Conseil de
l'Union européenne

Bruxelles, le 4 avril 2022
(OR. fr, en)

7052/22

Dossier interinstitutionnel:
2021/0106(COD)

LIMITE

TELECOM 96
JAI 317
COPEN 84
CYBER 77
DATAPROTECT 66
EJUSTICE 35
COSI 62
IXIM 49
ENFOPOL 120
FREMP 56
RELEX 323
MI 182
COMPET 146
CODEC 265

NOTE

Origine:	la présidence
Destinataire:	délégations
Nº doc. préc.:	6809/22 + REV 1
N° doc. Cion:	8115/21
Objet:	Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union - Dispositions relatives au domaine de la justice et des affaires intérieures (JAI)

I. INTRODUCTION

1. La Commission a adopté la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (loi sur l'intelligence artificielle, AIA) le 21 avril 2021.

2. La présidence slovène a rédigé la première proposition de compromis partiel, qui couvre **les articles 1 à 7** et **les annexes I à III** de l'AIA proposée. Cette proposition de compromis partiel a été présentée au groupe TELECOM le 30 novembre 2021 par la présidence slovène et a fait l'objet d'un examen approfondi lors de la réunion du groupe TELECOM du 11 janvier 2022 sous la présidence française.

3. La présidence française a repris les travaux de rédaction dans le cadre desquels elle s'est retirée et a rédigé les parties suivantes de la première proposition de compromis, couvrant **les articles 8 à 15, l'annexe IV, les articles 16 à 29 et les articles 40 à 55 bis**. La rédaction des autres parties de la première proposition de compromis (**les articles 30 à 39 et 56 à 85, les annexes V-IX**) est en cours.

4. En raison de sa nature horizontale, l'AIA proposée devrait avoir une incidence sur les acteurs opérant dans le domaine de **la justice et des affaires intérieures (JAI)**. S'il est prévu que le retour d'information des communautés JAI au niveau national passe déjà par les discussions et les commentaires/suggestions rédactionnelles gérés par le groupe TELECOM, la présidence française estime qu'il est important d'offrir une nouvelle occasion aux représentants de la communauté JAI de contribuer aux discussions. C'est pourquoi la présidence française a décidé d'organiser, le 7 avril 2022, une réunion distincte du groupe TELECOM consacrée exclusivement aux aspects JAI de la proposition, à laquelle des représentants de la communauté JAI ont également été invités.

5. La présidence française a recensé les dispositions suivantes de l'AIA qui ont une incidence directe sur le domaine de la JAI:
   - **Article 2, paragraphes 3 et 4** (Champ d'application);
   - **Article 3, paragraphes 33 à 41** (Définitions);
   - **Article 5, paragraphe 1, point (d)**, ainsi que **les paragraphes 4 et 4a** (Pratiques interdites en matière d'intelligence artificielle);
   - **Article 12, paragraphe 4** (Enregistrement);
   - **Article 14, paragraphe 5** (Contrôle humain);

- **Article 43, paragraphe 1** (Évaluation de la conformité);
- **Articles 47** (Dérogation à la procédure d'évaluation de la conformité);
- **Article 52** (Obligations de transparence pour certains systèmes d'IA);
- **Article 60** (Base de données de l'UE pour les systèmes d'IA listés à l'Annexe III);
- **Article 61** (Surveillance après commercialisation par les fournisseurs et plan de surveillance après commercialisation pour les systèmes d'IA à haut risque);
- **Article 63, paragraphe 5** (Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union);
- **Articles70, paragraphe 2** (Confidentialité);
- **Article 83** (Systèmes d'IA déjà mis sur le marché ou mis en service);
- **Annexe III, points 1, 6, 7 et 8** (Systèmes d'IA à haut risque visés à l'article 6, paragraphe 3);
- **Annexe VIII** (Informations à fournir lors de l'enregistrement d'un système d'IA à haut risque conformément à l'article 51).

Sur la base des observations écrites reçues des États membres jusqu'à présent, la présidence française a remanié certaines des dispositions susmentionnées afin de fournir aux États membres une base pour la poursuite des discussions sur ces aspects, en essayant de tenir compte des spécificités d'un certain nombre de sujets relevant de la JAI. Ces propositions de texte figurent à l'annexe du présent document. Les modifications apportées au document par rapport à la proposition de la Commission sont signalées comme suit: les ajouts sont signalés par des **caractères gras**, les suppressions sont signalées par ~~des crochets barrés~~ et les modifications par rapport au premier compromis partiel de la présidence SI sont ~~soulignées~~.

6. **La présidence française invite les délégations à examiner les modifications proposées ainsi que les autres dispositions énumérées au point 5 ci-dessus lors de la réunion du groupe TELECOM du 7 avril 2022, à laquelle participeront également des représentants de la communauté JAI**.

II. PRINCIPALES MODIFICATIONS

Les modifications détaillées ci-dessous sont celles proposées par la présidence française, mais la discussion peut également englober les modifications précédentes apportées par la présidence slovène. Les dispositions qui ont été mises entre crochets (article 2, paragraphe 3, article 3, paragraphe 39, et article 5, paragraphe 4 bis) peuvent soulever des enjeux particulièrs et la présidence souhaite que ces dispositions fassent l'objet d'un examen plus approfondi au cours de la réunion.

1. **Article 3 - Definitions**

1.1 La définition d'un «**système de catégorisation biométrique**» a été simplifiée et, dans un souci de clarté, des exemples de caractéristiques ont désormais été déplacés vers le considérant correspondant.

1.2 Les définitions de «**système d'identification biométrique à distance**» et de «**système d'identification biométrique à distance "en temps réel"**» ont été affinées afin de préciser quelles situations relèveraient de l'interdiction prévue à l'article 5 et quels seraient les cas d'utilisation qui ne le seraient pas (authentification/vérification de l'identité; vérification de l'identité pour accéder à un appareil/lieu/service). Étant donné que la notion de «à distance» a été supprimée par la présidence slovène en raison de l'impossibilité de la définir clairement, la notion de «instantané ou quasi instantané» a également été introduite dans la définition du «**système d'identification biométrique à distance "en temps réel"**».

1.3 La définition d'un «**système d'identification biométrique à distance "a posteriori"**» a été supprimée car cette notion a été définie mais n'a été utilisée nulle part dans le dispositif de la proposition.

1.4 La définition d'un «**espace accessible au public**» a également été révisée pour plus de clarté; des explications supplémentaires et des exemples de ce qui est exclu ont été ajoutés au considérant pertinent.

2. **Article 5 - Pratiques interdites en matière d'intelligence artificielle**

2.1 Les modifications apportées à **l'article 5, paragraphe 3**, visent à améliorer la formulation et à l'aligner sur la terminologie utilisée dans le droit de l'Union pertinent en matière de justice et d'application de la loi. En outre, les modifications apportées à **l'article 5, paragraphe 3, point iii)**, précisent que l'interdiction énoncée à **l'article 5** ne s'applique pas non plus aux infractions passibles d'une mesure de sûreté ou d'une peine privative de liberté d'au moins cinq ans.

2.2 Le nouvel **article 5, paragraphe 4 bis**, a été ajouté pour préciser que l'interdiction de l'identification biométrique en temps réel dans un espace accessible au public ne s'étend pas aux contrôles d'identité effectués par les autorités répressives lorsqu'une personne refuse de coopérer ou n'est pas en capacité d'indiquer son identité, sans préjudice des règles de procédure nationales ou de l'Union concernant les conditions permettant de tels contrôles.

3. **Article 14 - Contrôle humain**

3.1 Le terme «séparément» a été ajouté à **l'article 14, paragraphe 5**, afin de clarifier l'application du principe du double regard en ce qui concerne le contrôle humain des systèmes d'identification biométrique, sans exclure la possibilité pour l'utilisateur d'être l'une de ces deux personnes.

4. **Article 43 - Évaluation de la conformité**

4.1 Les modifications apportées à **l'article 43** visent à préciser que, pour les systèmes biométriques présentant un risque élevé au sens de l'annexe III, lorsque le fournisseur a appliqué des normes harmonisées ou des spécifications communes, il leur est proposé de choisir entre les procédures internes et externes d'évaluation de la conformité.

5. **Article 47 - Dérogation à la procédure d'évaluation de la conformité**

5.1 Les modifications apportées à **l'article 47**, paragraphe 1, et la suppression des **articles 47 (3), 47 (4) et 47 (5)** ont été introduites afin de simplifier et d'aligner le libellé de la procédure de dérogation sur la procédure équivalente qui s'applique aux dispositifs médicaux conformément au règlement relatif aux dispositifs médicaux, tout en s'efforçant de la rendre plus opérationnelle pour les situations répressives et en laissant davantage de marge d'appréciation aux États membres.

5.2 En outre, le nouvel **article 47, paragraphe 1 bis**, a été ajouté afin de créer la possibilité de demander une autorisation a posteriori aux autorités répressives, afin d'offrir une plus grande souplesse à ces autorités en cas d'urgence particulière et de garantir l'alignement sur **l'article 5**, **paragraphe 3**.

5.3 Le texte de **l'article 47, paragraphe 6**, a été clarifié et simplifié en incluant une référence plus simple aux «**systèmes d'IA à haut risque liés à des produits**», qui est un nouveau terme qui sera ajouté à **l'article 2** (Définitions). Cette modification englobe les deux situations précédemment mentionnées dans le texte.

6. **Article 52 - Obligations de transparence pour certains systèmes d'IA**

6.1 L'ajout à la fin de **l'article 52, paragraphe 2**, vise à assurer l'alignement sur un libellé similaire à la fin de **l'article 53, paragraphe 3**.

6.2 Le nouvel **article 52, paragraphe 2 bis**, prévoit une exception aux obligations de transparence pour les utilisateurs de systèmes d'IA utilisés pour la reconnaissance des émotions autorisées par la loi dans le cadre d'enquêtes pénales, qui a été déplacée de **l'article 52, paragraphe 2**.

6.3 Le nouvel **article 53, paragraphe 3 bis**, précise la manière dont les règles relatives aux obligations de transparence doivent être respectées.

6.4 Les modifications apportées à **l'article 53, paragraphe 4**, précisent que les États membres peuvent aller au-delà des exigences de transparence énoncées dans cet article s'ils le souhaitent (c'est-à-dire imposer davantage d'obligations).

7. **Article 60 - Base de données de l'UE pour les systèmes d'IA à haut risque autonomes**

7.1 Cet article devrait être lu conjointement avec **l'annexe VIII**, qui tient compte des spécificités en matière de répression, d'asile, de contrôle aux frontières et de migration. Les modifications apportées aux **articles 60 (1) et 60 (2)** visent à assurer l'alignement sur **l'article 54 bis** récemment ajouté sur les essais sur le terrain. Le texte supprimé à la fin de **l'article 60, paragraphe 2**, était superflu car il figure à **l'article 60, paragraphe 5**.

7.2 La disposition supprimée à **l'article 60, paragraphe 3**, a été déplacée vers le nouvel **article 60, paragraphe 5 bis**, qui contient également une disposition supplémentaire concernant l'accessibilité des informations enregistrées dans la base de données en ce qui concerne les essais sur le terrain.

8. **Article 61 - Surveillance après commercialisation par les fournisseurs et plan de surveillance après commercialisation pour les systèmes d'IA à haut risque**

8.1 Un nouvel **article 61, paragraphe 2 bis**, a été ajouté pour préciser que la confidentialité des informations détenues par les autorités répressives n'est pas affectée.

9. **Article 63 - Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union**

9.1 À **l'article 63, paragraphe 5**, l'ordre dans lequel les autorités de surveillance du marché possibles pour les systèmes d'IA à des fins répressives sont mentionnées a été inversé afin d'indiquer que les autorités chargées de la protection des données ne doivent pas nécessairement être le premier choix à cet égard. Cet article donne aux autorités répressives la possibilité de désigner, aux fins du présent règlement, soit l'autorité qui supervise leur activité, soit l'autorité de contrôle de la protection des données.

10. **Article 70 - Confidentialité**

10.1 À **l'article 70, paragraphe 1**, la référence au droit de l'Union et au droit national en matière de confidentialité a été ajoutée par souci de clarté juridique.

11. **Annexe III - Systèmes d'IA à haut risque visés à l'article 6, paragraphe 3**

11.1 La phrase introductive a été révisée afin de préciser que seuls des systèmes d'IA spécifiques dans certains domaines seraient répertoriés comme étant à haut risque, et non pas tous les domaines énumérés.

11.2 L'intitulé du **point 1** a été modifié afin d'indiquer une zone de biométrie de niveau supérieur, sans faire référence à des systèmes spécifiques.

11.3 Les modifications apportées au **point 1 a)** reflètent les modifications apportées à la définition du système d'identification biométrique à **l'article 3, paragraphe 34**.

11.4 La suppression du **point 7 c)** a été effectuée parce que la référence à la détection de documents non authentiques est redondante — elle est couverte par la vérification de l'authenticité mentionnée plus haut dans la même phrase.

12. Annexe VIII - Informations à fournir lors de l'enregistrement d'un système d'IA à haut risque conformément à l'article 51

12.1 L'ajout au **point 5** prévoit une exception pour les systèmes d'IA à haut risque dans les domaines de l'application de la loi et de la migration, de l'asile et du contrôle aux frontières, en ce qui concerne les informations à fournir lors de l'enregistrement des systèmes d'IA à haut risque dans la base de données de l'Union.

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

Provisions related to the area of justice and home affairs

Article 2
Scope

3. This Regulation shall not apply to AI systems developed or used **[**exclusively**]** for military **or national security** purposes.

4. This Regulation shall not apply to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations 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.

***

Article 3
Definitions

For the purpose of this Regulation, the following definitions apply:

(33) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, ~~which allow or confirm the unique identification of that natural person,~~ such as facial images or dactyloscopic data;

(34) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(35) 'biometric categorisation system' means an AI system for the purpose of assigning natural persons to specific categories~~, such as sex, age, hair colour, eye colour, tattoos,~~ **~~health, personal traits,~~** ~~ethnic origin or sexual or political orientation,~~ on the basis of their biometric data;

(36) '~~remote~~ biometric identification system' means an AI system for the purpose of identifying **natural persons**~~, at a distance~~ through the comparison of a person's biometric data with the biometric data contained in a reference ~~database~~ **data repository, excluding verification/authentification systems whose sole purpose is to confirm that a specific natural person is the person he or she claims to be, and systems that are used to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises;** ~~and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;~~

(37) ''real-time' ~~remote~~ biometric identification system' means a ~~remote~~ biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur **instantaneously or near instantaneously** ~~without a significant delay~~. ~~This comprises not only instant identification, but also limited short delays in order to avoid circumvention.~~

~~(38) ''post' remote biometric identification system' means a remote biometric identification system other than a 'real-time' remote biometric identification system;~~

(39) **[**'publicly accessible space' means any **publicly or privately owned** physical place accessible to **an undetermined number of natural persons** ~~the public~~, regardless of whether certain conditions **or circumstances** for access **have been predetermined, and regardless of the potential capacity restrictions** ~~may apply~~**]**;

(40) 'law enforcement authority' means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(41) 'law enforcement' means activities carried out by law enforcement authorities **or on their behalf** for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

***

Article 5

1. The following artificial intelligence practices shall be prohibited:

(d) the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces **by law enforcement authorities or on their behalf** for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

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

(ii) the prevention of a specific **and** substantial ~~and imminent~~ threat to **the critical infrastructure,** life**, health** or physical safety of natural persons or **the prevention** of ~~a~~ terrorist attack**s**;

(iii) the ~~detection,~~ localisation~~,~~ **or** identification ~~or prosecution~~ of a **natural person for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences** ~~perpetrator~~**,** ~~or~~ ~~suspect or convict of a criminal offence~~ referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[1] and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, **or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years,** as determined by the law of that Member State.

4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' ~~remote~~ biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision **and reporting** relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

4a. [The prohibition mentioned in Article 5(1)(d) shall not apply to situations where the person refuses or is not a capacity to disclose his or her identity in front of the law enforcement authority in publicly accessible spaces when that authority is authorised by Union or national law to carry out such identity checks.]

***

[1] 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).

Article 12
Record-keeping

4. For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum:

(a) recording of the period of each use of the system (start date and time and end date and time of each use);

(b) the reference database against which input data has been checked by the system;

(c) the input data for which the search has led to a match;

(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5).

***

Article 14
Human oversight

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been **separately** verified and confirmed by at least two natural persons.

***

Article 43
Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall ~~follow~~ **opt for** one of the following procedures:

(a) the conformity assessment procedure based on internal control referred to in Annex VI; **or**

(b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

Where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has not applied or has applied only in part harmonised standards referred to in Article 40, or where such harmonised standards do not exist and common specifications referred to in Article 41 are not available, the provider shall follow the conformity assessment procedure set out in Annex VII.

For the purpose of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, when the system is intended to be put into service by law enforcement, immigration or asylum authorities as well as EU institutions, bodies or agencies, the market surveillance authority referred to in Article 63(5) or (6), as applicable, shall act as a notified body.

***

Article 47
Derogation from conformity assessment procedure

1. By way of derogation from Article 43 **and upon a duly justified request**, 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. That authorisation shall be for a limited period of time **while the necessary conformity assessment procedures are being carried out, taking into account the exceptional reasons justifying the derogation.** ~~while the necessary conformity assessment procedures are being carried out, and shall terminate once those procedures have been completed~~. The completion of those procedures shall be undertaken without undue delay.

1a. In a duly justified situation of urgency for exceptional reasons of public security or in case of specific, substantial and imminent threat to the life or physical safety of natural persons, law enforcement authorities may put a specific high-risk AI system into service without the authorisation referred to in paragraph 1 provided that such authorisation is requested during or after the use without undue delay, and if such authorisation is rejected, its use shall be stopped with immediate effect.

2. The authorisation referred to in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies with the requirements of Chapter 2 of this Title. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraph 1.

~~3. Where, within 15 calendar days of receipt of the information referred to in paragraph 2, no objection has been raised by either a Member State or the Commission in respect of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.~~

~~4. Where, within 15 calendar days of receipt of the notification referred to in paragraph 2, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 2 to be unfounded, the Commission shall without delay enter into consultation with the relevant Member State; the operator(s) concerned shall be consulted and have the possibility to present their views. In view thereof, the Commission shall decide whether the authorisation is justified or not. The Commission shall address its decision to the Member State concerned and the relevant operator or operators.~~

~~5. If the authorisation is considered unjustified, this shall be withdrawn by the market surveillance authority of the Member State concerned.~~

6. ~~By way of derogation from paragraphs 1 to 5, f~~**F**or high-risk AI systems ~~*intended to be used as safety components of* devices~~ **related to products**~~, or which are themselves devices,~~ covered by **Union harmonisation legislation, only the conformity assessment derogation procedures established in that legislation shall apply.** ~~Regulation (EU) 2017/745 and Regulation (EU) 2017/746, Article 59 of Regulation (EU) 2017/745 and Article 54 of Regulation (EU) 2017/746 shall apply also with regard to the derogation from the conformity assessment of the compliance with the requirements set out in Chapter 2 of this Title.~~

***

Article 52
Transparency obligations for certain AI systems

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way **that those systems inform** ~~*that*~~ natural persons ~~are informed~~ that they are interacting with an AI system, unless this is obvious **from the point of view of a reasonable person** from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

2. Users of ~~an emotion recognition system or~~ a biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences**, subject to appropriate safeguards for the rights and freedoms of third parties**.

2a. Users of an emotion recognition system shall inform of the operation of the system the natural persons exposed thereto. This obligation shall not apply to AI systems used for emotion recognition which are permitted by law in the context of criminal investigations.

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated.

However, the first subparagraph shall not apply where the use is authorised by law to detect, prevent, investigate and prosecute criminal offences ~~or it is necessary for the exercise of the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter of Fundamental Rights of the EU, and~~ subject to appropriate safeguards for the rights and freedoms of third parties.

3a. The information referred to in paragraphs 1 to 3 shall be provided to natural persons in a clear and ~~visible~~ distinguishable manner at the latest at the time of the first interaction or exposure.

4. Paragraphs 1, 2**, 3** and 3**a** shall not affect the requirements and obligations set out in Title III of this Regulation~~.~~ **and shall be without prejudice to other transparency obligations for users of AI systems laid down in Union or national law.**

***

Article 60
*EU database for ~~stand-alone~~ high-risk AI systems **listed in Annex III***

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning high-risk AI systems **listed in Annex III** ~~referred to in Article 6(2)~~ which are registered in accordance with Article**s** 51 **and 54a**.

2. The data listed in Annex VIII shall be entered into the EU database by the providers **in accordance with Article 51. The data listed in Annex VIIIa shall be entered into the database by the prosepctive providers or providers in accordance with Article 54a**. ~~The Commission shall provide them with technical and administrative support.~~

3. ~~Information contained in the EU database shall be accessible to the public~~.

4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.

5. The Commission shall be the controller of the EU database. It shall ~~also~~ ~~**ensure**~~ **make available** to providers **and prospective providers** adequate technical and administrative support.

5a. Information contained in the EU database registered in accordance with Article 51 shall be accessible to the public. The information registered in accordance with Article 54a shall be accessible only to market surveillance authorites and the Commission, unless the prospective provider or provider has given consent for making this information also accessible the public.

***

Article 61

Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.

2a. Paragraph 2 shall be without prejudice to the obligations regarding the confidentiality of information held by law enforcement authorities.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

4. For high-risk AI systems covered by the legal acts referred to in Annex II, where a post-market monitoring system and plan is already established under that legislation, the elements described in paragraphs 1, 2 and 3 shall be integrated into that system and plan as appropriate.

The first subparagraph shall also apply to high-risk AI systems referred to in point 5(b) of Annex III placed on the market or put into service by credit institutions regulated by Directive 2013/36/EU.

***

Article 63
Market surveillance and control of AI systems in the Union market

5. For AI systems listed in point 1(a) in so far as the systems are used for law enforcement purposes, points 6 and 7 of Annex III, Member States shall designate as market surveillance authorities for the purposes of this Regulation either **the national authorities supervising the activities of the law enforcement, immigration or asylum authorities** ~~systems~~, or the competent data protection supervisory authorities under Directive (EU) 2016/680, or Regulation 2016/679 ~~or the national competent authorities supervising the activities of the law enforcement, immigration or asylum authorities putting into service or using those systems~~.

***

Article 70
Confidentiality

1. National competent authorities and notified bodies involved in the application of this Regulation shall**, in accordance with Union and national law,** respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

(a) intellectual property rights, and confidential business information or trade secrets of a natural or legal person, including source code, except the cases referred to in Article 5 of Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure apply.

(b) the effective implementation of this Regulation, in particular for the purpose of inspections, investigations or audits;

(c) public and national security interests;

~~(c)~~ **(d)** integrity of criminal or administrative proceedings.

2. Without prejudice to paragraph 1, information exchanged on a confidential basis between the national competent authorities and between national competent authorities and the Commission shall not be disclosed without the prior consultation of the originating national competent authority and the user when high-risk AI systems referred to in points 1, 6 and 7 of Annex III are used by law enforcement, immigration or asylum authorities, when such disclosure would jeopardise public and national security interests.

When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 63(5) and (6), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

3. Paragraphs 1 and 2 shall not affect the rights and obligations of the Commission, Member States and notified bodies with regard to the exchange of information and the dissemination of warnings, nor the obligations of the parties concerned to provide information under criminal law of the Member States.

***

Article 83

AI systems already placed on the market or put into service

1. This Regulation shall not apply to the AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex IX that have been placed on the market or put into service before *[12 months after the date of application of this Regulation referred to in Article 85(2)]*, unless the replacement or amendment of those legal acts leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.

   The requirements laid down in this Regulation shall be taken into account, where applicable, in the evaluation of each large-scale IT systems established by the legal acts listed in Annex IX to be undertaken as provided for in those respective acts.

***

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(~~2~~3)

In each of the areas listed under points 1-8, the AI systems specifically mentioned under each letter are considered to be h~~H~~igh-risk AI systems pursuant to Article 6(~~2~~3) ~~are the AI systems listed in any of the following areas~~:

1. Biometric**s** ~~**systems** identification and categorisation of natural persons~~:

   (a) ~~AI systems~~ **Biometric identification systems** ~~intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons~~ ~~**without their agreement**~~;

6. Law enforcement:

   (a) AI systems intended to be used by law enforcement authorities **or on their behalf** for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for for **a natural person to become a** potential victim~~s~~ of criminal offences;

   (b) AI systems intended to be used by law enforcement authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;

   (c) AI systems intended to be used by law enforcement authorities **or on their behalf for law enforcement purposes** to detect deep fakes as referred to in article 52(3);

(d) AI systems intended to be used by law enforcement authorities **or on their behalf** for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities **or on their behalf** for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities **or on their behalf** for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

~~(g) AI systems intended to be used **by law enforcement authorities or on their behalf** for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.~~

7. Migration, asylum and border control management:

(a) AI systems intended to be used by competent public authorities **or on their behalf** as polygraphs and similar tools or to detect the emotional state of a natural person;

(b) AI systems intended to be used by competent public authorities **or on their behalf** to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by competent public authorities **or on their behalf** for the verification of the authenticity of travel documents and supporting documentation of natural persons ~~and detect non-authentic documents~~ by checking their security features;

(d) AI systems intended to ~~assist~~ **to be used by** competent public authorities **or on their behalf** for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:

(a) AI systems intended to ~~assist~~ **be used by** a judicial authority **or on their behalf** ~~in~~ **for** ~~researching and~~ interpreting facts ~~and~~ **or** the law ~~and in~~ **for** applying the law to a concrete set of facts.

***

ANNEX VIII
INFORMATION TO BE SUBMITTED UPON THE REGISTRATION OF HIGH-RISK AI SYSTEMS IN ACCORDANCE WITH ARTICLE 51

The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 51.

1. Name, address and contact details of the provider;

2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;

3. Name, address and contact details of the authorised representative, where applicable;

4. AI system trade name and any additional unambiguous reference allowing identification and traceability of the AI system;

5. Description of the intended purpose of the AI system; **for high-risk AI systems in the areas of law enforcement and migration, asylum and border control management referred to in Annex III, points 1, 6 and 7, this information shall not include the specific context and conditions of use.**

6. Status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);

7. Type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body, when applicable;

8. A scanned copy of the certificate referred to in point 7, when applicable;

9. Member States in which the AI system is or has been placed on the market, put into service or made available in the Union;

10. A copy of the EU declaration of conformity referred to in Article 48;

11. Electronic instructions for use; this information shall not be provided for high-risk AI systems in the areas of law enforcement and migration, asylum and border control management referred to in Annex III, points 1, 6 and 7.

12. URL for additional information (optional).