Council of the European Union

Brussels, 12 May 2021
(OR. en)

8515/21

LIMITE

COSI 94
ENFOPOL 187
CYBER 143
DATAPROTECT 126
IXIM 84
COPEN 225
JAI 536

NOTE

From:	Presidency
To:	Delegations
Subject:	High risk AI applications: internal security outlook - Exchange of views

Delegations will find in Annex an outline of a paper that the Presidency intends to use as a basis for the exchange of views of Ministers at the June Council. The topic of the exchange of views is Artificial Intelligence (AI) applications from an internal security perspective in light of the recent Commission proposal for a Regulation on Artificial Intelligence[1] and Commission communication fostering a European approach to Artificial Intelligence[2].

The examination of the Proposal will be handled in the competent Working Party (TiS).

Delegations are invited to express their views on the issues raised as well as to indicate any other aspects or relevant points that should be brought to the attention of the Ministers from the internal security and home affairs community perspective.

1 COM(2021) 206 final
2 COM(2021) 205 final

To feed into the preparation of this item for the Council, delegations are also invited to address the following specific questions:

- What is your first assessment of the relevant parts of the proposed Regulation especially on law enforcement use of AI tools in the future? Which are the most relevant points to be raised to the Ministers for the exchange of views in June?

- According to article 5(1)(d), (2), (3) and (4), how do you assess the impact of the regime envisaged for the use of "real-time" remote biometric identification (RBI) systems for law enforcement purposes, notably the prohibition subject to specific exceptions taking into account the risks of such systems for fundamental rights and freedoms of the concerned persons?

- Based on article 6(2) and Annex III, what is your first assessment of the implications of the compliance regime established in Chapter 2 to which many AI tools used by law enforcement would be subject in the future being considered high-risk applications?

ANNEX

High risk AI applications: internal security outlook

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 Artificial Intelligence[3] is to ensure a trustworthy use of AI through categorisations of prohibited systems/uses (with certain exceptions for law enforcement), definitions and standards for systems regarded as high-risk and a relevant compliance framework.

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 fundamental rights and freedoms of individuals guaranteed by the Charter and, at the same time, new opportunities for innovation. A position paper[4] 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.

---

3 COM(2021) 206 final

4 INNOVATIVE AND TRUSTWORHTY 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

This sensitive balance is highlighted in article 5 which 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[5]. 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[6].

It will be important to assess how proportionate banning the use of RBI systems for law enforcement purposes 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 not considered as problematic. It is also essential to evaluate how well 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.

---

5 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.

6 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.

High-risk applications for law enforcement

In addition, it is envisaged that the degree of interference with the 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. Where an AI system is deemed high-risk, providers and users (together: operators) would have to follow an extensive range of obligations. These include requirements relating to the quality of training and testing data, documentation and record-keeping, transparency, human oversight, product safety, accuracy of outputs and security, as well as the need to register each AI system in a Commission-managed database. The proposal also includes a general obligation for providers to put in place a quality and a risk management system.

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. 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, or FRONTEX in the border security context. 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 private sector involvement in the innovation and 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.

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[7], 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 (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[8], would not be captured in the scope of the proposal[9]. 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, unless there are significant changes to the systems. 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.

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 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.

---

7 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.

8 24 months after the date of entry into force of the Regulation.

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

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.