Council of the European Union

Brussels, 29 October 2021
(OR. en)

13329/21

LIMITE

ENFOPOL 383
COSI 193
CRIMORG 90
IXIM 207
CT 138
CATS 67
CYBER 268
TELECOM 398
JAI 1149

NOTE

From:	Presidency
To:	Delegations
Subject:	Report on the JHA/law enforcement online workshop on the proposed AI Act (AIA)

Delegations will find attached the report from the JHA/law enforcement online workshop on the proposed AI Act (AIA) organised by the Slovenian Presidency on 30 September 2021.

Report on the JHA/law enforcement online workshop on the proposed AI Act (AIA)

30 September 2021

Report on the JHA/law enforcement online workshop on the proposed AI Act (AIA)

30 September 2021

SUMMARY AND MAIN CONCLUSIONS

The Slovenian presidency organised a full-day online workshop at expert level to address the remaining concerns raised by the law enforcement and internal security communities of the Member States regarding the proposed AI Act (AIA). The Commission services experts present at the workshop (hereinafter "the Commission") had prepared specific presentations to explain in detail, on an informal basis and without articulating a formal Commission position, the AIA, its approach and impact on the JHA area. The workshop was organised around six thematic clusters to respond to the questions submitted by the Member States outlined in document 11573/21: a general presentation of the AIA (including the AI definition); the legal issues of the AIA; the impact of the proposal on the security market and in-house innovation; high-risk AI applications; biometrics; and large-scale IT systems. Each presentation was followed by a Q&A session where the Commission replied to the questions raised.

Member State representatives highlighted three key issues:

- **the broad definition of AI that can lead to the labelling as AI of systems/applications that are arguably not considered AI;**
- **the actual impact on the JHA area of procedure and cost and availability of products and services in the high-risk categories, including impact on the product development of SMEs in this particular industry; and**
- **the restrictive approach to the use of AI systems for law enforcement purposes, in particular with regard to the use of real-time RBI in publicly accessible spaces.**

The Commission explained that a sectoral approach to JHA was not chosen since AI is often used across sectors and the Commission's objective is to regulate the whole AI market. In addition, it was assessed that the JHA sector would face broadly the same AI-related challenges as other sectors (opacity, complexity, data dependency etc.), although it is admittedly exposed to specific risks.

As regards the legal basis, the Commission underlined that Article 114 TFEU is the correct legal basis, since the AIA aims to regulate the internal market. However, this is complemented with an additional legal basis for the prohibition laid down in Article 5(1)(d) of the AIA on the use of real-time remote biometric identification (RBI) in publicly accessible spaces for the purposes of law enforcement. This article is based on Article 16 TFEU on personal data protection, and specifies the rules on the processing of biometric data contained in Article 10 of the Law Enforcement Directive (LED, 2016/80).

Member State representatives enquired about the scope of the AIA concerning systems used for national security purposes. The Commission recalled that under Article 4(2) TEU "*national security remains the sole responsibility of each Member State*". Therefore, a national intelligence agency developing its own AI device for national security purposes would not fall under the scope of the AIA. Nevertheless, if the AI device is for instance sold by a private provider to a State, the regulation would apply to the activities of the private provider who places the system on the market.

Concerning the impact of the AIA, Member State representatives requested more detailed information since in their view the cost assessment underestimated the actual costs in relation to the heavy procedure introduced. The Commission stressed that the current legal framework already imposes many demands on the JHA sector, both at the European and national level. Therefore, additional compliance costs introduced by the AIA would be lower for law enforcement users and providers.

High-risk AI systems covered by the AIA are listed in Annex II and Annex III of the proposal, but Member State representatives raised several questions in relation to concrete types of systems that would be covered. For instance, they enquired whether fuzzy search algorithms (approximate search), colour and shape recognition applications or deep fake recognition tools would be classified as high-risk. The Commission clarified that traditional database querying applications would in many cases not fulfil the AI definition and would thus not fall within the scope of the regulation.

According to the Commission the prohibition of the use of real-time RBI in publicly accessible spaces for the purpose of law enforcement is aligned with and specifies the existing legal framework on data protection. The AIA rules bring legal certainty and will enable the use of this technology under specific conditions and safeguards when this is strictly necessary and proportionate. Moreover, Article 5(1)(d) does not prohibit the *ex post* use of RBI.

The Commission highlighted the risks posed by the use of real-time RBI in publicly accessible spaces for law enforcement purposes, considering it a particularly intrusive tool because of the immediacy of its impact and also because it may evoke feelings or perceptions of constant mass surveillance. Such risks are considered unacceptable and the use of such systems is therefore prohibited, except in limited particular situations. Member State representatives recalled that Article 10 LED currently enables Member States to legislate on the use of RBI in public spaces on a broader range of situations than what the AIA provides for. For example, it could be used to identify witnesses of serious crime in order to investigate and to protect them. It would be important to understand why such cases are excluded in the AIA.

Despite the detailed explanation by the Commission, several Member State representatives expressed their concerns and found the proposal restrictive and not in line with the practical needs of law enforcement, especially when it comes to future innovation and taking into consideration the limitless technological development exploited by organised crime. The Commission stressed that it had carefully balanced the need for safety and security against the fundamental rights considerations and in particular the rights to privacy and protection of personal data, in line with Articles 7 and 8 of the Charter of Fundamental Rights. The Commission also underlined that Article 5(1)(d) AIA only applies to real-time biometric identification, a technology that currently appears rarely used by law enforcement authorities and for which most Member States do not have the legal basis required by Article 10 LED.

Page 2

Furthermore, a Member State representative raised concerns related to the harmonisation effects of the AIA and requested the Commission to further assess whether law enforcement needs would be sufficiently safeguarded. The Commission replied to the questions posed and offered a possibility for bilateral discussions to provide further clarification and to address specific concerns especially in relation to the assessment of concrete AI applications and whether they would fall under the high-risk use cases and the question on the harmonisation effects of the AIA.

In conclusion, the Chair urged Member States to take into account the concerns of the law enforcement and internal security communities when formulating national positions. The main objective is to find a balance between respect for fundamental rights and law enforcement needs. The two core values in question, security and freedom, should not be seen as conflicting but complementary and interdependent. The Chair reminded of the importance of Member States bringing relevant concerns to the negotiating table in the Telecom working party leading the negotiations on the AIA.

1. WORKSHOP INTRODUCTION

The Chair introduced the objective and background of the workshop. The Home Affairs Ministers had called for a more detailed assessment of the impact of the proposed AI Act (AIA) on law enforcement activities at the JHA Council in June and at their informal meeting in July. The call was echoed by delegations at both the May COSI meeting and the July informal meeting of COSI. In order to respond to this call, the Slovenian Presidency organised this workshop to address the questions and possible concerns of the Member States and specifically their relevant law enforcement communities.

The Commission had prepared specific presentations to explain in detail the AIA and its impact on the JHA field and to address the specific questions from the Member States outlined in document 11573/21 as well as posed *ad hoc* in the workshop. Six thematic clusters were presented to cover the issues outlined by the Member States: a general presentation of the AIA (including the AI definition); the legal issues linked to the AIA; the impact of the proposal on the security market and in-house innovation; high-risk AI applications; biometrics; and large-scale IT systems.

2. GENERAL PRESENTATION OF THE AIA

The Commission provided a general overview of the AIA with a focus on the JHA field in general and law enforcement in particular. The aim of the AIA is to propose harmonised rules on AI applications, with an approach shaped by EU values and based on risk assessment. The appropriate balance between the protection of fundamental rights and public safety is a key aspect of the proposal. It supports the objective of making the EU a world leader in the development of safe and trustworthy AI. The proposal allows for regulation that is appropriate to address the specific characteristics of AI systems that surface across sectors, proportionate and centred on a risk-based regulatory approach. One objective is to avoid creating unnecessary restrictions, but to take into account situations that carry high risks to fundamental rights and safety or could generate such risks in the near future.

The Commission outlined that a main objective of the AIA is to ensure the proper functioning of the internal market by setting harmonised rules on the development, placing on the market and the use of products and services making use of AI technologies or provided as stand-alone AI systems in the European Union. These rules are applicable horizontally across all sectors and not specific to law enforcement. For this reason, Article 114 TFEU is the appropriate legal basis for the proposal. However, considering that the proposal contains certain specific rules on the protection of individuals with regard to the processing of personal data, notably restrictions of the use of AI systems for real-time RBI in publicly accessible spaces for the purpose of law enforcement (Art. 5(1)(d) and following of the proposal), Article 16 TFEU is relied upon as a legal basis in as far as those specific rules are concerned.

The Commission also explained why a sectoral approach was not chosen for the proposal. According to the Commission this is mainly because the JHA sector faces broadly the same AI-related challenges as other sectors (opacity, complexity, unpredictability, data dependency, autonomy), although admittedly it is exposed to specific risks. Secondly, the Commission's ambition has been to regulate the AI market as a whole, which is and will be cross-sectoral since one and the same AI system can be used in different sectors. The AIA will also apply to both public and private providers and users, irrespective of whether the AI system is developed by a public or private entity and irrespective of the sector where the system is deployed. Relatedly, the proposal seeks to address an internal market problem, since the same AI application can be developed in-house by a public entity or procured from private technology providers active on the internal market. The same rules and standards should therefore apply to the same product in order to create a seamless internal market for trustworthy AI in Europe, to ensure a level playing field and to avoid inconsistencies in how the same AI applications are regulated.

The AIA would be applicable to providers (public or private) placing on the market or putting into service AI systems in the Union independent from their origin; users (public or private) located within the Union; and providers and users located in a third country, where the output produced by the system is used in the Union. However, it would not apply to public authorities in a third country or international organisations who use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States. AI systems developed or used exclusively for military as well as national security purposes are also outside the scope of the AIA.

The Commission explained that the AIA adopts a risk-based approach and provides a classification of risk under four categories: there are those applications or uses that imply minimal or no risk, AI systems that have to fulfil specific transparency obligations, AI classified as high-risk whose use is not prohibited *per se* but which are subject to compliance with AI requirements and ex ante conformity assessments (seven law enforcement use cases fall within this category), and those uses of AI which the AIA proposes to prohibit due to the unacceptable risk of contravening European values and fundamental rights.

According to the Commission, it has thus adopted a horizontal approach bearing in mind that many AI systems are characterized by the same challenges related to complexity, opacity, unpredictability, autonomy, and reliance on data. There is a need for a regulatory response that is uniform and consistent in its choices on the one hand, and articulated and flexible in implementing them on the other. The proposal has thus made a specific effort to consider, in particular, the specificities of the law enforcement sector with a number of tailored rules and exceptions. This is illustrated by the rule that the third party conformity assessments are performed by the market surveillance authorities, not by private bodies, that shall be the data protection authorities under LED or other national authorities already supervising the activities of the law enforcement sector. Furthermore, derogations from the obligations of transparency, enhanced confidentiality provisions, etc. are also provided where deemed appropriate.

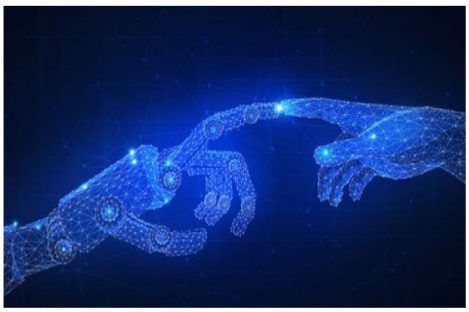
The definition of an AI system in the AIA has been formulated in as technology-neutral and future-proof ways as possible in order to anticipate technological developments in this field. The definition is complemented with specific techniques and approaches that should be used for the development of AI. These are listed in Annex I based on three main paradigms of artificial intelligence: 1) *learning* - systems that learn from data to achieve a human-defined objective; 2) *reasoning* - systems that reason on the basis of encoded knowledge; and 3) *modelling* - systems based on mathematical approaches concerned with the modelling of sample distribution or satisfaction of constraints.

In the discussion it was noted that the AI definition (Annex I) is very broad and includes for example systems based on statistics. The Commission clarified that it had relied on the OECD definition of AI and stated that it is important to note that not every technique or approach of AI detailed in Annex I would fall under the scope of application of the regulation if they do not fulfil simultaneously the requirements of the functional definition of AI in Article 3(1). AI systems can be used to solve problems for which humans fail to give a comprehensive specification that fits their objectives or solve problems for which the exact resolution following a mathematical or algorithmic specification is intractable.

According to the Commission, the goal of the AIA is to introduce specific requirements and obligations to address specific challenges posed by AI systems. These challenges are discussed in the Impact Assessment of the proposal and relate to complexity, lack of transparency and opacity, continuous adaptation and unpredictability, autonomous behaviour and data dependency. Not all of these challenges occur with all AI systems, but several challenges can occur in view of particular AI systems. According to the Commission, the proposal does not intend to introduce a comprehensive regulation of software systems or automated systems in general.

A Member State representative pointed out that the AIA seems to be based on the assumption that AI is autonomous or functions autonomously, which is generally not the case, as human experts are needed to monitor the systems. According to the Commission, it also presumes the presence of human oversight in the development and use of AI. However, AI systems that do not take the decision independently but rather assist human decision-makers are also covered by the scope of the definition because even those tools can be biased, opaque for humans and lead to violations of fundamental rights, such as discrimination.

A Member State representative enquired about a statistical system to prioritise suspects for investigation and wished to know whether this type of a system would fall under the scope of the AIA. In the Commission's view, this kind of system, if built based on statistical approaches within the meaning of Annex I c) with the objective to generate outputs such as predictions, decisions or recommendation influencing the environment it interacts with, will fall within the definition of AI systems in Article 3(1) AIA. Rule-based systems, however, where the AI output is the direct result of functional criteria explicitly pre-defined by humans, do not qualify as AI systems within the meaning of Article 3(1) AIA.



3. LEGAL QUESTIONS

The Commission's overall aim with the AIA is to create a horizontal internal market framework containing essential requirements for AI systems to ensure the protection of safety and fundamental rights and fostering the development of harmonized standards across the EU. The Commission stressed that an AI system is to be treated as a product as it is developed by humans to fulfil functions assigned to it in line with expected capabilities. Some Member States have already considered adopting national rules to ensure that AI is safe and that it is developed and used in compliance with fundamental rights obligations. Different national rules may lead to fragmentation of the internal market and reduce legal certainty for operators developing or using AI systems. This is why the AIA seeks to harmonize legislation and provides for comprehensive regulation of all issues within its scope. Member States may therefore not legislate on the same issues as those addressed in the AIA, unless explicitly foreseen in the AIA, such as in Articles 5(4) on real-time RBI and 29(2) on users obligations.

It is important to note that existing national and European legislation on the collection and admissibility of evidence is not challenged by the AIA, even for high-risk systems, since the AIA applies jointly with such existing rules, including on fundamental rights, and aims to facilitate its effective enforcement. Furthermore, Article 29(2) of the AIA allows Member States to impose additional requirements for the use of high-risk AI systems. A law enforcement agency may also define the tender specifications it needs for a specific high-risk system, as long as the AIA requirements are met and Union legislation on public procurement is respected. For low-risk systems, full-harmonization prevents Member States from imposing additional AI-specific requirements or transparency obligations, but Member States still have the possibility to introduce more general transparency obligations

that are not AI-specific, i.e. when they apply irrespective of the technology used.

As regards the legal basis of the AIA, which raised several questions from the Member State representatives, the Commission insisted that Article 114 TFEU is indeed the correct legal basis, as the AIA aims to regulate the internal market and introduces classic internal market harmonised rules for the placing on the market, putting into service and use of AI systems (Article 1 and recitals 1-2). Member State representatives raised concerns about the Schengen relevance of the AIA. Due to the horizontal approach, the focus on the internal market and the identified legal basis of Article 114 TFEU, according to the Commission the AIA is not a Schengen relevant instrument.

Only Article 5(1)(d) on the prohibition of the use of real-time RBI systems in publicly accessible spaces for the purposes of law enforcement, subject to specific exceptions, is based on a different legal basis, namely Article 16 TFEU on personal data protection. As explained in Recital 23, Article 5(1)(d) constitutes a *lex specialis* of Article 10 of the LED and requires transposition into national law, if Member States wish to make use of it.

The Commission also recalled that the definition of law enforcement authorities in Article 3(40) of the proposal corresponds with the definition of competent authorities in Article 3(7) of the LED. The AIA regulates exhaustively all matters falling within its scope, but it does not aim to regulate national criminal law procedures or other matters not covered by the AIA.

Member State representatives enquired whether a national intelligence agency developing its own AI device would fall under the scope of the regulation. The Commission recalled that under Article 4.2 TEU "*national security remains the sole responsibility of each Member State*" and therefore the AIA would not apply to that specific AI device if it was intended to be used for national security purposes. Nevertheless, if the AI device is for instance sold by a private provider to a national intelligence agency, then the AIA would apply accordingly.

Member State representatives asked about the level of obligation when law enforcement authorities develop AI solutions in-house. According to the Commission, this depends, in particular, on the risk classification: a system defined as a high-risk system must comply with the relevant requirements. The Commission also explained that whether an AI system falls under the scope of EU law and the AIA depends first and foremost on the intended purpose of that system, specifically whether it would be for national security purposes or for law enforcement, e.g. real-time RBI would fall under the scope of the AIA for law enforcement but not for national security purposes. Some Member State representatives pointed out that this separation might be sometimes difficult to make in practice, also taking into consideration the different mandates and competences of the relevant authorities.

4. IMPACT OF THE AIA ON SUPPLY AND IN-HOUSE DEVELOPMENT

The Commission presented the impact assessment carried out on the AIA and stressed that the impact on the relevant industry has been examined very closely. The Commission stressed that the current legal framework already imposes many demands on the JHA sector, both at European and national level. Therefore, compliance costs were estimated to be lower for law enforcement users and providers. For instance, in the JHA area Article 27 of the LED already requires a Data Protection Impact Assessment (DPIA). According to the Commission, the only additional expected cost factor is related to the legal constraints on external data reporting. Thus, in economic terms, the Commission expects that the AIA requirements will lead to a slight increase in costs, which should be partly or fully compensated by the increased trust in AI systems. Overall, according to the Commission, law enforcement users and providers will not carry greater costs than other AI operators.

According to the Commission, if there is greater public acceptance for AI solutions due to the high degree of trustworthiness of the AI system as a result of its compliance with the AIA, law enforcement authorities will find it easier to implement AI solutions, leading to higher demand for suppliers. Regarding competition from other suppliers, third country suppliers whose AI systems are used in the EU are subject to the same requirements as European suppliers, and in so far as the requirements in this sector are often already established, based on Commission assessment, SMEs will not be at an additional disadvantage compared to larger suppliers. Moreover, the AI regulation provides for specific support measures for SMEs, among other things in terms of access to sandboxes and lowered fees (Article 55).

Nevertheless, some Member State representatives found that the cost assessment underestimated the impact and wanted the Commission to elaborate on this issue, in order to show that the future AIA would not threaten the law enforcement sector with very demanding procedures in terms of time and efficiency having a direct impact on resources and costs. The Commission recognised that additional costs would be unavoidable, but considered that the law enforcement sector would be less exposed than others, because it is already subject to very demanding requirements under European or national legislation. According to it, there will in principle be virtually no impact on users.

As regards high-risk systems, the Commission underlined that its approach is to *regulate without prohibiting*. It seeks to maintain a balanced approach between the needs of law enforcement and the protection of fundamental rights, to ensure that AI tools are used in accordance with the principle of proportionality. As a result, there are new procedures and binding obligations introduced, but this is a necessity given the sensitivity of the sector and the risks to fundamental rights. According to the Commission, it has mainly clarified what needs to be done in terms of documentation, risk management, data quality, transparency, human oversight, security and accuracy to facilitate compliance with obligations under the already existing criminal law and fundamental rights legislation.

The Commission also pointed out that for law enforcement applications conformity assessment procedures are done by the provider based on internal checks. The case is different only for RBI applications where the competent supervisory authority must be involved in the assessment, but in case harmonised technical standards or technical specifications exist, the provider can do this based on self-assessment. To accommodate the exceptional circumstances of urgency that may

arise in the public security sector, a derogation from the conformity assessment procedure has also been provided e.g. for law enforcement in Article 47: any market surveillance authority may authorise the placing on the market or putting into service of specific high-risk AI systems within the territory of the Member State concerned for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets.

A Member State representative cited a "Center for Data Innovation" analysis published in July 2021[1], which estimates that the AIA would cost the European economy €31 billion over the next five years and would result in compliance costs of up to €400,000 for an SME deploying a high-risk AI system. This would lead to a 40 per cent decline in profits. The Commission disputed the CDI study as based on flawed assumptions that the AIA would apply to whole sectors. It also does not take into account 'business as usual' costs that the companies/public authorities already incur to comply with the requirements. The figure of €400 000 refers to a hypothetical extreme case based on a software integrated with hardware which previously did not need to be conformity assessed, but now has to be, and where against industry practice no quality management system was in place. According to the Commission, for many incumbent operators and public authorities the requirement of a quality management system is already fulfilled by virtue of the existing sectoral and public law regulations.

During the ensuing discussion it was noted that using a more disciplined approach of quality management to software development has shown that the development of software products can be better aligned with user requirements and lead to better quality, thus producing less malfunctions in the production environment, which in the long run could bring overall costs down for the whole ecosystem.

[1] https://www2.datainnovation.org/2021-aia-costs.pdf

5. HIGH-RISK APPLICATIONS

Apart from the AI systems referred to in Article 6(1) of the AIA, AI systems in the eight areas listed in Annex III are considered high-risk under Article 6(2). The areas of special importance for the JHA field are biometric identification and categorisation of natural persons; law enforcement; and migration, asylum and border control management. The assessment of the risk is only based on current AI development with the possibility to update the use cases in the future through delegated acts based on the same methodology and following an impact assessment and stakeholder consultation.

On the methodology for the evaluation of an AI use case as high-risk, the Commission referred to the criteria listed in Article 7 of AIA taking into consideration the intended use and objective of the AI system; whether it is in use or about to be used; whether the system has already caused harm or there are concerns on such possibility including the intensity of the harm; the adverse impact on fundamental rights for persons affected by the use of the AI systems; the reversibility of the outcome produced (the lower the degree of change, the more likely that the system is to be considered as high-risk); and the ineffectiveness of the existing Union law on redress as well as prevention and minimisation of risk.

Furthermore, recital 38 of the proposal describes types of AI systems that can lead to surveillance and have an impact on fundamental rights, including in the area of JHA. The risk assessment methodology described in the impact assessment was applied to a wide range of use cases and the Commission's impact assessment concluded that the initial list of high-risk AI systems presented should be annexed to the Commission's proposal. Point 6 of Annex III identifies seven types of AI systems used by law enforcement, ranging from individual risk assessment to deep fake detection to predicting the occurrence of a potential criminal offense based on profiling of identifiable natural persons within the meaning of LED. It is important to note that all other AI applications in the law enforcement sector would not be subject to additional requirements/conformity assessment procedures.

A Member State representative enquired whether a so-called fuzzy search would be considered AI. According to the Commission it would not qualify as AI, unless it applies 'search and optimization' methods listed in Annex I c) where the AI outcomes are based on rules that are not explicitly defined by humans. In the same vein, the SIS (Schengen Information System) would not be affected by the AIA. The Commission offered the Member States a possibility to evaluate and classify concrete use case scenarios.

Member State representatives enquired whether an automatic recognition application (to match shapes and colours, for example for clothes or cars) would be classified as high-risk. The Commission explained that it is difficult to make a judgement on this type of a case without more information, as this would depend on whether the application is able to profile identifiable natural persons within the meaning of LED.

A Member State representative enquired about the seeming contradiction concerning deep fakes between the AIA and Annex III, as the proposal subjects systems generating deep fakes only to certain transparency requirements, whilst according to point 6 of Annex III AI systems trying to detect deep fakes are categorised as high risk, when used by law enforcement. According to the Commission, this separation in how the systems are handled and regulated depends on the types of risks the rules address. In the case of the transparency obligations, the purpose of Article 52(3) is to

minimise the manipulative effects of deepfakes so that people know that this is not authentic, but artificially generated or modified content. On the other hand, the requirements for high-risk AI systems seek to ensure that AI tools used by law enforcement authorities to detect deep fakes are accurate, robust and secure, especially considering the fact that judges and police officers should be able to rely on them as evidence in criminal proceedings.

A Member State representative also enquired whether polygraphs used by defence/lawyers and provided by private entities and transferred to law enforcement would fall within the scope of the AIA. The Commission replied that the high-risk classification of polygraph systems relates only to AI systems used by law enforcement and migration, asylum and border control management authorities. If a lawyer submits an AI polygraph result during court proceedings, it is up to the court to assess the admissibility and reliability of this evidence.

As regards the requirements for high-risk AI systems, harmonised standards will be adopted by the ESOs (European Standards Organizations) based on a mandate and approval by the Commission.

A Member State representative enquired what would happen if a standard was modified and if it would require a new conformity assessment procedure. The Commission clarified that a distinction needs to be made between the legal requirement in the AIA and the standard, the latter being only the voluntary technical tool to demonstrate compliance. The essential requirement doesn't change even if the standard evolves. According to the Commission, in this case there is no need for re-certifying since conceptually it is the requirement that matters and compliance can be demonstrated in different ways. The standards normally follow the state of the art but this does not affect products which are already on the market and have been certified. Still, standards adaptations may have to be considered by the provider as part of the product performance analysis in the context of the post-market monitoring process established by the provider.

The Commission discussed the obligations of operators under Title III, Chapter 3 of the AIA, first underlining how the compliance with such obligations guarantees that the product is already validated. In this regard a distinction is made between providers (including also law enforcement authorities developing in-house AI systems) and users (AI developed in-house or bought off the shelf). The providers' obligations are related to e.g. undergoing conformity and compliance assessment of the system, implementing quality management systems, affixing CE marking and signing the declaration of compliance, keeping up-to-date documentation, establishing a post market monitoring system and reporting malfunctioning and serious incidents to competent authorities. On the user side, the obligations mainly relate to guaranteeing human oversight of the AI system and following the instruction of use, monitoring of operations' risks, and committing to inform the provider and/or distributor of any serious incident or malfunctioning related to the AI system. The Commission also clarified that if users make substantial modifications to the purpose or any component of the system impacting on the compliance with the requirements under Title III, Chapter 2 of the AIA, then the user becomes a provider who should ensure compliance with the AI requirements.

The Commission addressed the possibility of overlap between AIA and existing criminal law safeguards, explaining that the two systems of rules are not expected to overlap or conflict but to complement each other in order to create a strong legal and procedural framework for AI products and their uses.

When it comes to data quality requirements in Article 10, several Member State representatives noted that a 100 per cent error-free database or system is an unrealistic requirement. The Commission agreed and recalled that Article 9(3) refers to "state of the art". Therefore it is sufficient that the data is as good as possible for the purpose to be achieved.

The importance of the AIA enabling providers and users to control biases to prevent discrimination was stressed in the discussion.

Member State representatives enquired whether the Market Surveillance Authorities (MSAs) need to be independent. The Commission stated that it is a decision of each Member State to define and appoint the competent authority in accordance with the applicable legal requirements, which in the case of the law enforcement and border management sectors allows for two options: the national data protection authorities or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those system. In relation to the independence, the Commission replied that Article 11(2) of the Market Surveillance Regulation requires MSAs to be independent, but that it is not clear whether this includes organisational independence from the executive as is required for the data protection authorities (reference was made to the existing list of MSAs which covers also various ministries and agencies).

6. BIOMETRICS

Article 3 of the AIA defines biometrics. The Commission explained that the definition of biometric data provided in the regulation is fully aligned with the GDPR and LED. Data protection rules and requirements apply also with reference to biometric systems which are defined as those systems that can identify a person by their voice, face, movements, etc. In respect to these systems the Commission identified specific risks as they are considered highly intrusive in relation to the freedom of people, they may affect peoples' rights (i.e. privacy, data protection, equality and non-discrimination, freedom of expression, freedom of assembly, non-discrimination), and can raise concerns on possible inaccuracy and bias.

According to the Commission, whilst AI systems for biometric identification and categorisation of natural persons are considered high-risk in accordance with Annex III, a biometric authentication system will however not be considered high-risk, because it does not lead to the surveillance of people in general but only to the verification of the identity of an individual (for example for a customs control at an airport). Also excluded from the scope of the prohibition in Article 5(1)d) are biometric identification systems that are not "remote" and RBI systems used in spaces that are not publicly accessible or are publicly accessible but in a controlled environment such as border check facilities.

The prohibition of real-time RBI in publicly accessible spaces in the AIA (Article 5(1)(d)) is based on, and further specifies, the existing legal framework. Article 9 of the GDPR already prohibits in principle the use of biometric systems for identification purposes for any purpose that is not law enforcement unless limited exceptions apply: the processing of biometric data for the purpose of uniquely identifying a natural person is forbidden unless it

falls within one of the situations listed under Article 9(2) GDPR, e.g. consent, establishment, exercise or defence of legal claims, or substantial public interest.

The GDPR does not however apply to RBI used for law enforcement purposes, which are covered by the LED. Article 10 of the LED allows biometric identification systems when strictly necessary and subject to further conditions, such as authorisation by Union or Member State law, and further appropriate safeguards.

With the AIA the Commission proposes a *lex specialis* to Article 10 LED for real-time RBI, for law enforcement purposes, in publicly accessible spaces. In principle the use of such systems shall be prohibited. However, some exceptions to the ban have been outlined in Article 5(1)(d) of the AIA: targeted search for specific potential victims of crime, including missing children; prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; or detection of perpetrator or suspect of a criminal offence referred to in the European Arrest Warrant (EAW) and punished in the Member State concerned for a maximum period of at least three years. Moreover, Article 5(1)(d) does not prohibit the *ex post* identification of persons by a biometric system, given that it only relates to real-time RBI.

The Commission underlined the risks posed by the use of real-time RBI in public spaces for law enforcement purposes, considering it a particularly intrusive tool due to the immediacy of its impact and also because it may evoke feelings of constant mass surveillance with the public. Such risks are considered unacceptable and therefore prohibited, unless there are limited particular situations described above in which the use of RBI by law enforcement is authorised beforehand by judicial authorities or an independent administrative body. In case of an urgency, there can be an ex-post authorisation.

The Commission provided additional information regarding cases that would not be prohibited by Article 5(1)(d), also addressing a concern expressed at COSI regarding a seemingly different treatment of real-time RBI use in public spaces between law enforcement and other purposes, for example by private entities or operators. According to the Commission, a football club, contrary to what is possible for law enforcement purposes, can use real time facial recognition outside its stadium to identify persons that have been banned from attending. The Commission derives this from a recent decision of a national data protection authority which authorised the use as long as the club is committed to a number of safeguards and the system is prohibited from internet connectivity.

Member State representatives enquired about the meaning of the term "*prevention of a terrorist attack*". According to the Commission, whilst this is intended as an EU law concept that is ultimately to be interpreted by the Court of Justice of the EU, it is for the Member States to apply it in practice. The Member States' authorities are therefore to decide, on the basis of current circumstances and objective evidence, and subject to judicial control, when in a given situation the use of real-time RBI in publicly accessible spaces for law enforcement purposes is strictly necessary for the prevention of a terrorist attack. As regards, more specifically, the term "terrorist attack", although the proposal contains no express reference, according to the Commission it seems to make sense to interpret and apply it having regard to Directive 2017/541 on combating terrorism.

Despite the detailed explanations by the Commission, some Member State representatives found the proposal very restrictive in this respect and underlined that it would not match with the actual needs of law enforcement in its daily work. The Commission stressed that Article 5 AIA only applies to real-time biometric identification, a technology that appears rarely to be used by law enforcement authorities nowadays and for which most Member States do not yet have the legal basis required by Article 10 LED. Accordingly, Member States in most cases would not have to change an existing practice, but the AIA would apply to new forensic methods and tools.

Furthermore, Member State representatives argued that the risks of the use of real-time RBI for law enforcement purposes are deemed unacceptable because the impact is immediate, due to the feeling or perception of constant surveillance and because of limited chance for checks before action is taken. **However, the immediate impact usually means protecting a physical person or a group of people *in time*, i.e. before it is too late to protect them, where the temporal aspect is crucial.** In addition, the perception of surveillance may be caused by any cameras, be they part of an AI system or not. Finally, law enforcement will always be responsible for any action it takes and the fact that the use is in relation to an AI system does not diminish that responsibility in any way. Several Member State representatives supported this view.

The Commission explained that in the case of real-time systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. The use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons that are concerned by law enforcement activities.

The Commission stressed that it had carefully balanced the need for safety and security with the fundamental rights considerations and in particular the rights to privacy and data protection, in line with Articles 7 and 8 of the Charter of Fundamental Rights.

Member State representatives also pointed out that what is important is against which database the relevant images are cross-checked. There is a big difference between situations where cross-checks are made against a database on all inhabitants (i.e. where each and every person passing by can be identified) and, on the other hand, where cross-checks are made against a database of known suspects of terrorism or of serious crimes. The Commission agreed to this.

A Member State representative recalled that Article 10 LED currently enables Member States to legislate on the use of RBI in publicly accessible spaces on a broader range of situations than what the AIA and the exceptions in Article 5 provide for. For example, it could be used to identify witnesses of serious crime in order to investigate and also to offer them protection if they are in danger. It would be important to understand why such cases are excluded in the AIA. The Commission confirmed that when there is a specific, substantial and imminent threat to the life or physical safety of a person, which can be a witness, real-time RBI can be used if strictly necessary for the

prevention of this threat under the conditions in Article 5(2) to (4), if national law allows it. In case there is no such danger, Member States could explore the possibility to use post-processing RBI systems to find the witness.

A Member State representative also noted that regarding the list of criminal offences established in the EAW, there may be some very important serious crimes cases that are not included in the EAW, for example intentional damage to a water dam or to electricity distribution which endangers property on large scale – this could be classified as intentionally causing public danger under national legislation – similar to a terrorist attack but without the terrorist intent. According to the Commission, in many jurisdictions this would be considered sabotage or depending on the situation could also be covered by other EAW offences.

A Member State representative also pointed out that the three year qualifying criteria creates differences across the EU where in some Member States only very serious crimes carry a maximum sentence of at least three years whilst in others the threshold is significantly lower. Based on this, they considered that it should be reconsidered whether the EAW list is indeed the most useful or practical choice in relation to such a critical article where uniform application is key. The Commission explained that such threshold in accordance with national law contributes to ensuring that the offence should be serious enough to potentially justify the use of real-time RBI systems. Moreover, of the 32 criminal offences listed in the Council Framework Decision some are in practice likely to be more relevant than others, depending also on the Member State.

A Member State representative requested a clarification on the meaning of the "Four eyes" procedure. In Article 5(1)(d) it would be important to know whether counter-terrorism is considered part of national security. The Commission clarified that the "Four eyes" procedure mainly means that two people are needed to verify the result of the RBI system. A cumbersome procedure is not required. Furthermore, there are overlaps between national security and counter-terrorism, but depending on the concrete use-case, counter-terrorism as such could fall under Article 5(1)(d) in as far as it concerns the use of real-time RBI in publicly accessible spaces for any of the three objectives listed in that provision, including the prevention of a terrorist attack.

A Member State representative stated that the criteria to enter a relevant alert in the SIS should by default be the same for allowing - and activating - the use of real-time RBI in the cases specified under the exceptions. The Commission clarified that real-time RBI in publicly accessible spaces can be also used to check SIS alerts if the conditions of AIA and the implementing national law are met.

7. LARGE-SCALE IT SYSTEMS

The Commission highlighted the importance of the large-scale IT systems which have components that are AI systems. In the AIA the JHA-relevant systems are listed in Annex IX: SIS, Visa Information System (VIS), Eurodac (negotiations on-going), Entry-Exit System (EES), European Travel Information and Authorisation System (ETIAS), European Criminal Records Information System on third-country nationals and stateless persons (ECRIS-TCN) and specific components of the interoperability package (i.e. s-BMS). The Commission addressed the matter of date of application of the AIA that is 24 months following the entry into force, with the exception of the penalties that apply already after 12 months. The AIA has no retroactive effect. For the above-mentioned large-scale IT systems there are special provisions in Article 83(1) AIA: no application of the AIA for those systems placed on the market or put into service before a date that is 36 months after the entry into force of the AIA, unless the legal acts on which the systems are based are amended or replaced leading to a significant change in the system's design or purpose.

Based on this, the Commission expects that the AIA will not bring significant changes to the interoperability framework. Firstly, changes to the scope of large-scale IT systems have so far only been made following a formal evaluation of these systems after five years of operation. Secondly, since the objective of interoperability is to address the identities of persons, and given that such issues are specifically tackled in the AIA, according to the Commission, there is currently no need to change the framework.

The Commission stated that the implementation of the functionalities of AI systems will be done in compliance with both the legal bases of the individual systems and the AIA, to guarantee full transparency. Moreover, before the entry into operation of any system, eu-LISA will provide a data protection impact assessment in consultation with the EDPS. The impact of the AIA on eu-LISA will also affect the budget and resources involved in the in-house or commercial development of such systems, since it imposes additional requirements (i.e. concerning data, documentation and traceability, transparency, human oversight, accuracy and robustness) that were not covered by existing legal frameworks.

At the end of the discussion, a Member State representative expressed general concerns about the harmonisation effects of the AIA and their detailed impact on law enforcement activities. They requested the Commission to further assess whether law enforcement needs would be sufficiently safeguarded.

The Commission reiterated its readiness to address any Member State concerns bilaterally to provide additional information.

8. CONCLUSIONS

In conclusion, the Commission stated that it strongly believes to have provided a balanced proposal which addresses not only serious concerns from an internal market viewpoint, but also fundamental rights concerns in relation to the use of AI, whilst allowing for law enforcement use in clearly defined areas and with necessary safeguards. Furthermore, the Commission emphasised that law enforcement needs and fundamental rights protection are not considered mutually exclusive, and that all actors involved in the decision-making process and related discussions should ensure that all EU citizens can live a safe life with the guarantee of full respect of their rights.

The Commission took the opportunity to remind that the AI workshop is part of a long process aiming at tackling a sensitive area, which has and will have direct and significant impact on citizens' lives. Therefore, it is deemed necessary to work to make AI sustainable, functioning in accordance with fundamental rights, and providing a useful basis for any future development and innovation. According to the Commission all relevant risks have been carefully weighed and assessed. Finally, it is important to note that the AIA aims to build trust in AI technologies and their use, which makes addressing concerns and managing relevant risks central.

The Chair expressed his gratitude to all the participants and to the Commission for the detailed presentations and the ability to provide answers *ad hoc* to Member State concerns. It is crucial for the Member States to consolidate their positions in a way that takes into account the concerns of the JHA field in general and the law enforcement and internal security communities in particular. The main aim is to find a balance between fundamental rights requirements and law enforcement needs: these two important values, security and freedom, should not be seen as conflicting but rather as complementary and interdependent. The Chair reminded of the importance of Member States bringing relevant concerns to the negotiating table in the Telecom working party leading the negotiations on the proposal.