Dear EDPS Colleagues,

We are contacting you in relation to one of Europol's most successful operation in the area of serious and organised crime – the takedown of the Encrochat platform.

We would like to inform you about recent developments related to the investigation as well as ask for your opinion on a couple of pertinent questions.

Background of the investigation

The investigation involves a criminal organization that has set up a legitimate company to provide encrypted communications services (applications and devices) to other criminal organizations involved in a number of areas of serious and organized crime that pose a high security risk to EU MS and other countries. It is suspected that the company developed and disseminated encrypted communications services worldwide, offering them specifically to criminal organizations as a means of hiding and facilitating illegal activities. The investigation has revealed that this service had about 60,000 users globally. It is already clear from the information obtained that the criminal activities facilitated by these encrypted communication services include large-scale smuggling of dangerous drugs and serious violent crimes such as murders, kidnappings and tortures.

For the purpose of this investigation, a Joint investigation Team (JIT) is established by these two Member States (MS) to facilitate a direct information exchange between the participants. Europol and Eurojust are also formally associated to the JIT. Additionally, an Operational Task Force (OTF) has been set up at Europol to support JIT countries and other EU MS affected by the suspected criminal activities.

The main objective of the investigation is to establish the criminal liability of the organization that provided these communication services for the promotion of illegal activities. This includes the need to identify the users of these services and the nature of their illegal activities, as well as the criminal content of the communications.

The information collected within the framework of the judicial investigations is shared with Europol in accordance with the terms of the JIT agreement. This includes contents of the encrypted communications, as they are suspected to be related to criminal activities.

At Europol, the available information is processed in [redacted]. It is stored in the [redacted] environment. This information is extremely relevant for the prevention and investigation of organised crime posing a high security risk.

Europol has invested a large amount of resources for an extended period of time in order to manually search and evaluate the available information. The operational value of the encrypted communication is reduced over time. Therefore, Europol aims to process the available data as quickly and efficiently as possible. Due to the large number of encrypted messages, the complexity of networks and the difficulty of identifying and locating those involved in criminal activities, it is essential that analytical tools be used in the processing of data to enable action to be prioritized.

Phases of the investigation

The operation began with a **live-phase** during which the Member States intercepted criminal communications data related to organized criminal groups and networks. At this stage, the priority was to prevent crimes that pose an immediate threat to life and security and that had a direct impact on EU citizens. During the operation, a significant number of planned murders and other serious violent crimes were uncovered on a daily basis, a remarkable proportion of which were successfully prevented. During this phase, activities also focused on the distribution of dangerous drugs and other similar crimes that pose a concrete security risk and on the detection and identification of those involved in the acts.

During the current (post-live) phase of the investigation, Europol supports the evaluation of the contents of the communications linked to the Encrochat devices and the JIT countries have requested Agency's support for the following tasks:

- Assess, analyse and cross check the communications and their contents to support the JIT countries and other Member States in their investigations in detecting crime incidents posing an immediate threat to life or other type of high security risk and in detecting and identifying involved suspects
- Assess and analyse the communications and their contents to support the JIT countries in their investigations on the company which is suspected of providing encrypted communication services for the individuals involved in high risk organised crime incidents
- Assess and analyse the communications and their contents to support the JIT countries in their investigations in detecting and identifying persons suspected of the dissemination of the encrypted communication services and related devices
- Assess, analyse and cross check the communications and their contents to support the JIT countries and other Member States in their ongoing investigations on suspects involved in high risk organized crime activities

Europol's role in supporting this very high-profile investigation is key, given the amount of data to be evaluated (approximately 120 million messages) and the evaluation of data related to criminal activities taking place or having taken place outside the Member States currently involved in the investigation.

Our inquiry for your opinion is related to the post-live phase of the investigation.

Post-live phase of the investigation

As outlined in the Europol Strategy 2020 , Agency's key objective is the delivery of agile operational support to Member States, including high quality analysis. Encrochat case is in line with this goal.

To ensure it's capability, Europol aims at developing a solution to enhance Agency operational support and to meet the requirements which are based on the changing serious and organized crime. More specifically, Europol's goal is to develop a machine learning based model that assists Agency in identifying and prioritizing the decrypted communications which are linked to high risk crime incidents. The required functionalities of the model include at least the following:

a) Developing a machine learning model based on text or image to detect communications of persons that could be involved in high risk criminal activities such as assassinations, kidnappings and trafficking of dangerous type and/or large amounts of drugs
b) Clustering of chat messages, images and videos which could be linked to high risk criminal activities and extracting related entities to facilitate the detection of the networks and the assessment of the roles of the suspects
c) Enhancement of a machine learning model based on face extraction of images and videos to detect in a quick way in which chat messages the persons suspected of criminal activities might appear and link objects to suspects and so detect their travel patterns, contacts and other relevant activities
d) Speech to text translation and classification of audio files to facilitate the link between the messages and the right suspects

Examples of entities to be extracted are:

- Person information (first name, surname, and date of birth)
- Dates of criminal events
- Geographical information
- Means of transportation (license plate, flight number)
- Means of payment (bank account)
- Names of organisations

- Container numbers

Example of objects to be extracted are:
- People
- Firearms
- Vehicles and other means of transportation including vessels
- ID Documents
- Drug packages with logo
- Containers
- Monetary instruments

These entities will be extracted from chat messages and pictures in order to analyse data and discover links between them and with other information.

The pre-defined parameters of the algorithms will not include any sensitive personal data. Europol will define internally the parameters. The objective is not to process sensitive personal data and it will not be part of the 'extraction' criteria. However, we recognise that the produced results will contain sensitive data and it's processing will be in line with Europol Regulation. To manage the risks, Europol will ensure that the extracted data is subject to human validation and only after that it will be stored under relevant AP.

Question to be addressed:

Our inquiry relates to the development of these machine-learning models so that Europol can support ongoing investigations by Member States into a significant number of crimes that pose a high security risk.

Currently, the information is in the AP, through which Europol provides its operational support to JIT countries and other Member States. Therefore, the Agency's position is that the use of the algorithm is for operational and not scientific purposes. Furthermore, according to Preamble paragraph 50 of the Europol Regulation, the prior consultation mechanism "should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data and any substantial changes thereto".

Therefore, we would like to ask if you agree with Europol's position that the operational support described above does not fall within the scope of Article 39 of the Europol Regulation?

Given the high security risks posed by the criminal activities currently being investigated by the various Member States and the significant number of ongoing related investigations supported by Europol, we would be grateful for your timely feedback.

Thank you.