CM2301

NOTE ON THE EU POLICE CODE AND EXCHANGE OF FACIAL IMAGES

FEBRUARY 2023

On 8 December 2021, the European Commission adopted a Proposal for a Regulation on automated data exchange for police cooperation (known as Prüm II) amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations 2018/1726, 2019/817 and 2019/818. Subject of the proposed regulation is the automated searching of DNA profiles, fingerprints, facial images, police records and vehicle registration data. The proposed regulation is also referred to as the "EU Police Code" and has the aim to strengthen police cooperation and information exchange for preventing, detecting, and investigating criminal offences. The Meijers Committee holds that the proposed measures on the processing of facial images do not fully conform to the requirements of necessity and proportionality. Therefore, the proposal provides insufficient safeguards to protect the rights to private life and data protection in Article 7 and 8 of the Charter on Fundamental Rights. In this note, the Meijers Committee puts forwards several recommendations for the EU legislator to take on board during the further negotiations on the EU Police Code.

Meijers Committee

Standing Committee of Experts on International Migration, Refugee and Criminal Law

Commissie Meijers

CM2301 Note on EU Police Code and exchange of facial images

On 8 December 2021, the European Commission adopted a Proposal for a Regulation on automated data exchange for police cooperation (known as Prüm II) amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations 2018/1726, 2019/817 and 2019/818.[1] The proposed regulation is part of a legislative package that is referred to as the "EU Police Code" and has the aim to strengthen police cooperation and information exchange for preventing, detecting and investigating criminal offences. Subject of the proposed regulation is the automated searching of DNA profiles, fingerprints, facial images, police records and vehicle registration data. The Meijers Committee would like to bring forward that that the proposed measures on the processing of facial images do not fully conform to the requirements of necessity and proportionality. Therefore, the proposal provides insufficient safeguards to protect the rights to private life and data protection in Article 7 and 8 of the Charter on Fundamental Rights.

Level of protection

Facial images are to be viewed as personal data that can reveal racial or ethnic origin. Therefore, facial images constitute a special category of personal data, as indicated by Article 10 of the LED, not only because they are biometric data, but also because they reveal racial or ethnic origin. Processing these creates a risk of racial profiling. Hence, the processing of facial images should be allowed only when it is strictly necessary, and should be subject to appropriate safeguards for the rights and freedoms of the data subject. Furthermore, in accordance with Article 10 LED, processing is only allowed if authorized by Union or Member State law and if it is either protecting the vital interests of the data subject or of another natural person, or if it relates to data which are manifestly made public by the data subject. As to this last criterion, the proposed Regulation does not limit the exchange of information on facial images to take place with regard to images which are manifestly made public by the data subject. This will mostly not be the case. Therefore, the processing must take place to protect the vital interests of the data subject or of another natural person. It is unconvincing that the proposed Regulation complies with this requirement. Rather, it should limit the exchange of facial images in some way to the most serious crimes.

Article 4 of the proposed Regulation defines biometric data as DNA profiles, dactyloscopic data or facial images. In accordance with the Law Enforcement

[1] COM(2021) 784 final Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council.

Directive (LED)[2], biometric data are personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person. In that last definition, not all facial images are included but only those that allow for the recording of patterns of the face and measurements of facial features and contours. This ensures that facial images can be used only if they allow a high level of precision. Consequently, the level of protection is higher[3] under the LED compared to the proposed Regulation, Article 4 of which includes all facial images in the term biometric data. In practice, this means that facial images can be exchanged among police authorities under the proposed Regulation that were not collected in accordance with the higher data protection level that applies to biometric data under the LED.[4]

Facial images significantly differ from DNA profiles and fingerprints. First, a change of appearance can increase the risk of identifying the wrong person based on an image. Furthermore, that risk of misidentification might be higher be increased due to the circumstances in which an image is taken (such as angle and lighting). The risk of a false identification is also higher because, unlike DNA and fingerprints, which are uniquely[5] identifying one individual, a facial image can lead to the identification of more than one person, especially when the quality of the image is low. Second, facial images can be recorded without knowledge of the data subject.

For the aforementioned reasons, it is important to pay careful attention when processing facial images in the context of prevention, detection and investigation of criminal offences.

Necessity and proportionality

The proposed Regulation covers the prevention, detection and investigation of *all* criminal offences. No distinction is made between minor and serious offences. Considering that the proposed regulation provides for automated searching of facial images by other Member States' authorities and Europol, such intrusive measure should be restricted to only serious offences to fulfil the necessity and proportionality

[2] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[3] ECHR, S. and Marper v. the United Kingdom, case 30562/04 and 30566/04, 2008, § 76-77.

[4] See also EDRI (2022), Respecting fundamental rights in the cross-border investigation of serious crimes, p. 26-27.

[5] See M. Willebrands, 'Kansen om eeneiige tweelingen in strafzaken te onderscheiden' (NFI 2020), available at https://magazines.forensischinstituut.nl/atnfi/2020/34/kansen-om-eeneiige-tweelingen-in-strafzaken-te-onderscheiden.

requirement.[6] Moreover, such limitation would function as a barrier for using remote identification systems in publicly accessible spaces.[7] It is important to add that in accordance with the subsidiarity principle the term "serious offence" should be defined by national law.

In addition, the proposed regulation does not make a distinction between different categories of data subjects in accordance with article 6 of the LED. Considering the risks involved in automated searching of facial images, it is necessary to distinguish between facial images of convicted persons, suspects, victims or other parties, such as witnesses. The necessity and proportionality of including facial images of victims or witnesses is unclear.

Recommendations

Against this background, the Meijers Committee recommends:

- to harmonise the definition of 'biometric data' that is used in the proposed Regulation with the definition in the Law Enforcement Directive and make an explicit reference in art. 4 (11) of the proposed Regulation to art. 3 (13) of the LED;
- to limit the scope of the proposed Regulation to serious offences by amending art. 2 of the proposed Regulation accordingly;
- to distinguish in Section 4 of the proposed Regulation between facial images of convicted persons, suspects, victims, in accordance with art. 6 of the LED;
- to refrain from designing a system for the exchange of facial images, revealing racial or ethnic origin without proper safeguards.

[6] See CJEU, Digital Rights Ireland and others, C-293/12 and C-594/12, §54-55.
[7] See also EDPS Opinion 4/2022 on the Proposal for a Regulation on automated data exchange for police cooperation ("Prüm II"), 7 March 2022, p. 10.