Council of the
European Union

Brussels, 8 May 2023
(OR. en)

8534/23

LIMITE

COSI 89
ENFOPOL 228
CRIMORG 74
IXIM 121
CT 87
CATS 27
CYBER 117
TELECOM 136
JAI 583

NOTE

From:	Presidency
To:	Delegations
Subject:	Artificial intelligence from a law enforcement perspective

1. Introduction

COSI started discussing the opportunities and challenges of Artificial Intelligence (AI) for internal security at the informal VTC during the German Presidency on 13 July 2020 and agreed on its particular significance for law enforcement across the EU. The use of AI systems has potential to facilitate the work of law enforcement authorities, supporting and contributing to investigations, while at the same time these tools pose challenges in relation to fundamental rights. The discussion highlighted the need to establish trust in AI tools, and to identify appropriate governance and safeguards.

COSI has also considered the implications of the Commission's proposal for a Regulation on Artificial Intelligence (AI Act). Following the Justice and Home Affairs Council on 8 June 2021 where ministers discussed AI from an internal security perspective and called for a more detailed assessment of the impact of the proposed AI Act on the JHA sector, the Slovenian Presidency organised a discussion at the informal COSI meeting in July 2021 and a full-day online workshop in September 2021 to address the concerns of the internal security communities of the Member States regarding the proposed Regulation.

The draft AI Act is one of several horizontal digital files on a non-JHA legal basis and negotiated outside the JHA sector with important implications for the internal security of the EU and has thus remained of interest to COSI. From the Czech Presidency onwards, COSI has received regular updates on the status of digital files. During the COSI meeting of February 2023, the Presidency emphasised the need for Member States to consolidate their internal security positions and reflect them within other Working Groups, which becomes particularly important given the expected start of the trilogues on the draft AI Act in the weeks to come.

2. Europol’s practical support capabilities

Europol has developed and will continue to develop capabilities to support the law enforcement authorities of Member States in their efforts to have in place fundamental rights compliant AI tools. The agency also assists in flagging potential issues of common concern or interest to Member States. Some specific initiatives are outlined in this paper below and will be presented to delegations.

2.1 Europol sandbox environment

On 21-23 March 2023, the Europol Management Board adopted the “Binding document defining the general scope of the research and innovation projects.” Europol is creating now a technical sandbox environment in line with Article 33a of the Europol amended Regulation. The development of a Europol sandbox environment is intended to enable Europol and the Member States to develop, train and validate AI and machine learning models on operational data for operational purposes.

According to the findings of a study prepared for the Commission, the Europol sandbox environment might also play an important role in supporting the development of the envisaged EU Security Data Space for Innovation.

2.2 ChatGPT – The impact of Large Language Models (LLM) on Law Enforcement

In response to the growing public attention given to ChatGPT, the Europol Innovation Lab organised expert workshops to explore how criminals can abuse large language models such as ChatGPT, as well as how it may assist investigators in their daily work. Europol's innovation lab published a short report[1] in March 2023, describing a range of worrying potential criminal abuse cases.

The key findings suggest that LLMs such as ChatGPT can be abused by criminals for a number of crime areas, among them fraud and social engineering, disinformation and propaganda, as well as cybercrime and child sexual abuse, notably the online grooming of children. ChatGPT's ability to draft highly authentic texts on the basis of a user prompt helps generate criminal content at speed and at scale. At the same time, these types of models can facilitate the production of malicious codes for the purpose of cyberattacks even if the criminal has little technical knowledge.

Most of these models have integrated safeguards to prevent users from soliciting harmful content. However, a significant number of these can be circumvented easily through prompt engineering.

LLMs may however also offer some benefits to law enforcement agencies. These include supporting officers investigating unfamiliar crime areas, facilitating open-source research and intelligence analysis, as well as the development of technical investigative tools. The use of LLMs by law enforcement would, however, require a secure environment and thorough assessments with regard to safeguarding fundamental rights and mitigating potential bias.

Based on the findings, Europol recommends raising awareness among law enforcement authorities to understand the impact of LLMs on all potentially affected crime areas to be better able to predict, prevent, and investigate different types of criminal abuse. In addition, potential loopholes should be discovered and closed as quickly as possible. Europol is available to actively engage with the technology sector to ensure relevant safety mechanisms remain a key consideration and are constantly being improved.

Finally, law enforcement authorities could start developing the skills necessary to make use of these types of AI systems. This means not only building up knowledge on how to use these systems, but also to assess the content produced by generative AI models in terms of accuracy and potential bias.

[1] 8535/23

2.3 Accountability Principles for Artificial Intelligence (AP4AI)

AP4AI is a project led by Europol and CENTRIC within the EU Innovation Hub for Internal Security. The project has developed a comprehensive Framework for AI Accountability for Policing, Security and Justice which is operationally grounded and provides concrete support to practitioners at all stages of the AI lifecycle (design, procurement, deployment, modification, etc.). The AP4AI Framework available at www.AP4AI.eu is based on 12 Accountability Principles for AI use in the internal security domain, which have been developed and verified by internal security practitioners and validated by the consultation of more than 6,000 citizens in 30 countries (all Member States, UK, US, Australia). The ambition of the project is to contribute to the practical implementation of the future AI Act in the internal security domain.

In 2023, the Europol Innovation Lab has been organising a series of workshops where experts from Member States came together to validate a new web-based tool developed by Europol and CENTRIC. This tool aims to assist practitioners in self-assessing their compliance with the accountability principles, to identify areas for improvement, and ultimately enhance the ethical use of AI in their work. The beta version of the tool was launched on 23 March 2023 and is available to interested parties for evaluation. The tool is offered free to law enforcement agencies and will be translated into various EU languages.

3. Questions for discussion

1. What are the most important needs and requirements for your law enforcement authorities to develop, train and validate AI and machine learning models? In that regard, how do you assess the potential of the Europol sandbox environment?

2. Do you agree that there is a need for developing a common strategic approach to tackle the risks of criminal abuse of general-purpose AI systems such as large language models?

3. What other challenges related to the use of AI are your law enforcement authorities facing that might require attention at Union level?

4. Do you agree that the AP4AI framework could be used by law enforcement and other internal security and justice authorities as a common standard self-assessment tool to ensure the accountability of AI tools?

5. What useful practices/pilot projects/experiences could you share regarding the development of AI tools for law enforcement in cooperation with industry?