

The Hague, 21 October 2021

Joint Parliamentary Scrutiny Group (JPSG)
Secretariat

To the attention of the JPSG Co-Chairs

By email only:

jpsg.libesecretariat@europarl.europa.eu

Europol answer to written question from the JPSG delegation of the Swedish Parliament to the Joint Parliamentary Scrutiny Group (JPSG)

Dear Co-Chairs,

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 delegation of the Swedish Parliament, received by Europol on 24 September as follows:

Written questions from JPSG delegation of the Swedish Parliament to Europol – ahead of the JPSG meeting on 25-26 October 2021

In the opinion of Europol, what needs to be done in order to continue to be at the forefront as regards digital communication technology that can be exploited by criminals?

- Are new platforms and tools for cooperation needed at the EU level and/or in the member states?
- How can we prevent criminals from simply moving to other platforms or other technical solutions?
- Experience from the above-mentioned operations also shows that the EU member states have different legal and practical preconditions in this area.
- Does Europol see any problems regarding the differences between member states in being able to intercept and read communications on these platforms?
- Is there any risk that these differences will be exploited and that, for example, servers will be placed in member states whose legislation makes it more difficult to access these communication services, or that the differences between our legal systems are exploited in some other, detrimental, way?
- Does national legislation in the member states have an impact on which countries are able to participate actively in Europol-led operations in this area?

Page 1 of 3

Europol's answer

The digital transformation of societies including their economies and citizens lives is progressing fast and will continue to impact on all aspects of life. These developments also affect serious and organised crime and terrorism in the EU. Criminal activities are now consistently featuring online components, with digital solutions facilitating criminal communications.

There is a need to improve possibilities to tackle criminal content online, as well as the illegal exploitation of encryption and other new technology-related methods employed by criminals to avoid detection and hide their communications.

The Justice and Home Affairs Council Resolution from November 2020 with respect to the 10 Points on the Future of Europol, highlighted:

- In Point 6 that "Europol must be capable of harnessing the potential of technological innovation – for the benefit of national law enforcement authorities and for that of its own. This includes the development and use of artificial intelligence for analysis and operational support. ..."
- in Point 7 that there should be an effort for "Optimising the legal framework - The legal framework must ensure that Europol is able to fulfil its tasks in the best possible way. Europol must be – and remain – capable of working effectively in the virtual world and of processing large amounts of data. At the same time, a high level of data protection must be guaranteed. ..."

Accordingly, the proposed amendments to the Europol Regulation, currently in the co-legislation process, seeks to provide Europol with an enhanced legal basis.

Member States should 'jointly' invest in new tools to tackle criminal content online. The EU Innovation Hub for Internal Security at Europol provides a platform for pooling innovative approaches to respond to criminal activities in the virtual world.

Criminals seeking new ways to circumvent law enforcement measures represents a continuous risk profile, which requires to be addressed by enhanced EU cooperation and with global partners. Europol brings together a wide network of liaison officers in law enforcement, which is being further expanded based on business needs.¹ Recent highly successful operational activities show that the pooling of law enforcement efforts at Europol provides tangible added value to tackle cyber-related criminal activities for the security interests of Member States and beyond².

Europol cannot assess Member States' national legislation, however, from a law enforcement perspective, a common strengthened approach to tackle criminal content online increasingly becomes a necessary requirement for cross border investigations. Mutual legal assistance should be further facilitated, in particular regarding standard measures (e.g. subscriber identification) with a view to improving information exchange. The European Commission's initiative for law enforcement and judicial authorities to obtain cross-border electronic evidence,


¹ <https://www.europol.europa.eu/about-europol/statistics-data>

² <https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication>

which is in the legislative trilogue process since the end of 2019, could further promote cooperation in this direction.

I hope that this answer will prove satisfactory. Europol remains available for further clarifications.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'Alfredo Nunzi'.

Alfredo Nunzi

Head of Department "Institutional & Legal Affairs"
(Acting Deputy Executive Director of Governance)