Council of the European Union

Brussels, 12 September 2022
(OR. en)

12302/22

Interinstitutional File:
2021/0106(COD)

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

OPINION OF THE LEGAL SERVICE[1]

From:	Legal Service
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence – Appropriateness of the legal bases of Articles 114 and 16 TFEU in relation to the provisions applicable to law enforcement and judicial authorities

1

I. INTRODUCTION

1. The proposed Regulation lays down harmonised rules for the placing on the market and the putting into service of artificial intelligence systems ('AI systems') in the Union (the "proposed Regulation")[2].

[1] This document contains legal advice protected under Article 4(2) of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, and not released by the Council of the European Union to the public. The Council reserves all its rights in law as regards any unauthorised publication.

[2] Doc. 8115/21.

2. At the meeting of the Telecommunications and Information Society Working Party on 7 April 2022, the Council Legal Service ("CLS") intervened on the issue of the appropriateness of the dual legal bases (Articles 16 and 114 TFEU) for the proposed Regulation on artificial intelligence systems ('AI systems'). The explanations confirmed that Articles 16 and 114 TFEU are the correct legal bases for the proposal and that recourse to Article 87(2) TFEU, instead of Article 114 TFEU, is not suitable. At the request of the Working Party, the present opinion sets out in writing and further develops the intervention provided by the representative of the CLS at that meeting.

3. AI systems are defined in Article 3(1) of the proposed Regulation. In general, they correspond to certain types of software. The proposed Regulation applies both to providers placing AI systems on the market and to providers putting AI systems into service. In addition, the proposed Regulation applies also to users. A provider may be a natural or legal person or a public authority/body which develops an AI system or which has an AI system developed, with a view to placing it on the market or putting it into service under its own name or trademark. A user may be any natural or legal person, public authority, agency or any other body using an AI system under its authority.

4. Under the definitions in Article 3, law enforcement and judicial authorities could qualify either as providers and/or users of an AI system. AI systems whose intended purpose, as defined by the provider, is law enforcement or the administration of justice, are classified as high-risk under Annex III. As such, they are subject to essential requirements (risk management, testing, data governance, technical documentation, transparency, human oversight, accuracy, robustness and cybersecurity) and to obligations (such as quality management systems, technical documentation, conformity assessment, corrective actions, duty of information, obligations of importers and distributors) as well as standards and conformity assessment. These harmonised rules are inspired from those applying to product safety in Directive 2006/42/EC (machinery)[3] and Regulation 2017/745 (medical devices).[4]

5. As regards AI systems involving the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, they fall under the category of prohibited AI systems. This prohibition on the use of AI systems is nevertheless subject to exceptions. Indeed, the use of such systems may or may not be authorised by Member States. If they are authorised, they are subject to detailed restrictions and safeguards so as to limit their use to what is strictly necessary, and in order to protect the fundamental right to the protection of personal data. Those restrictions and safeguards are provided for in the proposed Regulation on the basis of Article 16 of the Treaty on the Functioning of the European Union ("TFEU") and have to be complemented by national law. Articles 5(1)(d), (2), (3) and (4) of the proposed Regulation constitute *a lex specialis* to Directive 2016/680 (law enforcement data protection directive "LED") which was adopted on the basis of Article 16(2) TFEU.

---

3 Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC, OJ L 157, 9.6.2006, p 24-86.

4 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017, p. 1–175.

In accordance with Article 5(1)(d), the objectives of those systems are limited to:

i) the targeted search for specific potential victims of crime, including missing children;

ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of the European Arrest Warrant Decision [5] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State

Pursuant to Article 5(3), the use of such technologies by law enforcement must be subject to a prior authorisation by a judicial or administrative authority. However, in a duly justified situation of urgency, the use of the system may begin without an authorisation and the authorisation may be requested during or after that.

Pursuant to Article 5(4), a Member State may decide to authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement and define the necessary detailed rules for the request, issuance and exercise of the prior authorisation as well as the related criminal offences.

6. The legal bases of the proposed Regulation are Articles 16 TFEU (protection of personal data) and 114 TFEU (the functioning of the internal market). Therefore, the question arises as to the appropriateness of those legal bases in relation to the harmonised rules applicable to AI systems provided or used by law enforcement and judicial authorities.

[5] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002, p. 1.

7. This opinion focuses first on the appropriateness of the legal basis of Article 114 TFEU, in the particular context of law enforcement authorities which are mentioned in several provisions of the proposed Regulation, i.e. with respect to 'real-time' remote biometric identification systems in publicly accessible spaces, and high-risk AI systems referred to in point 6 of Annex III. Therefore, it addresses the issue whether Article 87(2) TFEU (police cooperation) would be a more appropriate legal basis to cover the provision and use of AI systems by law enforcement authorities, instead of Article 114 TFEU (Section II). By analogy, the conclusion of this note can be applied to judicial authorities referred to in Annex III concerning high-risk AI systems.

8. This note also addresses the appropriateness of the additional legal basis of Article 16 TFEU and the application of Protocols 21 and 22 in the context of the use of 'real-time' remote biometric identification systems in publicly accessible spaces by law enforcement (Section III).

II. APPROPRIATENESS OF THE LEGAL BASIS OF ARTICLE 114 TFEU

9. According to well-established case law, the legal basis of a Union act does not depend on an institution's conviction as to the objective pursued, but must be determined according to objective criteria amenable to judicial review, including in particular the aim and the content of the measure. If the examination of a measure reveals that it pursues a twofold purpose or that it has a twofold component and if one of those is identifiable as the main or predominant purpose or component, whereas the other is merely incidental, that measure must be based on a single legal basis, namely the one required by the main or predominant purpose or component. Only exceptionally, if it is established that the act simultaneously pursues a number of objectives, inextricably linked, without one being secondary and indirect in relation to the other, may such an act be founded on the various corresponding legal bases, unless these legal bases prescribe procedures which are incompatible with each other. It should also be noted, that the first sentence of Article 114(1) TFEU makes clear that the Article's provisions apply "[s]*ave where otherwise provided in the Treaties*". Accordingly, the use of Article 114 TFEU is justified only if no more specific provision is capable of constituting the legal basis for the adoption of the measure in question.[6] If the Treaty contains a more specific provision that is capable of constituting the legal basis for the measure in question, that measure must be founded on such provision.[7]

---

6 Opinion of the CLS of 17 May 2016, 9007/16, paragraph 6.

7 Judgment of 29 April 2004, *Commission v Council*, C-338/01, EU:C:2004:253, paragraph 60.

A. AIM OF THE PROPOSED REGULATION

10. The proposed Regulation harmonises the placing on the market, the putting into service and the use of a particular type of software (AI systems). The fact that public authorities and private operators may be providers or users of such AI systems is not incompatible *per se* with the legal basis of Article 114 TFEU.[8]

11. Furthermore, the fact that law enforcement authorities or those acting on their behalf may be among the providers or users of such AI systems is not sufficient to justify recourse to the legal basis of Article 87 TFEU. The aim and content of the proposed Regulation must be analysed in order to determine whether this is necessary.

12. The proposed Regulation aims in general, including with respect to 'real-time' remote biometric identification systems in publicly accessible spaces, and high-risk AI systems, to ensure a consistent and high level of protection throughout the Union while preventing divergences from hampering the free movement of AI systems and related products and services within the internal market. It lays down uniform obligations for operators and it guarantees the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market (Recital 2). More specifically, the proposed Regulation lays down rules regulating the placing on the market and putting into service of certain AI systems, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services (Recital 5). Overall, the proposal seeks to establish a trustworthy AI by design, applicable across the board, with a complete set of rules for the development, marketing and use of AI-driven products, services and systems. Given that AI has already found its way into a vast number of services and products and will continue to do so in the future, the proposal follows an internal market logic by setting out a 'product safety framework' constructed around a set of four risk categories. It imposes requirements for market entrance and certification of High-Risk AI Systems through a mandatory CE-marking procedure.

---

8 See CLS Legal Opinion (ST 11395/14 points 39 to 41) and precedents such as Directive (EU) 2016/2102, Directives 2014/24/EU, 2014/25/EU and 2014/23/EU.

13. None of the stated aims of the proposed Regulation refers to ensuring public security objectives. Even if public security objectives are to be fulfilled indirectly through the harmonising process of the placing on the market/putting into service/use of AI systems by law enforcement authorities, the Court[9], interpreting Article 87(2) TFEU in the light of Article 67 TFEU, stated that, in order for an act of the Union, having regard to its purpose and its content, to be based on the former article, it must be directly linked to the objectives set out in Article 67 TFEU (i.e. in this case, prevention of crime and police cooperation). This is excluded in the context of the proposed Regulation, since the only harmonised rules on the use of such systems by law enforcement authorities are either (1) product-safety type rules applying uniformly to all providers and users in relation to the placing on the market/putting into service or use of the AI systems or (2) rules on the protection of personal data for which the legal basis of Article 16 TFEU was added (see Part III below).

14. In another case[10], even though the objective of the amendment to the Firearms Directive consisted in ensuring a higher level of public security in relation to the terrorist threat and other forms of crime, the Court held that the harmonisation of aspects relating to the safety of goods is one of the essential elements for the proper functioning of the internal market, disparate rules in that area being such as to create obstacles to trade.[11]

---

9 Judgment of 6 May 2014, *European Commission v European Parliament and Council of the European Union,* C-43/12, EU:C:2014:298.

10 Judgment of 03 December 2019, *Czech Republic v European Parliament,* C- 482/17, EU:C:2019:1035.

11 Ibid., para 57: "*Given that the specificity of firearms resides, contrary to what the Republic of Poland claims, in the danger that they pose not only to users but also to the public at large, as the Court found in paragraph 54 of the judgment of 23 January 2018, Buhagiar and Others, C 267/16, EU:C:2018:26, public safety considerations are, as the fifth recital of Directive 91/477 recalls, essential in the context of rules on the acquisition and possession of those goods*". See also Judgment of 23 January 2018, *Albert Buhagiar and Others v Minister for Justice*, C-267/16, EU:C:2018:26, paragraph 54: *"In that regard, it must be stated that, in the light of the risk for the safety of persons that firearms pose, their free movement could be achieved only by laying down strict conditions for their transfer between Member States, one of which is the principle that prior authorisation is to be issued by Member States concerned by a transfer of such goods"*.

15. The objectives of the proposed Regulation including Article 5(1)(d), (2), (3) and (4) on the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement and the provisions relating to high-risk AI systems referred to in point 6 of Annex III, are not directly linked to a public security objective. On the contrary, the proposal responds to the main concerns related to how AI systems affect health, safety and fundamental rights. Therefore, the relevant provisions are directly linked to the objective of ensuring a level playing field in the placing on the market/putting into service or use of AI systems in the internal market, while protecting the health, safety and fundamental rights of users.

16. In the light of the above, the main objective of the proposed Regulation is to improve the functioning of the internal market within the meaning of Article 114 TFEU and the objectives referred to in Article 67 TFEU are only indirectly and incidentally linked to that main objective.

B. CONTENT OF THE PROPOSED REGULATION

17. The proposed Regulation essentially contains rules on what is needed to place a specific product (an AI software) on the market (or to put it into service) so as to ensure that it is safe and respects fundamental rights. It sets out a complete set of rules for the development, marketing and use of AI-driven products, services and systems. The proposed Regulation neither obliges law enforcement authorities to use an AI system which is lawfully placed on the market, nor does it directly regulate how law enforcement authorities should use such an AI system. Instead, it clearly delimits situations where the intended use is considered high-risk simply because an AI system will be used by law enforcement or judicial authorities.

18. Incidentally, Article 29 of the proposed Regulation contains rules on the conditions for the use of high-risk AI systems but such a provision is not sector-specific, it has a limited scope (mainly on the instructions for use of the product) and is intrinsically linked to the obligations placed on developers of AI systems under the proposed Regulation. It also gives Member States some leeway to provide for further rules on the use of such high-risk AI systems. With regard to 'real-time' remote biometric identification systems in public accessible spaces used for the purpose of law enforcement (Article 5), the proposed Regulation partly regulates the use of such systems from a data protection perspective on the basis of Article 16 TFEU (see part III below).

19. Furthermore, only Member States can decide to provide for the possibility to fully or partially authorise the use of such 'real-time' remote biometric identification systems. The specific conditions for such use remain to be laid down in national law but have to respect the general criteria and safeguards set out in the Regulation: prior judicial or administrative authorisation, request, issuance and exercise of the prior authorisation as well as the indication of the criminal offences in relation to which such systems may be used.

20. AI systems are a particular type of software. The harmonised rules applying to the placing on the market or putting into service/use of AI systems are thus product safety- like harmonised rules. They apply in a uniform way without distinguishing between public and private users. According to the relevant Recitals of the proposed Regulation, a consistent and high-level of protection throughout the Union should therefore be ensured. At the same time, divergences hampering the free movement of AI systems and related products and services within the internal market should be prevented. This would be achieved by laying down uniform obligations for operators and guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market based on Article 114 TFEU.[12]

21. The proposed Regulation contains several references to law enforcement, border control management and administration of justice in Annex III on high-risk AI systems (respectively items 6, 7 and 8). These include a detailed and exhaustive enumeration corresponding to Article 6(2) in addition to other high-risk systems in relation to product-safety risks referred to in Article 6(1). Indeed, according to Article 6(1), some AI systems are to be considered high-risk by definition because of their expected severity and high risks for the fundamental rights, health and safety. Other systems considered to be high-risk and listed in Annex III include education, management of critical infrastructures, employment, biometric identification and categorization as well as access to essential public and private services.

12 A Union legal framework laying down harmonised rules on artificial intelligence is therefore needed to foster the development, use and uptake of artificial intelligence in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market and putting into service of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services (see Recitals 2 and 5 of the Proposal).

22. However, such rules on high-risk AI systems do not provide whether law enforcement and judicial authorities (or those in the other identified fields) should or should not use those systems. The proposed Regulation will only indirectly produce its effects on the actual development of AI systems that may be used by law enforcement authorities, and on the AI systems in use currently and in the future. Thus, the rules refer to AI systems that are "*intended to be used*" by such authorities (see e.g. Articles 3(12), 8(2) and Annex III). The consequence of listing a certain AI system as high-risk is the application of a specific set of rules on risk management, data governance and technical specifications. Users of such high-risk AI systems must respect the instructions of use, keep logs and perform data protection impact assessments.

23. Furthermore, user obligations other than those relating to the instructions for use, may be laid down in Union or national law and without prejudice to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider (Article 29(2) of the proposed Regulation). These rules provide for further fundamental rights safeguards for high-risk AI systems.

24. In the light of the above, it should be emphasised that the proposed Regulation does not contain rules that aim to allow or prevent a high-risk AI system placed on the market from being used by law enforcement authorities. By effect of the proposed rules, a distinct label (high-risk) will be applied to an AI system developed or used by law enforcement authorities as a result of its intended use. This use would be governed by national law and, to a certain extent, decided by law enforcement authorities themselves. Indeed, the proposed Regulation lays down minimum conditions of use in Article 29 (limited to instructions of use) for the high-risk AI systems including those listed in items 6, 7 and 8 of Annex III which will be complemented by national law. Therefore, a distinction should be made, in line with the Court's case law, between on the one hand, the intended aim of the proposed Regulation which is not to regulate the use of AI systems by law enforcement authorities and, on the other hand, the effects it may indirectly produce[13] which are irrelevant for the purpose of analysing the appropriateness of the legal basis.

25. Items 6, 7 and 8 (on law enforcement, migration and administration of justice respectively) are not predominant among high-risk AI systems. Indeed, under the proposed Regulation, a high-risk AI system is not necessarily one which is listed in Annex III. Most high-risk systems are in fact those listed generically in Article 6(1)(a) and (b) of the proposed Regulation (in connection with the safety of products). Other high-risk AI systems are listed in Annex III containing items 1 (biometric identification), 2 (critical infrastructure), 3 (education and vocational training), and 4 (employment, workers management and access to self-employment) which relate to areas other than Justice and Home Affairs ("JHA"). All users of such high-risk AI systems are subject to a uniform regime established not in view of their specific status (such as whether they are an economic operator or a public authority), but from the perspective of protecting health, safety and fundamental rights.

[13] See judgment of the Court of 21 June 2018, *Republic of Poland v European Parliament, Council of the European Union*, C-5/16, EU:C:2018:483 paragraphs 63 to 68, and judgment of the Court of 22 June 2022, *Leistritz AG v LH*, C-534/20, EU:C:2022:495 paragraph 28.

26. The proposed Regulation thus contains harmonised rules on the placing on the market, the putting into service and use of AI systems whether they are used by private operators or public authorities including, incidentally[14], law enforcement and judicial authorities.

27. Leaving aside the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, which is subject to specific rules on the processing of personal data (see part III below), the proposed Regulation contains no harmonised rules on the use of high-risk AI systems. As explained in paragraphs 18 and 19 above, the reference to the use of high-risk AI systems essentially relates to the instructions on the use of the product (Article 29) and is linked to the obligations placed on developers. As pointed out in paragraph 22, the decision as to whether or not law enforcement or judicial authorities may use a high-risk AI system which is lawfully placed on the market under the proposed Regulation, lies with national law and national authorities.

28. Therefore, Article 87(2) TFEU, in particular its point (a), is not an appropriate legal basis for the proposed Regulation. The rules in the proposal neither promote nor impede the collection, storage, processing, analysis and exchange of relevant information. Simply, when such activities are performed by law enforcement authorities, a number of non-specific, harmonised conditions will need to be respected to safeguard users' rights. Similarly, the stated aims of the proposed Regulation do not include the development of common investigative techniques. The proposed requirements concerning the use of high-risk AI systems are not specific to the JHA area, and they do not concern police cooperation *stricto sensu* as defined in the TFEU.

[14] See Opinion of the Court, on the *Istanbul Convention*, A-1/19, EU:C:2021:198, in particular paragraphs 298, and 301.

29. In respect of the provisions of Article 5(4) of the proposed Regulation, a Member State may still decide to authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement. Where it does so decide, the Member State has a duty to set out the necessary detailed rules for the request, issuance and exercise of the prior authorisation as well as the related criminal offences for the investigation or prosecution of which the use is authorised[15]. On the basis of the outcome of the discussions within the Council, these proposed rules would not result in granting new powers in the hands of the respective national authorities. Instead, the use of existing or possible future mechanisms is circumscribed with a view to ensuring the protection of the right to privacy and personal data.

30. In the light of the above, Article 114 TFEU is the only appropriate legal basis for harmonised rules on high-risk AI systems, including those used by law enforcement and judicial authorities, and any JHA legal basis in Title V of Part Three of the TFEU, such as Article 87 TFEU with respect to those harmonised rules, is neither justified nor appropriate.

[15] It is noteworthy that Article 5(4) of the proposal presents certain characteristics similar to Article 15(1) of E-commerce Directive 2002/58. In particular, it provides for a possibility for the Member States to derogate from certain prohibitions set out in Union law. In the light of the settled case-law, the national provisions intended to derogate from those prohibition will necessarily come within the scope of Union law which, in turn, will trigger the application of the Charter in their regard.

III. APPROPRIATENESS OF ARTICLE 16 TFEU AS AN ADDITIONAL LEGAL BASIS

31. The proposed Regulation includes Article 16 TFEU as a legal basis, concerning the processing of personal data in the law enforcement area its Recitals 25 and 26 include a reference to Article 6a of Protocol 21 and Article 2a of Protocol 22 on the processing of personal data in the area of crime prevention. Article 16 TFEU is meant, in the Commission's view, to serve exclusively as a legal basis for the provisions placing restrictions on the processing of biometric personal data in a complementary manner as compared to Directive 2016/680 ("LED Directive"). Article 5(1)(c) is formulated as a prohibition in principle, to which a set of three exceptions apply. Concretely, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is prohibited unless strictly necessary to (a) perform targeted searches for potential victims of crime, (b) prevent an imminent terrorist attack or attack to the physical integrity/life of a person, (c) locate or identify or prosecute a perpetrator or suspect of a serious crime (with a reference to the European Arrest Warrant). Further requirements in Article 5(2), (3) and (4) attach to this specific use of AI systems by law enforcement authorities, notably an assessment of necessity and proportionality, a prior authorisation (except in emergency situations), and a decision by the Member States whether or not to authorise nationally the specific use of AI tools in such situations.

32. Article 5 is a detailed provision regulating a specific use of AI tools that not only purports to supplement the existing Union legislative framework (the LED, itself based on Article 16 TFEU), but also requires a national implementation framework.

33. In substance, despite its formulation as a prohibition, the specific rule in Article 5 may be described as laying out a strict and exceptional framing of the generalised, 'real-time' monitoring by AI instruments of individuals in open spaces for the purpose of identifying them. The prohibition also goes beyond the simple use of cameras for recording, and refers to the use of AI tools for the automated recognition of human features in publicly accessible spaces (features such as faces but also gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals). It also implies a concomitant capturing and identification of persons by analysis comparison/checking of data. In addition, the rule must also be assessed in light of the fact that 'real-time' identification by private users in public spaces may also be permitted (for events such as football matches).

34. Further clarifications offered by the Commission appear to indicate that, currently, no or possibly a very few Member States have regulated this specific issue, with a view to permitting law enforcement authorities to use AI tools in 'real-time' detection of individuals in public spaces. However, in practical terms, while no hard evidence was adduced to prove that existing practices and tools will need to change, it seems clear that future investigation techniques, forensic methods and rules on gathering evidence will have to integrate this prohibition/exceptions approach.

35. In so far as the legal basis is concerned, it appears that the provisions placing restrictions on the processing of biometric personal data in a complementary manner (as compared to the LED Directive) pursue the objective of protecting personal data by laying down appropriate safeguards. Such an objective is inextricably linked to the objective of the provisions falling within the ambit of Article 114 TFEU, without one being secondary and indirect in relation to the other. The proposed Regulation aims at laying down a general framework on AI systems following a risk-based approach. In this context, regulating AI systems horizontally may include strict safeguards applicable to this specific AI system of 'real time' detection. Such a specific AI system containing appropriate personal data protection safeguards is therefore inextricably linked to the overall objective of improving the functioning of the internal market and is not secondary or indirect in relation to the latter. The proposed Regulation should thus be governed by a dual basis in accordance with the relevant case law (see paragraph 9 above).

36. However, the question remains as to which legal basis should be used for regulating the processing of personal data for the use of systems referred to in Article 5(1)(c) to (4) of the proposed Regulation. Indeed, Article 87(2)(a) TFEU constitutes a legal basis for measures by law enforcement services in relation to the prevention, detection and investigation of criminal offences, concerning the collection, storage, processing, analysis and exchange of relevant information.

37. As the Advocate General explained in the PNR Canada Opinion (A1/15), Article 16 TFEU, on the one hand, and Articles 87(2)(a) and 82(1)(d) TFEU, on the other, cannot however maintain relationships of a '*lex generalis — lex specialis'* hierarchical type.[16]
Article 16(2) TFEU is the only provision applying to rules relating to the protection of individuals with regard to the processing of personal data by Member States' law enforcement authorities when carrying out activities for the prevention of crime. The mere fact that Article 5 refers to the list of serious crimes in the European Arrest Warrant Framework Decision does not change this assessment: that reference does not mean that that Framework Decision applies as such[17]. It is merely a legislative technique to list serious crimes without the need to create a separate Annex.

38. The fact remains that the rule in Article 5 is established not as a means of further delimiting the conditions of application of those JHA-related measures, but with a view to ensuring that, for the future, any use of 'real-time' biometric identification by AI systems will adequately respond to fundamental rights concerns, and primarily to the need to ensure that biometric data is collected and processed while respecting the right to privacy and to personal data.

In this respect, the Regulation does not aim to set out a new, mandatory JHA-specific procedure, but rather relies on tried and tested procedural means to ensure respect for fundamental rights.

---

16 See Opinion of AG P. Mengozzi of 8 September 2016, *Draft agreement between Canada and the European Union*, Case Opinion 1/15, EU:C:2016:656 paragraphs 112 to 120.

17 On the implementation of this list of serious crimes by the Member States, see judgment of the Court of 21 June 2022, *Human Rights League v Council of Ministers*, C-817/19, EU:C:2022:65 paragraphs 150 to 152.

39. If Article 16 TFEU is an appropriate additional legal basis, this raises questions as to the application of Articles 6a and 2a of Protocols 21 and 22 respectively. As explained in Recitals 25 and 26 of the Proposal, this means that when law enforcement authorities in Ireland or in Denmark use 'real-time' remote biometric identification systems in publicly accessible spaces for the prevention of crime, and where Ireland or Denmark are not bound by the corresponding rules on police cooperation or judicial cooperation in criminal matters, those two Member States will not be bound by Articles 5(1)(d), (2) and (3) of the proposed Regulation. This does not mean that Articles 5(1)(d), (2) and (3) contain rules on police cooperation, such as rules on information sharing between law enforcement authorities. This simply means that Articles 5(1)(d), (2) and (3) of the proposed Regulation, similarly to Directive 2016/680 (the "LED") which is *lex generalis* adopted on the basis of Article 16 TFEU, regulate the processing of biometric personal data in the particular context of 'real-time' remote biometric identification systems in publicly accessible spaces for the prevention of crime and nothing more. The Commission proposal in this respect follows the approach retained by the Union legislator for the LED, and, as such, confirms that recourse to Article87(2) TFEU in this context is therefore not justified.

40. The addition of Article 16 TFEU to Article 114 TFEU in this case is justified by the fact that Articles 5(1)(d), (2) and (3) are the only instances regulating the use of an AI system that have been authorised which interferes with the right to the protection of personal data, which is *lex specialis* to the general data protection framework. Such *lex specialis* data protection rules affecting the use of those sensitive AI systems cannot be considered secondary or indirect in relation to the internal market legal basis. Therefore, the addition of Article 16 TFEU as a legal basis is sufficiently justified in the proposed Regulation and recourse to Article 87(2)(a) TFEU is not appropriate.

IV. CONCLUSION

41. In the light of the above, the CLS is of the opinion that:

a) Recourse to Articles 16 and 114 TFEU as legal bases for the proposed Regulation is justified and appropriate;

b) Recourse to Article 87(2) TFEU or any other JHA legal basis is not justified or appropriate in relation to the harmonised rules applicable to AI systems which may be provided or used by law enforcement or judicial authorities.