Council of the European Union

Brussels, 31 May 2021
(OR. en)

9096/21

LIMITE

COSI 107
ENFOPOL 207
CYBER 167
DATAPROTECT 147
IXIM 100
COPEN 253
JAI 652

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Permanent Representatives Committee/Council |
| Subject: | Artificial Intelligence: internal security outlook<br>- Presentation by the Commission and exchange of views |

## Introduction

Artificial intelligence (AI) is a fast evolving family of technologies that can bring a wide array of economic and societal benefits. By improving prediction, optimising operations and resource allocation, and personalising service delivery, the use of AI can provide key competitive advantages to companies and the European economy in a wide range of sectors. However, while the use of AI can do much good, some of its uses and applications constitute interference with the fundamental rights of individuals concerned and may also cause harm. One of the objectives of the recently published **Commission proposal for a Regulation on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)**[1] is to ensure a trustworthy use of AI through categorisations of prohibited systems/uses (with certain exceptions for law enforcement), a set of requirements and obligations for systems regarded as high-risk and a relevant compliance framework.

[1] COM(2021) 206 final

At the same time, several Member States are calling for **strategic autonomy and digital leadership of the EU,** and reminding of the need to strike a reasonable balance between inherent risks of AI products and their use, in particular on the fundamental rights and freedoms of individuals guaranteed by the Charter and, at the same time, new opportunities for innovation. A position paper[2] issued by 14 Member States in October 2020 reminded that a European AI approach should be balanced, taking into account the opportunities and potential AI provides in different sectors. Furthermore, the countries reminded that *"serious risks cannot solely be determined by the sector and application in which the AI application is used"* since there is a risk that this kind of an approach would likely categorise too much AI as serious risk. Instead, those Member States consider that the risk assessment should be qualified by both the potential impact and the probability of the risks.

The **AI Proposal (Annex III) lists eight sensitive areas**, three of which are relevant for internal security (Biometric identification and categorisation of natural persons; Law enforcement; Migration, asylum and border control management). Only those AI applications that are listed in the AI proposal under these eight sensitive areas are considered high risk. This has the consequence that the very same AI applications qualifying as high risk when used by law enforcement authorities would not be high risk when used by the private sector, unless they fall under any of the sensitive areas and are listed in Annex III. The specific high-risk AI applications listed in Annex III could be amended by virtue of delegated acts by applying the pre-defined methodology and criteria as defined in Article 7 of the proposal.

[2] Innovative and trustworthy AI: two sides of the same coin. Position paper on behalf of Denmark, Belgium, the Czech Republic, Finland, France, Estonia, Ireland, Latvia, Luxembourg, the Netherlands, Poland, Portugal, Spain and Sweden on innovative and trustworthy AI, 8 October 2020.

**Prohibition of (the use of) "real-time" remote identification systems**

Article 5 prohibits, on fundamental rights grounds, certain AI systems (manipulation of human behaviour; exploitation of information to target vulnerabilities; and social scoring). By consequence, other AI systems may be used, under certain conditions, according to a proposed set of classes. Whilst AI systems for "real-time" and "post" remote biometric identification (RBI) of natural persons are classified as high-risk systems in Article 6(2) and Annex III, and thus usable as long as the ensuing requirements are followed, the *use* of "real-time" RBI systems in public spaces *for the purposes of law enforcement*, such as the use of "real-time" facial recognition tools, **would be prohibited as a principle,** due to the heightened risks for the rights and freedoms of the persons concerned. There are **specific exceptions to this ban**, however, and they can be categorised in three groups: situations that involve the search for specific potential victims of crime (e.g. a missing child case); prevention of a specific, substantial and eminent threat to the life or physical safety of natural persons or of a terrorist attack; and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA[3]. Furthermore, **each individual use would be subject to a prior authorisation** granted by a judicial authority or by an independent administrative authority of the relevant Member State, unless the case were categorised as urgent[4].

[3] If those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State.

[4] In a duly justified situation of urgency, the use of the RBI systems could be commenced without an authorisation and the authorisation could be requested only during or after the use.

It will be important to assess **how proportionate banning the use of real time RBI systems for law enforcement purposes** in publicly accessible spaces would be, and how well it would respond to the risks evaluated to be inherent to this specific use, especially when uses for other purposes are allowed provided that they are covered by one of the exceptions established by Article 9(2) GDPR[5]. It is also essential to ascertain that the exceptions to the prohibition respond to realistic situations where the importance of the substantial public interest, such as a missing child case, can be seen to outweigh the risks inherent to the use.

**High-risk applications for JHA in general and law enforcement in particular**

In addition, it is envisaged that the degree of interference with fundamental rights serves as one of the **criteria to assess the potential harm that an AI system could cause**, to qualify it as a high-risk system. According to the draft Article 6(2), stand-alone high-risk AI systems are listed in Annex III. A variety of law enforcement tools used for example for risk assessment, polygraphs, detection of deep fakes, evaluation of reliability of evidence, prediction of the occurrence or reoccurrence of a criminal offence, profiling and crime analytics is listed as high-risk. Similarly, tools assisting migration, asylum and border control authorities are listed. Where an AI system is deemed high-risk, providers and, to a more limited extent, users (together: operators) would have to follow **clear obligations.** These would mostly need to be applied prior to putting the system for the first time on the EU market and include requirements relating to the quality of training and testing data, documentation and record-keeping, transparency, human oversight, product safety, accuracy of outputs and cybersecurity, as well as the need to register each AI system in a Commission-managed database (with specific exceptions and confidentiality rules in the field of law enforcement). The proposal also includes a general obligation for providers to put in place a quality and a risk management system.

[5] The exception provided by Article 9(2) GDPR includes processing of sensitive data when the processing is necessary to protect the vital interests of the data subject or of another natural person, processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law, the data was made explicitly public by the data subject or processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, medical diagnosis, etc.

At national level, Member States would have to designate one or more national competent authorities and, among them, the national supervisory authority, for the purpose of supervising the application and implementation of the proposed Regulation. In so far as the high-risk systems are used for law enforcement, migration, asylum or border control purposes, Member States are obliged to designate as market surveillance authorities for the purposes of the AI Regulation either the competent data protection supervisory authorities or the national competent authorities supervising the activities of law enforcement, immigration or asylum authorities putting into service or using those systems. It is important to note that certain systems and tools of the JHA Agencies would also fall in the scope of the proposed Regulation and the categorisation of certain systems and tools as high-risk will thus also affect them, for example Europol in relation to certain crime analytics tools, Frontex in the border security context, or if EASO develops asylum management tools using AI. The European Data Protection Supervisor (EDPS) would act as the competent independent authority for the supervision of the Union institutions, agencies and bodies when they fall within the scope of the proposed Regulation.

The **detailed implications of such a range of law enforcement tools**, including some of those used at the JHA Agencies, becoming listed as high-risk should be closely assessed. It will be particularly important to evaluate whether these requirements covering so many types of essential law enforcement systems could turn into an obstacle that, in practice, may prevent or at least render more difficult both private sector involvement in the innovation and provision of relevant solutions and public sector development of these tools in the future. The EU Innovation Hub for Internal Security could foster the dialogue with the industry including on the implications to research and development in this specific field. As part of this assessment, the positive benefits of the Regulation should also be considered, notably the objective to increase public trust and acceptance and to render the design and use of those high-risk AI systems compatible with the existing high standards for accountability.

It is essential to ensure that we are not unnecessarily limiting the development and use of technological development at a stage where we are not yet aware of the actual impact of such limitations. Even the exceptions and obligations mentioned in the high-risk categorisation may not be realistic and feasible at operational level, requiring first a full understanding of their implications. The respect for the fundamental rights and freedoms of individuals is essential, but the use of AI should be practical, useful and improve the efficiency with which law enforcement authorities work, always keeping in mind that criminals do not follow any type of restrictions in achieving their goals.

**Other relevant issues**

Certain specific issues, such as the implications of the high-risk categorisation of certain AI systems that are **components of large-scale IT systems in the JHA area** managed by eu-LISA[6], should be studied more closely. Similarly, it is necessary to evaluate the effects on the use of JHA large-scale IT systems as well as on (automated) data exchange in the EU, for example under the auspices of the Prüm framework, including the foreseen future inclusion of facial images. It is important to consider all relevant phases of the process (the collection, comparison, exchange, post-processing and analysis of data) when AI systems within the scope of the proposed Regulation are concerned.

The **temporal aspect of the proposal** is also relevant. AI applications to be listed as high-risk currently in use by law enforcement authorities, or in use by the date of application[7], would not be captured in the scope of the proposal[8]. In relation to AI systems that are components of large-scale IT systems in the JHA area managed by eu-LISA, the date of application is one year after the general date of application (with 2 years of transitional period after entering into force), unless there are significant changes to those components based upon a legal amendment. Though the implications for current or mid-term use and development of those systems or their components would be limited, it is highly likely that any new developments in the overall JHA information architecture would need to be evaluated from a different perspective.

---

6 eu-LISA is responsible for the operational management of Eurodac, the SIS and the VIS. Regulation (EU) 2018/1726 furthermore entrusts the agency with the development and running of the EES, the ETIAS and the ECRIS-TCN.

7 24 months after the date of entry into force of the Regulation.

8 Unless significant modifications are made to them after the Regulation becomes applicable.

**Conclusions**

The provisions on the prohibitions (Article 5) and on the classification of certain AI systems as high-risk and the ensuing requirements (TITLE III) are critical for the protection of fundamental rights, but **these limitations and safeguards should be in balance with the possibilities of law enforcement authorities to use and develop AI systems** in the future, in line with the rest of the society. The objective should be to equip law enforcement authorities with appropriate modern tools to ensure the security of citizens, with applicable safeguards in place to respect their fundamental rights and freedoms.

Accordingly, it is important that **the security and criminal justice sectors should not be stalled in their ability to innovate and use products** that are the result of latest technological development. One of the main objectives of the Commission proposal is to foster the development of safe and lawful AI that respects fundamental rights across the Single Market, by both private and public actors, aiming to provide for a text that can withstand legal challenges before the Court of Justice. It is particularly demanding to strike the right balance between this important objective, the fundamental rights and freedoms of individuals and the needs of law enforcement authorities to perform their legitimate primary duties of providing security and maintaining public order, but also the need to respond to the challenge of limitless exploitation of technological development in the criminal underworld. Providing possibilities for all relevant sectors of the society, including those whose use of AI may be seen categorically as high-risk, to exploit the latest developments in technology is going to be one of the critical points - and success factors - of the proposal. If the AI Regulation were to become, in time, a global example of a coherent and consistent cross-sectoral AI legislation, it is even more important to get this balance right at the outset.

It is important to categorise the AI systems in terms of **degree of risk based not only on their users or the relevant sector in which they are used, but also on a thorough analysis of the overall implications,** especially in the online context where similar tasks can be bestowed upon both public and private actors. A strictly evidence - and information - based approach is needed to evaluate inherent risks - and their potential impact.

The precise effects of a horizontal proposal of such diverse and significant implications, including of the law enforcement relevant use cases listed in Annex III as high risk, should be evaluated in detail. A **sectoral impact assessment for JHA** could support a better understanding of the practical implications for JHA and the security chain processes in particular, considering their specificities.

**Questions to ministers:**

- What is your preliminary assessment on the impact of the relevant parts of the proposed Regulation regarding law enforcement use of AI tools in the future?
- Are you satisfied with the overall impact assessment or would you like to see a more detailed assessment of the critical implications for JHA in general and law enforcement in particular?