Council of the European Union

Brussels, 7 September 2021
(OR. en)

11573/21

LIMITE

ENFOPOL 312
COSI 166
IXIM 168
CT 118
TELECOM 332
JAI 956

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	CM 4103/21
Subject:	The proposed AI Regulation Relevant themes to explore at a JHA/law enforcement workshop

At the JHA Council in June and at their informal meeting in July, Home Affairs Ministers called for a more detailed assessment of the impact of the proposed AI Regulation on law enforcement activities. This was also echoed by delegations at both the May COSI meeting and the July informal meeting of COSI. In order to respond to this call, a JHA/law enforcement-themed online workshop will be organised to address the questions and possible concerns of the Member States and their relevant communities.

A thematic JHA/law enforcement online workshop will be organised together with the TELECOM experts on 30 September 2021 to clarify the implications of the proposal. The workshop will be addressed in particular to the COSI, IXIM, LEWP and TWP communities.

The main objective of the JHA/law enforcement workshop will be to identify and address those issues in the proposed AI Regulation that are the most central for the JHA sector and in particular for the internal security, including criminal justice, communities. There has been a clear call to better understand the short, medium and long term implications of the proposal and especially of some of its key aspects (e.g. the prohibition of real time remote biometric identification in public places for law enforcement purposes and of the use cases outlined in Annex III many of which are law enforcement relevant) on JHA/law enforcement activities before the national positions on the proposal on the whole are consolidated.

Further to CM 4103/21, delegations will find attached in Annex I the list of the themes and specific questions updated by Member State contributions. This list will be used as the basis for the online workshop taking place on 30 September 2021.

ANNEX I

RELEVANT THEMES TO EXPLORE AT A JHA/LAW ENFORCEMENT WORKSHOP ON THE PROPOSED AI REGULATION

Internal market and competitiveness aspects

- What is the concrete impact on the industry and especially on the European SMEs that develop and provide these tools, often tailored for specific purposes? How can we guarantee that the EU continues to be able to resume product development, so that updates to existing systems, and innovation of new products, will remain possible, in line with the requirements of the proposed legislation?

- How much and to what extent would in-house development or the commercial development of tailor made systems of high-risk systems for law enforcement be impacted?

- To what extent is the market for these products and services affected in the mid and long term?

Legal aspects

- To what extent is the legal basis of the proposal - Article 114 - sufficient to regulate AI uses, including bans and exceptions thereof for matters that fall under Title V, TFEU? How the issue of variable geometry is resolved when it comes to Schengen and non-Schengen relevant matters?

- What is the impact of the proposal, when it comes to AI applications for national security purposes? Are the national security services affected by the biometric identification ban in art 5 (d)? Are they affected under the applications considered high risk in Annex III?

- What exactly does the notion of "prevention of a terrorist attack" referred to in article 5 (d) of the Regulation refer to?

- Would the differences between the public and private sectors justify a separate regulatory framework for the use of AI systems by law enforcement, or a specific Title in the proposed Regulation?

- Exceptions for real-time RBI for other uses than law enforcement are according to the Commission regulated by the GDPR. Are these exceptions similar or indeed wider than the exceptions provided for law enforcement use (for example the child kidnap cases) in the proposed Regulation, taking into account the relevant purposes and availability of formal safeguards and redress?

- Are the exceptions outlined in the proposal on real-time RBI in public spaces used for law enforcement purposes sufficient/realistic? Should for example real-time RBI in certain security-sensitive public spaces[1] be limited to the objectives listed in Art. 5(2)(d)?

- When granting authorisation by a judicial authority or by an independent administrative authority, is it necessary to take into account temporal, geographic and personal limitations pursuant to Article 5 (2) or would it be sufficient only to assess necessity and proportionality of the use of such system in each individual case?

- Should it be possible that modalities of authorization of the use of AI systems by judicial or administrative authorities are further specified by national law, in line with highly intrusive measures (such as a bodily search)?

- AI used for law enforcement is qualified as high risk in general. At the same time, the same AI applications used by the private sector are not. How this is justified and to what extent this approach provides the necessary legal certainty?

- With regard to existing national and European obligations, would it not be relevant to take stock of existing legislation in particular on data protection and conduct an analysis of the draft regulation on AI in relation to the European legal framework (directive 2016/680) to identify shortcomings in advance?

[1] E.g. parts of airports, see paragraph 150 of judgment in cases C-511/18 and C-512/18.

- Are there sufficient safeguards in the proposal to guarantee the exercise of the right to an effective remedy (Article 47 of the Charter) in the context of AI applications used by law enforcement? How can we improve the legal guarantees in this regard?

- Does the proposal provide for the elimination of bias in AI tools and their discriminatory impact regarding law enforcement use? How does the proposed legislation achieve this goal?

- To what extent will it still be possible (for national governments) to set up additional rules and/or standards for AI in law enforcement in the national context? For example, one can imagine that certain AI tools used in the context of criminal cases need to adhere to additional – national - quality standards relating to how evidence is viewed, when used to obtain evidence.

- To what extent will it still be possible for national governments, as clients in tender procedures, to introduce additional requirements or standards for a high-risk AI system, beyond the requirements of the AI proposal or the standards that emanate from this Act?

- To what extent will it be possible for Member States to create or maintain national transparency obligations?[2]

- To what extent will it be possible to create more precise exceptions regarding transparency for law enforcement (Article 52)? For example, could the national legislator stipulate that any exception that is made possible in Article 52 ceases to exist when the interests of law enforcement are no longer at stake or when another interest (for instance for fair trial) trumps this interest?

- To what extent will it still be possible to regulate systems that are not high risk according to the AI proposal?

---

[2] Either from another point of view than human dignity (for instance accountability) or to offer stronger protection of human dignity (e.g. transparency obligations for other use cases than those already covered in article 52 or the introduction of rights for persons subjected to a certain use case).

Practical law enforcement aspects

- What are the actual practical implications of the law enforcement relevant use cases listed in Annex III? Which concrete tools would be in the scope and affected? Could you provide real case examples for the listed use cases? Would for example a system, which on the basis of input data and fixed algorithms identifies certain persons as potential reoffenders while it conducts tasks clearly defined by humans without the possibility for self-judgement or self-modification, be considered a high-risk system?

- Future criminal uses of AI will by definition not be subject to any limitation, hence the risk of creating a situation of imbalance between the relevant authorities and their objectives, if their capacity for innovation were hampered and investors dissuaded from funding high-risk applications. What solutions can be considered to minimize this risk?

- The AI proposal narrows down the definition of law enforcement to activities focused on criminal offenses or criminal penalties and excludes administrative proceedings by, for example, tax and customs authorities. What is the reason for this and what is understood under the term administrative proceedings? Which organisations would then fall under the defined definition of law enforcement? For example, some authorities in some Member States are not specifically focused on law enforcement, but do contribute to the field in a more indirect way. Examples are tax and customs authorities, child protective services, etc.

- By default, law enforcement is not allowed to share any operational data with external providers. Would you agree that in these cases the obligations that now rest upon (commercial) external providers, like monitoring, should be executed by the user?

- To what extent will there be a possibility of an exception to publication of high risk AI tools in the EU AI Dashboard, in cases where the publication at that moment will hinder a criminal investigation or endanger people?

- If law enforcement authorities exchange in-house made applications among each other and some law enforcement authority users make changes in the application, or retrain parts of the application (e.g. with transfer learning), who is regarded as the provider? On whom would the obligations of the provider rest in the cases where law enforcement authorities use AI Systems that are based on open source code?

- Are law enforcement authorities required to get a CE marker, when in-house products are not put on the internal market? The current proposal does not differ between in-house and commercial use.

- Is it possible that law enforcement authorities have their own AI regulatory sandboxes? Would a shared development environment for EU law enforcement authorities (e.g. for machine learning applications, including specific law enforcement authority data) be considered an AI regulatory sandbox and what authority would oversee this?

- To what extent do law enforcement authorities need to comply with the AI proposal when experimenting or when they do pilots with AI Systems?

- If the onus on the conformity process regarding high-risk applications is on the provider, and the systems are tailored and produced in cooperation with the user, such as complex crime analysis systems, will some of the requirements in practice however fall on the user, i.e. Europol or a national competent authority?

- To what extent does the conformity process regarding high-risk applications duplicate existing procedural safeguards provided by the criminal justice system?

- Will the exclusion of international law enforcement cooperation from the scope of the proposal create a bias that will actually prevent some forms of cooperation with the competent authorities of third countries or with Interpol? Will this create an uneven footing or further discrepancies btw the EU and the rest of the world in relation to for example the use of high risk AI applications in law enforcement work?

Information systems and information exchange aspects

- Which are the AI components of large-scale IT systems that are included in the scope?
- What will be the legal and practical impact on existing large-scale EU information systems (SIS and the national information systems feeding it, VIS, EURODAC, etc.) or on those to come (EES, ETIAS, ECRIS-TCN) as well as on their interoperability? To what extent will interoperability framework be affected especially in the medium to long term?
- How probable is it that there would be changes to the interoperability framework in the short run that would put these changes in the scope of the proposed Regulation?
- How will the exchange of data collected while using AI by law enforcement authorities be regulated, both between the competent national authorities of Member States, as well as with third countries and organizations, e.g. Interpol? Will there need to be some practical changes in the information exchange processes?