EUROPOL

The Hague, 07 May 2020

Joint Parliamentary Scrutiny Group Secretariat

To the attention of the JPSG Co-Chairs

By email only:
jpsg.libesecretariat@europarl.europa.eu

Europol reply to written questions from Mr Patrick Breyer, Member of the European Parliament

Dear Mr López Aguilar,

Dear Mr Ostojić,

In accordance with Article 4.2 of the JPSG Rules of Procedure and Article 51 of the Europol Regulation, Europol would like to respond to the question raised by the JPSG and European Parliament member, Mr Breyer, received by Europol on 9 March 2020, as follows:

Written questions by Mr Breyer:

- **Does Europol use software to recognize faces in video recordings?**

Europol uses face recognition software to facilitate semi-automated facial comparisons and identification of suspects from images and videos.

- **Who provides the software and what is its name?**

One facial recognition software that is being used at Europol has been developed internally with own resources and it is not commercially available. A second software, Griffeye Analyze DI Pro, developed and commercialized by the Griffeye company (www.griffeye.com), purchased by Europol via a framework contract with Safer Society Sweden AB, has facial detection and comparison features and is being used since Q3 2019 for supporting investigations related to online child sexual exploitation.

- **What is the rate of false positives and false negatives of this software?**

Europol is not relying solely on face recognition software for the identification of suspects, but rather uses the software as an additional tool to provide intelligence leads for suspects' identification. The system is able to compare images or stills from videos against Europol's dataset and potentially retrieve a number of potential matches for further assessment. Human assessment is always mandatory and carried out to ensure the reliability of the identification. Only a small number of specifically trained staff is authorised to conduct such assessments.

- **How many people (targets) were sought in this way in 2018, and how many of those people were matched?**

In 2018, the European Counter Terrorism Centre (ECTC) handled 1650 cases of facial recognition support requests about 1 or more suspects, resulting in 103 match results reported to Member States and Third Parties. In accordance with Europol's legal framework, any reporting to Europol's partners is subject to possible restrictions on the dissemination of the respective information, in line with the legal possibilities to transfer data and the instructions given by the data owner, required for in particular by Article 19 of the Europol Regulation. Europol does not perform forensic identifications, and facial comparison results are used merely as information for new lines of investigation.

Furthermore, the solution does not include an automatic check against any systems outside the Europol domain.

In 2018, the European Cybercrime Centre (EC3) has handled 13 requests for crosschecking facial similarities of suspects and victims related to ongoing investigations related to child sexual exploitation, all resulted with negative results.

- **What video material has the software been used on?**

In principle, every contribution addressed to ECTC by law enforcement partners from Member States or Third Parties that contains images or videos will be assessed using face recognition software. A significant part of Europol's video material consists of images extracted from videos containing terrorist propaganda stored in Europol's dedicated database.

EC3 has used the software to crosscheck based on facial similarities, images and videos sourced from investigations related to online child sexual exploitation.

I hope that these answers will prove satisfactory and remain available for further clarifications.

Yours sincerely,

Jürgen Ebner
Deputy Executive Director Governance