The Hague, 15 June 2020
EDOC# 1115091

EU Commission White Paper on Artificial Intelligence
[COM(2020) 65 final]

Europol contribution to the public consultation

1. Introduction

Europol welcomes the Commission's White Paper and the policy options presented therein on Artificial Intelligence (AI), and the aim of promoting a coordinated EU approach to the development of AI solutions as well as managing the associated risks. This contribution reflects the views of Europol and was fed by the input of several national police forces and partners.

For law enforcement one of the risks is the criminal abuse of AI, which poses a number of challenges and law enforcement needs to be in a position to address these risks. At the same time AI tools can significantly contribute to improving law enforcement activities by creating new ways of preventing and investigating crimes as well as by ensuring greater efficiency of operations.

Against this background, Europol however would see the need to expand on the law enforcement perspective in the Commission's White Paper on AI.

2. Important aspects for consideration from a law enforcement perspective

AI is an important tool for law enforcement and should also be considered a key enabling technology to ensure safety and security of citizens. From Europol's perspective, the facilitation of law enforcement use of AI deserves greater attention from the Commission in light of the benefits to the internal security that the deployment of AI tools can bring but also in terms of addressing the criminal abuse of AI.

The Commission does acknowledge that *"AI tools can provide an opportunity for better protecting EU citizens from crime and acts of terrorism"*. It is however unclear in what way the Commission's initiative and further work on this topic could facilitate this development. It is noted that law enforcement in general is framed as a risk in the White Paper. The Commission could clarify that AI is also an important asset for improving public safety and achieving the policy goals of the European Union (EU) in this area. Moreover, law enforcement should be seen as an important player in addressing some of the risks and challenges linked to the use of AI. As criminals start to abuse AI-based tools and services to endanger the life and well-being of European citizens, law enforcement needs to be empowered to adequately respond to these threats.

Risk-based regulatory framework

Europol notes that the risks highlighted in the White Paper mainly concern effects on the single market and threats to fundamental rights. Other types of risks to the safety and security of the Union, its businesses and citizens such as e.g. cyberattacks and attacks on critical infrastructure enabled by AI technologies should also be acknowledged. It is crucial to have a full picture of the threats the use of AI could pose to European societies.

In the White Paper, the Commission proposes a risk-based regulatory framework that would only cover areas that are considered high risk. The risk assessment

would be based on both the sector in which the AI tool is deployed and its specific area of use.

Europol would like to bring to the Commission's attention the fact that recent developments have shown how challenging it can be to identify certain sectors as high risk and others as low risk in advance. This is especially true with regard to a technology that is developing rapidly as is the case with AI. The level of risk associated with a specific use case should always be weighed against its potential benefits to the safety and security of the EU and its citizens.

On a general note, Europol would like to ask for caution in regulating a technology that is undergoing rapid development, as such regulation may unnecessarily limit its development and potentially stifle innovation. This would be unfortunate and may run contrary to the ambitions of the Commission.

Finally, harmonisation of the single market does not seem to establish an appropriate legal basis for regulating law enforcement activities. For all these reasons, Europol would kindly ask the Commission to consider the appropriateness of including law enforcement in the scope of any new regulatory framework.

Data governance

Data governance i.e. the management of the entire data lifecycle, which includes ensuring the quality, protection, availability, integrity, etc. of the data, lies at the heart of AI. For AI systems to produce meaningful results, high-quality and relevant data is a key requirement. Equally, it is necessary to have adequate controls and auditing mechanisms in place to ensure that the output produced by an AI system meets the required standards not just in terms of the purpose the system was designed for but also in relation to wider aspects such as data biases. This needs to be an ongoing process.

It is crucial to guarantee privacy and data protection at all stages of the AI system's life cycle. As such systems may infer individuals' preferences, age, gender or political views, the design of such systems and the data governance must include provisions to address any biases in the training data and to ensure that individuals have full control over their own data, and that data concerning them will not be used to harm or discriminate against them.

Data is an integral part of AI-based systems. It is required to train such systems and essential for learning purposes. AI systems continuously interact with the data encountered during operations. One can assume that the amount of data available will further increase, thereby providing better conditions for the training of AI tools. The ability to trace the data used for training and re-training purposes and for the continued development and decision-making ability of a deployed AI system is an important requirement to ensure accountability.

The 'black box' problem of AI systems means that the decision-making process may not be fully explainable or reproducible. In a criminal investigation, being able to recreate and trace such decision-making processes is critical. There must be clear requirements on businesses to include this kind of functionality. This requires further attention in the continued policy development.

For public actors to be able to ensure sufficient accountability and traceability of AI systems used, there must be clear requirements for transparency on the part of businesses when developing an AI tool for e.g. law enforcement purposes, including an appropriate data governance model.

Safeguards

Europol identifies the need for sound ethical, legal, privacy and data protection frameworks around AI, in line with the applicable legal framework to Europol and any EU-wide measures. A robust governance of AI is required in order to prevent

and identify any tampering with AI such as the manipulation of a particular algorithm or the training process and/or the data sets used for training purposes.

The continuous human involvement and supervision in training and retraining AI algorithms is paramount. In the same vein, the European law enforcement workforce needs to adapt to the challenges posed by AI, including the adaptation of its learning and training programmes to the specific need for a multi-disciplinary approach to using AI.

It is self-evident that all law enforcement AI systems and tools need to be well-protected from malicious actors. This includes attacks against AI systems, data manipulation, training data 'poisoning' and other attempts to manipulate the functionality of such systems.

Law enforcement should address potential negative aspects such as the criminal abuse of AI, building on ongoing efforts to ensure that AI is trustworthy, i.e. lawful, ethically adherent and technically robust.

Capacity building and knowledge

Capacity, expertise and knowledge among concerned stakeholders of the risks and benefits of AI technology must increase among law enforcement as well as citizens in general. This should include supervisory authorities to ensure that they are in a position to supervise the use of AI tools by public actors, including law enforcement.

3. Conclusion

Europol kindly asks the Commission to consider taking a holistic view of law enforcement and AI, and the benefits AI can bring to the internal security of the EU. To this end, the Commission could consider including the use of AI for law enforcement purposes as an important dimension.

In line with the Commission's White Paper and to mitigate the challenges and benefit from the opportunities of AI in law enforcement, a coordinated EU approach would be required to avoid fragmentation. A European regulatory framework would therefore be appreciated.

Europol stands ready to support the Commission's efforts in encouraging the development of AI capabilities for the European law enforcement community and at the same time manage and minimise the risks, without disproportionately limiting the development and use of AI that could substantially contribute to the safety and security of the EU and its citizens.