apdcat
Autoritat Catalana de Protecció de Dades

Opinion in relation to the inquiry made by the Protection Delegate of Data from a city council on the legal viability and legitimacy of capturing images of people for the purpose of maritime rescue of people

A query formulated by the Catalan Data Protection Authority is presented Data Protection Officer (DPD) of a city council on the legal viability and legitimacy of capturing images of people for the purpose of maritime rescue of people.

In the consultation it is stated that the city council is interested in developing a software that allows to improve and optimize the tasks of maritime rescue of people. The company to which the city council has commissioned its development needs, for this purpose, to have *"a large amount of images of the sea and of the people who are bathing in it so that the computer program can understand which situations drowning is occurring and which are normal situations that can occur in the interior of the sea and, consequently, distinguish situations of risk and danger from common situations in which no danger situation is occurring. Although it is true that this type of information is collected, it is not possible to identify the specific people who are being recorded because the data that will be used for the operation of the software is not the identification of specific people through the images but the movements and behaviors in the water in the framework of safety."*

As indicated, the recording of images of people at sea is necessary for the implementation and training of the program. Once the data is entered, no further recordings will be required. The recording would be limited to the period from July to October 2022 at a beach in the municipality. Once the software is configured, it continues to indicate, it will only capture images in real time but they will not be recorded.

In this context, the Data Protection Officer requests *an "opinion on the legal feasibility and legitimacy of the recording identified in the body of this letter, specifying, where appropriate, the necessary measures to be taken to avoid the violation of rights and the protection of the higher public interest that we understand this practice entails."*

Having analyzed the query, and in view of the current applicable regulations, in accordance with the report of the Legal Counsel, I inform you of the following:

I

(...)

II

The data protection representative of a town hall requests that the Authority issue an opinion on the legal feasibility and legitimacy of the recordings described in the consultation, without attaching any other information in this regard (technical documentation, prior analysis of risks of the treatment to be carried out, etc.). It is not specified in the consultation whether the recordings will be made using image recording systems installed in drones or other mobile devices or if it will be done from fixed cameras installed on the beach, nor what is the recording technology used (whether it incorporates image anonymization tools or not), it is only specified that *"it is not possible to identify the specific people who are being recorded because the data that will be used for the operation of the software is not the identification of specific people through the images but the movements and behavior in the water in the framework of safety".*

From the information provided it appears that they want to carry out, on the one hand, the recording of the sea and the people who are bathing in it in order, as indicated, to have a large amount of these images available so that the computer program can understand in which situations a drowning is occurring and which are normal bathing situations.

On the other hand, it seems that, once the software has been developed, a system based on the real-time capture of images of the beaches (without recording) is to be implemented in order to serve as support in maritime rescue tasks.

III

In order to focus the answer to this query, it must be taken into account that the concept of personal data in the RGPD is a broad concept that covers any information referring to a natural person, whether this person is identified or can be identified. Thus article 4.1 of Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereafter, RGPD), establishes that personal data is: *"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;*

In this regard, recital 26 of the RGPD establishes:

> *"The principles of data protection must be applied to all information relating to an identified or identifiable natural person. Pseudonymized personal data, which could be attributed to a natural person through the use of additional information, must be considered information about an identifiable natural person. To determine whether a natural person is identifiable, all means, such as identification, that can reasonably be used by the data controller or any other person to directly or indirectly identify the natural person must be taken into account. To determine whether there is a reasonable probability that means will be used to identify a natural person, all objective factors must be taken into account, such as the costs and time required for identification, taking into account both the technology available at the time of the treatment as technological advances. Therefore the principles of data protection should not be applied to the information*

anonymous, that is, information that is not related to an identified or identifiable natural person, or to data converted into anonymous data so that the interested party is not identifiable, or ceases to be so. Consequently, this Regulation does not affect the treatment of said anonymous information, including for statistical or research purposes."

In the case raised in the consultation, the capture of images of the sea could allow to obtain images of people who are bathing in the sea, and also of boats, jet skis and any other vessel that is equipped with license plates or numbers identification that makes the physical users or owners of the same identifiable.

Therefore, any operation of collecting images, sounds, geolocation data, or any other information related to an identified or identifiable natural person that is carried out with the recording systems referred to in the query, whether mobile (for example drones) or fixed, involves the processing of personal data and, consequently, will remain subject to compliance with the principles and guarantees of data protection regulations. Specifically, in the RGPD, in Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD) and, specifically, in Instruction 1/2009, of February 10 , of the Catalan Data Protection Agency, on the processing of personal data using cameras for video surveillance purposes, where it has not been affected by the RGPD and the LOPDGDD.

It should be taken into consideration that whether or not it is appropriate to use a certain video surveillance system, from the perspective of data protection, must respond to a prior assessment and weighting by the City Council, which must take into account, among others, the impact on citizens' rights and compliance with the principles and guarantees of the aforementioned data protection regulations.

In this sense, the use of cameras or video surveillance systems must respect, among others, the principles of legality (Article 5.1.a) RGPD), purpose limitation (Article 5.1.b) RGPD) and data minimization (article 5.1.c) RGPD), from which data can only be captured and processed through video surveillance systems under the protection of a legal basis, with specific, explicit and legitimate purposes, and adhering to the data that are adequate, relevant and limited to what is necessary in relation to the intended purpose.

In relation to the principle of lawfulness, the RGPD establishes that all processing of personal data must be lawful, fair and transparent (Article 5.1.a)). And, in order to consider the treatment lawful, the RGPD establishes the need to meet one of the legal bases of article 6.1.

As this Authority has decided on other occasions (among others, in opinions CNS 4/2022, CNS 42/2021, CNS 33/2021 or CNS 21/2021, available on the Authority's website), in the scope of public administrations, the capture of images for video surveillance purposes can be authorized in the legal basis of article 6.1.e) of the RGPD, according to which the processing of data can be lawful if *"it 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 the LOPDGDD, data processing can only be considered based on this legal basis of article 6.1.e) of RGPD when so established by a rule with the rank of law.

III

As indicated in the consultation, the systems that want to be implemented have the purpose of developing and installing support tools in the tasks of saving people at sea that the municipality has attributed.

Article 84.2.n) of the Statute of Autonomy of Catalonia attributes to the municipality the powers on *"The regulation, management and monitoring of the activities and uses that are carried out on the beaches, the rivers, the lakes and the mountain".*

For its part, Law 17/2015, of July 9, of the National Civil Protection System establishes that .

> *"1. Civil protection, as an instrument of public security policy, is the public service that protects people and goods by guaranteeing an adequate response to the different types of emergencies and catastrophes caused by natural causes or derived from human action, be it accidental or intentional."*

In this sense, his statement of reasons states that *"This system of civil protection is understood as an instrument of public security, integrated in the policy of National Security".*

In addition, the LRBRL in its article 25.2.f) attributes to the municipalities competences in the matter of *"Local police, civil protection, prevention and extinguishing of fires"* and municipalities with more than 20,000 inhabitants must provide civil protection services (article 26).
Likewise, Law 22/1988, of July 28, on coasts (hereafter LC) establishes a competence attribution in favor of the municipalities in matters of beaches, thus, article 115.d) of LC attributes them among its functions: *"Maintain the beaches and public bathing places in the proper conditions of cleanliness, hygiene and health, as well as monitor the observance of the rules and instructions issued by the State Administration on the safety and security of human lives".*

Therefore, the city council would have a legal basis for the processing of the personal data necessary for the exercise of the functions attributed by the rules mentioned in relation to article 6.1.e) RGPD.

Now, in the case at hand, the fact that, both for the development of the software and for the operation of the proposed system, it is planned to capture images of natural persons who are in the bathing area of the municipality's beaches is of particular relevance.

It must be taken into account that beaches are public spaces that, despite not being strictly speaking "public roads", guarantees equivalent to those provided for in article 22.2 of LOPDGDD for catchments on public roads must be applied. Citizens who are on the beach should not see their privacy less protected than when they are in other public spaces such as streets, squares, parks, etc. Thus, as this Authority highlighted in opinion CNS 27/2015 (FJ V), available on the Authority's website, the application regulations *"provide a broad conception of the concept, that is any space*

public whether open or closed. This concept has traditionally been understood to refer to those places in the public domain that are intended for general use (eg a road, a beach or a park). However, the concept "public place" tends to prevail today to more commonly designate the places that the public usually frequents, regardless of their ownership. Thus, other private spaces open to the public (such as commercial areas) are also considered public places. It seems, therefore, that, for the purposes of establishing the scope that must be given to the concept of "public place", the elements of accessibility and the use that citizens make of this space acquire greater relevance in the face of legal nature of the asset (among others, SAN of May 20, 2011).

It is not superfluous to point out, at this point, that the various municipal ordinances regulating public places or spaces - to, among other things, guarantee citizen coexistence - tend to define these spaces as streets, thoroughfares, squares, avenues, passages, parks, gardens and other spaces or green or forest areas, bridges, tunnels and underpasses, car parks, fountains and ponds, public buildings and other spaces intended for use or public service owned by the municipality (...) ".

In the case of beaches, moreover, there is the circumstance that they are spaces in which, both by their nature and by the leisure activities that take place there, there are
special expectations of privacy on the part of its users.

According to article 22 of the LOPDGDD:

*"2. **Only images of the public road may be captured to the extent that it is essential** for the purpose mentioned in the previous section.*
However, it will be possible to capture the public road in a higher extent when it is necessary to guarantee the security of assets or strategic facilities or infrastructures linked to transport, without in any case being able to suppose the capture of images of the interior of a home private

(...)
6. The processing of personal data from the images and sounds obtained through the use of cameras and video cameras by the Security Forces and Bodies and by the competent bodies for surveillance and control in prisons and for control, regulation, traffic surveillance and discipline, will be governed by the legislation transposing Directive (EU) 2016/680, when the treatment has the purpose of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including the protection and prevention against threats to public security. Outside of these assumptions, said treatment will be governed by its specific legislation and additionally by Regulation (EU) 2016/679 and this organic law.

(...)."

In the same sense, article 5.4.b) of Instruction 1/2009, establishes that it is not considered legitimate *"the capture of images of people on the public road, unless it is carried out by the forces and bodies of security in accordance with its specific regulations. The **incidental capture** of images from the public road for the surveillance of buildings or installations is only legitimate if it is unavoidable to achieve the purpose of monitoring the building or installation".*

In the case we are dealing with, the capture cannot be considered incidental since the objective is the capture of images of people bathing on the beaches, both for the development of the software and for subsequent operation. And what's more, it would not only affect people who might be in danger, but would affect any bather.
Likewise, the fact that the images are transmitted in real time and are not recorded (as seems to be done when the software is put into operation) would not exclude the application to this treatment of the data protection regulations (the same Instruction 1/2009, considers treatment for the purposes of that instruction *"the capture, including the real-time emission of images and, where appropriate, voices regardless of the support used"),* and in this sense the European Committee has pronounced of Data Protection in Guidelines 3/2019, on the processing of personal data using video devices.

The capture of images on *"public roads"* corresponds only, in principle, to the Security Forces and Bodies for certain purposes linked to the prevention, investigation, detection or prosecution of criminal offenses and the protection and prevention against threats against public security, in accordance with the provisions of the applicable specific regulations.

In this sense, it should be in accordance with the provisions of Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal sanctions.

This rule repeals what is opposed to the regulations applicable to police video surveillance established until then by Organic Law 4/1997, of August 4, which regulates the use of video cameras by the Security Forces and Bodies in public spaces (LOVFCS), developed in Catalonia by Decree 134/1999, of 18 May, regulating video surveillance by the police of the Generalitat and the local police of Catalonia, by the Order of 29 June of 2001, regulating the means by which the existence of fixed video cameras installed by the police of the Generalitat and the local police of Catalonia in public places is reported.

This regulation, which allows the capture of images from public roads, is limited to those video surveillance systems managed by police forces for one of the purposes established within the scope of application of Organic Law 7/2021, established in its article 2.1: *"It will apply to the total or partially automated processing of personal data, as well as to the non-automated processing of personal data contained or destined to be included in a file, carried out by the competent authorities, for the purposes of prevention, detection , investigation and prosecution of criminal offenses and execution of criminal sanctions, including the protection and prevention against threats against public security*

In this sense, even though the city council has powers in matters of civil protection and civil protection is an instrument of public security, it does not seem that the purpose linked to the protection of people on the beaches can be considered included in the purposes of prevention, detection, investigation and prosecution of criminal offences, including those relating to threats against public security defined by Organic Law 7/2021.

Consequently, the City Council would not be entitled to install the intended video surveillance systems if they allow physical persons to be identified, with the purpose of to collaborate in maritime rescue tasks, to the extent that it involves the capture of images of public spaces such as the beaches of the municipality.

Personal data protection regulations would not, however, oppose the use of systems that do not capture images of identifiable natural persons. This in the understanding that the mere capture of the images, even if they are then treated with automated systems that anonymize them, already involves the processing of personal data (art. 4.2 RGPD).

conclusion

Current regulations do not give the City Council sufficient authority to implement video surveillance systems that involve the capture of images of identifiable natural persons in the bathing areas of the beaches for the purpose set out in the consultation.

Barcelona, August 23, 2022