Response to Public consultation n°10/2024 about Guidelines 1/2024 on processing of personal data based on Article 6 (1) (f) GDPR

To be submitted before the 20th of November

1. Context

We are a company that provides software that is integrated into surveillance cameras in supermarkets or everyday shops and automatically detects suspicious gestures that could be interpreted as theft.

We therefore operate in what might be called the 'smart camera' or 'augmented camera' sector.

We have noticed that this subject is not addressed in your guidelines on legitimate interest.

However, **augmented cameras are personal data processing operations that should be based on legitimate interest**, provided that they are not implemented by public authorities and that they do not involve the processing of sensitive data (including no biometric processing).

In particular, in your guidelines on video devices, you indicated that legitimate interest should be the legal basis given priority in the absence of a legal obligation or execution of a public service[1].

However, we regret that the specific subject of augmented cameras has not been addressed by the EDPB, despite the fact that it has been particularly questioned by national supervisory authorities in recent years.

We believe that your new guidelines on legitimate interest provide an opportunity to reaffirm the legality of this type of personal data processing.

We have therefore developed below the points that we believe should be taken into account by the EDPB in its second version of its guidelines on legitimate interest.

2. No need for specific legal authorization

The main topic of our contribution is to get the EDPB to restate an important principle of the GDPR that some national supervisory authorities seem to want to call into question: **no processing of personal data should as such require a specific law to be based on legitimate interest**.

The CNIL is asking a specific legislative framework for augmented cameras, in total contradiction with the spirit of the GDPR, which is intended not to prohibit any particular processing as long as it complies with the fundamental principles and documentary requirements of the GDPR.

In its position on the conditions for the deployment of augmented cameras, the CNIL stated that: '*In order to be legally implemented, most systems require the existence of a legislative or regulatory text authorizing or supervising them*'[2].

---

[1] Section 3.1, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0 Adopted on 29 January 2020

[2] Position on the conditions for the deployment of 'intelligent' or 'augmented' cameras in public spaces, July 2022, CNIL

Your guidelines never mention that a law should specify whether a particular processing operation has the 'right' to rely on legitimate interest as a legal basis.

You set out three conditions and accept that once they have been met, the processing is lawful: "*In order to determine whether a given processing of personal data may be based on Article 6(1)(f) GDPR, controllers must carefully assess whether the three cumulative conditions listed above can be met so as to ensure that the processing is lawful*.". [3]

Therefore, we think it is important that you make it clear that the legitimate interest basis can be used for any kind of processing, without the need for a law, as long as these three conditions are met.

3. Meeting the three conditions

In its guidelines, the EDPB recalls that the three conditions for relying on legitimate interest are as follows:

- pursuing a legitimate interest
- that the processing is indeed necessary to pursue this legitimate interest
- that the processing does not disproportionately affect the fundamental rights and interests of the persons concerned.

We believe that the EDPB should clarify in which cases augmented camera processing can meet these three criteria.

3.1 Physical security as a legitimate interest

In its guidelines, the EDPB does not list the legitimate interests that may be pursued directly by data controllers (other than those recognized by case law). In order to establish legal certainty, we believe that the EDPB should take a clear stance on both the interests that are inherently legitimate and those that are not.

We believe that ensuring the physical safety of people and property should be added to this list.

More to the point, automatic, real-time video analysis of individuals to detect behavior suggesting theft should be able to be based on legitimate interest.

We consider that this processing can be based on the legitimate interest of shops in ensuring security and detecting thefts and incidents in their shops. This legitimate interest is both a public policy imperative (combating criminal offences) and an economic imperative (combating loss of turnover due to theft).

It should be noted that the fight against shoplifting has also had a positive economic impact on the data subjects: shops pass on the loss of sales due to theft in the prices of their products. If this loss of turnover is reduced, prices for consumers will fall.

In-store theft is responsible for an estimated annual loss of sales of around €49 billions for 11 countries[4] in Europe, around 2,1% of retail sector turnover.[5]

---

[3] §12 of your guidelines

[4] Belgium (BE), Germany (DE), Finland (FI), France (FR), Italy (IT), the Netherlands (NL), Poland (PL), Russia (RU), Spain (ES), Sweden (SE) and the United Kingdom (UK).

[5] https://crimetech.it/2019/06/20/retail-security-in-europe-going-beyond-shrinkage/

Clarifying to data controllers in which cases the interests pursued are considered legitimate in principle therefore appears to us to be one of the objectives that your guidelines must pursue.

3.2 Assessing the need

The EDPB indicates in its guidelines that: "*Assessing what is "necessary" involves ascertaining whether in practice the legitimate data processing interests pursued cannot reasonably be achieved just as effectively by other means less restrictive of the fundamental rights and freedoms of data subjects*[6]."

However, it is not described in detail how in practice a data controller can ensure that its processing is necessary.

In the case of augmented cameras and our software in particular, it seems very clear to us that the processing of personal data is indeed necessary to meet the legitimate interest pursued.

Augmented cameras respond to a need identified in the convenience retail sector: making it easier to detect theft without the need for additional staff.

These augmented camera mechanisms offer the following undeniable advantages:

- Compensate for staff shortages in property and personal security[7]
- Replacing the least skilled and most tiring jobs (constantly looking at several cameras at once is not a desirable activity for the human brain) with an artificial intelligence algorithm;
- Eliminate human bias in theft detection: while theft detection is often based on facial features when operated by staff, it is based solely on neutral gestures when operated by our augmented camera solution.

The CNIL itself recognizes the usefulness of this type of processing: "*Augmented video systems offer a number of technical advantages: on the one hand, they automate the processing of images captured by cameras, which was previously carried out by humans; on the other, they offer the possibility of analyzing certain parameters that the human eye would not be able to achieve. In this way, they can add value to existing camera installations."*[8]

However, the CNIL has decided to add a condition that does not exist in the GDPR for smart cameras, stating that: '*Furthermore, the very existence of a right to object could, in some cases, appear to be incompatible with the very purpose of the processing: this is the case for the detection of abnormal, suspicious or dangerous behavior for the purposes of protecting people and property'*[9]. The CNIL does not base this assertion on any specific analysis or study with figures. However, this statement has direct consequences for the augmented camera sector for the purposes of ensuring the safety of people and property.

The CNIL deduces that this type of system would have to benefit from a law that would exclude the right to object in this case in order to be lawful : "*As a result, 'augmented' video devices will have to be authorized by a specific legal framework that is at least regulatory in nature and complies with the conditions set out in Article 23 of the RGPD27, unless it is not possible to justify the effective and acceptable implementation of a right to object (...)*".

We therefore ask the EDPB to take a position on this point: exercising the right to object does not prevent effective processing for the purposes of fraud or ensuring the safety of persons and property.

---

[6] §49
[7] https://www.euractiv.com/section/economy-jobs/video/tackling-eu-labour-shortages-in-private-security-services/
[8] Position on the conditions for the deployment of 'intelligent' or 'augmented' cameras in public spaces, July 2022, CNIL
[9] Position on the conditions for the deployment of 'intelligent' or 'augmented' cameras in public spaces, July 2022, CNIL

There is no tangible evidence to support the fact that a person committing a theft would wish to draw attention to itself by exercising its right to object. Moreover, this position is based on the assumption that thefts are necessarily committed by people with an organized modus operandi, who enter the shop with the intention of committing a theft and who will take the initiative of exercising their right to object in order to escape the surveillance system. This is a pure assumption on the part of the CNIL: people who commit theft are diverse, act differently and do not have a single modus operandi.

For the CNIL, the rights of data subjects should therefore be diminished by specific laws on the pretext that otherwise the processing of their data would not be effective.

We therefore call on the EDPB to affirm that allowing data subjects to exercise their rights is never an obstacle to the effectiveness of the processing of personal data.

3.3 No disproportionate infringement regarding the interests and rights of data subject

We believe it should be made clear that the processing of personal data by an artificial intelligence algorithm rather than by a human being does not necessarily mean that the processing is more intrusive.

Obviously, this reasoning is only valid if no sensitive data is processed by the artificial intelligence algorithm.

In that respect, an augmented camera that simply detects suspicious gestures in shops to prevent shoplifting does not constitute a disproportionate infringement of the rights and freedoms of data subjects.

It allows checks carried out by security officers to be based on neutral, objective causes rather than on their necessarily subjective impressions.

In particular, we believe that our augmented camera system, which only analyses the movements of the data subjects, is less intrusive than constant surveillance by security staff for the following reasons:

- there is no risk that this system will enable a person to be identified (whereas a person in charge of surveillance could recognize a known person or someone he or she knows).
- no risk of discrimination on the basis of physical appearance, since only gestures are analyzed (whereas a security guard might tend to keep a closer eye on people on racial grounds or because of their clothing).
- no risk of being judged/monitored in a general way for anything other than suspicious gestures that could qualify as theft (for example, a person in charge of surveillance could observe people kissing or picking their nose in the shop, which the augmented camera system will never monitor or record).

It is clear from this that the fate of augmented cameras must be assessed on a case-by-case basis, without their mere use being automatically considered to infringe the rights and freedoms of the data subjects to a greater extent than a conventional video surveillance system.