

**The European Data Protection Board****The National Criminal Investigation  
Service**

Your reference:

Our reference:

Date:

22/117381 - 1

27.06.2022

## **Opinion from the Norwegian National Criminal Investigation Service concerning the EDPB's Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**

The Norwegian National Criminal Investigation Service (NCIS) is the National Centre of Excellence in biometrics and is responsible for use of facial recognition technology in the area of law enforcement in Norway. Facial recognition technology is constantly evolving, and NCIS recognizes the need for guidelines for the use of this technology. The use of facial recognition technology raises several questions related to the processing of personal data, and involves an intervention in the individual's privacy and in other fundamental rights. However, NCIS considers that the proposed guidelines place too high demands on national lawmakers in terms of the level of detail required when regulating use of facial recognition technology and the required monitoring of the continuous technological developments regarding facial recognition technology.

### **Facial recognition technology in Norway**

There are no legal rules specifically regulating the use of facial recognition technology for police purposes in Norwegian law. However, facial recognition technology involves the processing of biometric data, which is a type of personal data that falls under the European privacy regulations, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED). LED regulates the processing of information for police purposes, and is implemented in Norwegian law by the Police Databases Act and the Police Databases Regulations.

Since the use of biometric information included in facial recognition technology involves the processing of personal data, the use must be in compliance with the general principles and rules in LED, and the Police Databases Act and the Police Databases Regulations. Norwegian law permits the use of facial recognition technology in law enforcement activities under the condition that it is strictly necessary, that the processing is carried out for specified, explicit and legitimate purposes, and that other relevant provisions are followed. Biometric information processed for identification purposes must follow stricter requirements for necessity.

NCIS currently uses automated facial recognition to search the police photo register with images secured in connection with an investigation. NCIS does not use a real-time monitoring

**The National Criminal Investigation Service**

---

method with facial recognition. In order to get a search result, the person must already be registered with a photo in the police photo register in accordance with provisions in the Criminal Procedure Act and the Police Databases Act. Employees with special expertise always review the search results. Today the review of the search results is conducted by experts at NCIS. However, as long as a law enforcement employee has adequate expertise in conducting the searches, we do not find it necessary "that only a very limited number of employees at the forensic department have permission to conduct the actual matching procedure" (point 4.1 in the proposed guidelines). The primary purpose of using facial recognition technology is to reduce analysis time and improve the quality of analysis. The method does not in itself provide access to any additional information than if the photo had been analyzed manually.

### **Technology-neutral regulation versus specific legislation**

The technology is constantly evolving and it is difficult to predict what will be possible in the future. The Norwegian Police Databases Act and the Police Databases Regulations constitute a technology-neutral regulation that applies to the processing of information in general. It is our view that it provides a sufficient legal basis also for the regulation of the present and future use of facial recognition technology for law enforcement purposes. Specific legislation quickly becomes obsolete due to technological developments, and there is a risk that it will have a negative impact on the lawmakers and authorities in terms of making use of the possibilities offered by technology to more effectively prevent and investigate crime and to protect people's fundamental rights and freedoms.

### **Conclusion**

NCIS considers that the proposed guidelines place too high demands on national lawmakers in terms of the level of detail required when regulating use of facial recognition technology and the required monitoring of the continuous technological developments regarding facial recognition technology. In our opinion, the requirements for detailed regulations, and the fact that the guidelines limit the use of facial recognition technology to an "absolute minimum" and only when "strictly necessary", will complicate and may put unnecessary and unintended limitations to the use of this effective and useful technology in law enforcement activities in the future.

Yours sincerely,

**Ketil Haukaas**

*Deputy Director of the NCIS*

*The document has been approved electronically without a signature.*