



Brussels, 8 September 2021  
(OR. en)

11368/21

**LIMITE**

**TELECOM 321  
JAI 926  
COPEN 342  
CYBER 229  
DATAPROTECT 211  
EJUSTICE 82  
COSI 159  
IXIM 165  
ENFOPOL 307  
FREMP 225  
RELEX 718  
MI 622  
COMPET 600  
CODEC 1174  
CATS 51**

**NOTE**

---

From: Presidency  
To: CATS

---

Subject: Justice aspects of Artificial intelligence in the context of the proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act)  
- Discussion

---

**Background**

On 21 April 2021 the Commission submitted its horizontal proposal for a Regulation laying down harmonised rules on artificial intelligence (AI Act)<sup>1</sup>. The preparation of the Council's position is taking place in the Working Party on Telecommunications and Information Society (Telecom Working Party). Five meetings of the working party and two workshops have already taken place, and a progress report was published in June<sup>2</sup>.

---

<sup>1</sup> 8115/21

<sup>2</sup> 9674/21

On 16 July ministers for justice meeting informally in Ljubljana discussed justice aspects of the proposal. The Presidency would like to continue this discussion in the high-level format of the CATS meeting in order to further develop the reflection and be able to give useful guidance on justice aspects of the proposal, so as to facilitate the negotiations taking place in the Telecom structure.

During their first discussion, ministers for justice expressed support for the initiative in general but also insisted that some justice aspects deserved further work. One of the key issues is the distinction used in the proposal for justice-related uses of AI when it comes to defining which systems are considered ‘high risk’. As the proposal relies on a risk-based approach, the question of whether an AI system is considered high risk or not plays a key role in the regime provided for in the proposal for an AI Act.

#### *The criteria for high-risk AI systems in the justice sector*

For the justice sector, the relevant description of AI systems considered high risk is to be found in Annex III to the proposal. This includes primarily point 8 of the Annex, specifically dedicated to the ‘administration of justice’, but also several aspects of point 6 of the Annex, dedicated to ‘law enforcement’.

- ‘Administration of justice’ (point 8 of Annex III)

Point 8 of Annex III defines as high-risk systems ‘*AI systems intended to assist a judicial authority in researching and interpreting facts and the law **and** in applying the law to a concrete set of facts*’.

The wording of this definition has not yet been discussed in the Telecom Working Party.

The word ‘assist’ means it would be enough that the system provides a support to the judicial authority for it to fall under the definition. There is no threshold for the magnitude of the impact on the actual decision of the judicial authority.

*‘researching **and** interpreting facts and the law **and** [...] applying the law’*: the wording seems to indicate cumulative criteria. An AI system that only assists the judicial authority ‘in researching facts’ but not in ‘interpreting’ them or ‘in applying the law’ would thus not be considered high risk. The concrete impact of this cumulative wording is, however, difficult to assess.

It is also important to take recital 40 of the proposal into account: *‘[s]uch qualification should not extend, however, to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks or allocation of resources’*.

A difficulty for the justice sector is that the use of AI by judicial authorities is not very advanced compared to other sectors. This is at least partly due to the fact that use of digital technologies in the justice sector is highly sensitive, as recognised in the Council conclusions of 7 October 2020 on ‘Access to justice – seizing the opportunities of digitalisation’ (11599/20). This makes it even more difficult to evaluate the scope of the definition contained in point 8 of Annex III, as there are at this stage relatively few concrete uses of AI in the judiciary that can be assessed in relation to it<sup>3</sup>.

During the discussion at the informal meeting on 16 July, several ministers expressed concerns regarding the differentiation proposed by the Commission. The Presidency invites delegations to reflect in more detail and to discuss this concept of high-risk AI systems in the area of ‘administration of justice’.

---

<sup>3</sup> During the discussion at the informal meeting on 16 July, some ministers indicated that work is ongoing regarding the use of AI for the anonymisation of judgments, but this aspect is explicitly excluded from the scope of high-risk systems in recital 40.

- ‘Law enforcement’ (point 6 of Annex III)

It is important to note that several items contained in point 6 of Annex III will often, depending on the exact scope and the Member State concerned, at least partly cover criminal procedure aspects. In many cases, again depending on the Member State concerned, the use of such AI systems would concern acts that are under the supervision of a judicial authority.

It is also important to note that some of the wording would apply to aspects related to the penitentiary system and the execution of sentences.

The following items seem particularly relevant:

- *‘AI systems intended to be used by law enforcement authorities 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 potential victims of criminal offences’* (point a);
- *‘AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person’* (point b);
- *‘AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences’* (point d);
- *‘AI systems intended to be used by law enforcement authorities 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’* (point f).

One can imagine types of system falling under these categories which would require the extra safeguards attached to a high-risk system. It will also be necessary to analyse whether there are systems that would, with this wording, fall under these categories although they would actually have a relatively limited impact on the decision of the competent authority in a concrete case.

It is also important to examine whether the penitentiary sector is sufficiently taken into account in the text, considering that some decisions related to the execution of sentences are not taken by judicial authorities and would therefore not fall under the ‘administration of justice’.

In any case, the above-mentioned parts of the text seem to be rather new in the field of justice, which means that it is important to reflect on these concepts.

**Question for delegations:**

**What are your views on the criteria used to identify high-risk AI systems in the areas of ‘administration of justice’ and, as far as criminal proceedings may be concerned, ‘law enforcement’?**

---