation of a time control system using facial recognition as described in the consultation.

It would be necessary to provide for this control system in a legal provision or in an applicable collective agreement, or if applicable, in a pact or agreement resulting from collective bargaining, circumstances that do not seem to occur in the analyzed case. In any case, before the implementation of a system of this type, it is necessary to carry out an assessment of the impact on data protection in view of the specific circumstances in which the treatment is carried out to determine the legality and proportionality, including the analysis of the existence of less intrusive alternatives, and establishing appropriate safeguards.

Barcelona, February 2, 2022