European Committee of the Regions

SEDEC-VII/022

147th plenary session, 1-2 December 2021

OPINION

European approach to artificial intelligence – Artificial Intelligence Act (revised opinion)

THE EUROPEAN COMMITTEE OF THE REGIONS

- stresses that defining AI systems is an ongoing process that should take into account the context in which AI operates, keep pace with societal developments in this field, and not lose sight of the link between the ecosystem of excellence and the ecosystem of trust;
- regrets that the proposal for a regulation does not refer to local and regional authorities, despite the fact that the legal framework will apply to both public and private players;
- notes, to this effect, that AI systems can play an important role in local and regional authorities' interaction with citizens and service provision. Furthermore, AI systems have the potential, among other things, to improve public-sector efficiency and help local and regional authorities to respond to the adjustments that need to take place at local and regional level in the context of the green and digital transitions. It is therefore important that the experience gained by local and regional authorities is actively used in the ongoing revision of the Regulation;
- stresses the need for prior consultation of the relevant local and regional authorities where AI systems are to be used for the real-time remote biometric identification of natural persons in publicly accessible spaces for law enforcement purposes;
- points out that, concerning social classification by public authorities or on their behalf, it should be banned if carried out for general purposes, given the dangers resulting from such practices, as explained in Recital 17. The generation or collection of data for specific purposes should only be allowed with human oversight and provided that it does not violate the right to dignity and non-discrimination and the values of equality and justice;
- calls on the Commission to consider in greater depth the high-risk classification of AI systems intended for use by public authorities;
- calls for conformity assessments to be transparent and accessible to the public. Moreover, local and regional authorities should also be able to participate in the monitoring of AI systems, report on their implementation on the ground, and make a formal contribution to the European Commission's evaluation of the application of the regulation.

Rapporteur

Guido Rink (NL/PES), Member of the Executive Council of Emmen

Reference documents

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Fostering a European approach to Artificial Intelligence
COM(2021) 205

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
COM(2021) 206

Opinion of the European Committee of the Regions – European approach to artificial intelligence – Artificial Intelligence Act
(revised opinion)

I. RECOMMENDATIONS FOR AMENDMENTS

COM(2021) 206

Amendment 1
Recital 1

Text proposed by the Commission	*CoR amendment*
The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.	The purpose of this Regulation is to improve the functioning of the internal market ***and protect the fundamental rights of citizens*** by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

Reason
The reference to fundamental rights is intended to emphasise the link with the EU Charter of Fundamental Rights.

Amendment 2
New recital after Recital 6

Text proposed by the Commission	*CoR amendment*
	Defining AI systems is an ongoing process that should take into account the context in which AI operates, keep pace with societal developments in this field and not lose sight of the link between the ecosystem of excellence and the ecosystem of trust.

Reason
Developments in AI and technology require an adaptive and evolving approach. This recital reflects the fact that the definition of AI should move with the times and state of development of AI systems and applications.

Amendment 3

Recital 20

Text proposed by the Commission	*CoR amendment*
In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to ***appropriate*** limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.	In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those three exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. ***Consultation of the relevant local and regional authorities should take place prior to the exceptional use of those systems.*** In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be subject to ***stringent*** limits in time and space, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The reference database of persons should be appropriate for each use case in each of the three situations mentioned above.

Reason
"Real-time" remote biometric identification systems should not be used lightly.

Amendment 4

Recital 21

Text proposed by the Commission	*CoR amendment*
Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should ***in***	Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State. Such authorisation should be obtained prior to the use,

principle be obtained prior to the use, except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In ***such situations of urgency***, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law ***and specified in the context of each individual urgent use case by the law enforcement authority itself.*** In addition, the law enforcement authority should ***in such situations*** seek to obtain an authorisation ***as soon as possible, whilst providing the reasons for not having been able to request it earlier.***	except in duly justified situations of urgency, that is, situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use. In ***any case***, the use should be restricted to the absolute minimum necessary and be subject to appropriate safeguards and conditions, as determined in national law. In addition, the law enforcement authority should ***immediately inform the relevant local and regional authorities and*** seek to obtain an authorisation ***from the competent authorities***.

Reason
The political and administrative responsibility for managing and monitoring public spaces lies with local and regional authorities. They should therefore be duly involved in the deployment of such systems in public spaces. In urgent situations where it would not be reasonable to await prior consultation, the local or regional authority concerned should be immediately informed about the deployment of biometric systems in the public space.

Amendment 5

Recital 39

Text proposed by the Commission	***CoR amendment***
AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore ***appropriate*** to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the	AI systems used in migration, asylum and border control management affect people who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee the respect of the fundamental rights of the affected persons, notably their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore ***necessary*** to classify as high-risk AI systems intended to be used by the competent public authorities charged with tasks in the fields of migration, asylum and border control

fields of migration, asylum and border control management as polygraphs and similar tools or to detect the emotional state of a natural person; for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council, the Regulation (EC) No 810/2009 of the European Parliament and of the Council and other relevant legislation.	management as polygraphs and similar tools or to detect the emotional state of a natural person; for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum; for verifying the authenticity of the relevant documents of natural persons; for assisting competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Directive 2013/32/EU of the European Parliament and of the Council, the Regulation (EC) No 810/2009 of the European Parliament and of the Council and other relevant legislation.

Reason
This adaptation expresses the need to subject the AI systems concerned to the more robust regime for high-risk AI systems.

Amendment 6

Recital 43

Text proposed by the Commission	***CoR amendment***
Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the ***intended*** purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.	Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety**,** ***data security, consumer rights*** and fundamental rights, as applicable in the light of the purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade. ***Natural persons or groups of persons affected by high-risk AI systems placed on the EU market or otherwise put into service should be informed in an appropriate,***

	easily accessible and comprehensible manner, and have access to explicit, readily accessible and publicly available information explaining that they are subject to such systems.

Reason
The transparency and information requirements applicable to providers and users should be extended to the persons or groups of persons potentially affected by the use of high-risk AI systems, as listed in Annex III to the Regulation. In a comprehensible manner also means "in a language that is comprehensible and accessible to the user, including oral-auditory and manual visual languages".

Amendment 7

New recital after Recital 44

Text proposed by the Commission	***CoR amendment***
	AI system providers shall refrain from any measure promoting unjustified discrimination based on sex, origin, religion or belief, disability, age, sexual orientation, or discrimination on any other grounds, in their quality management system.

Reason
Unlawful discrimination originates in human action. AI system providers should refrain from any measures in their quality system that could promote discrimination.

Amendment 8

Recital 47

Text proposed by the Commission	***CoR amendment***
To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a ***certain degree*** of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.	To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons ***or public authorities at all levels of governance***, a ***high level*** of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.

Reason
The accountability of those who design high-risk AI systems is weakened by the use of the words "a certain degree of transparency".

Amendment 9

Recital 48

Text proposed by the Commission	*CoR amendment*
High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role.	High-risk AI systems should be designed and developed in such a way that natural persons ***and public authorities at all levels of governance*** can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role.

Reason
Self-explanatory.

Amendment 10

Recital 67

Text proposed by the Commission	*CoR amendment*
High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create ***unjustified*** obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.	High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking. ***Member States shall have the power to regulate high-risk AI practices and AI systems solely on the basis of overriding and duly justified public and national security interests***.

Reason
While Member States should not obstruct the application of the Regulation, they should retain the right to regulate high-risk AI systems if public and national security interests are at stake.

Amendment 11

Recital 70

Text proposed by the Commission	*CoR amendment*
Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. ***In certain circumstances, t***he use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be notified that they are interacting with an AI system***, unless this is obvious from the circumstances and the context of use***. Moreover, natural persons should be notified when they are exposed to an emotion recognition system or a biometric categorisation system. Such information and notifications should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin.	Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. ***T***he use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems. In particular, natural persons should be ***systematically*** notified that they are interacting with an AI system. Moreover, natural persons should be notified when they are exposed to an emotion recognition system or a biometric categorisation system. Such information and notifications should be provided in accessible formats for persons with disabilities. Further, users, who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, places or events and would falsely appear to a person to be authentic, should disclose that the content has been artificially created or manipulated by labelling the artificial intelligence output accordingly and disclosing its artificial origin.

Reason
No exceptions should be made to the transparency and notification requirement when natural persons interact with AI systems.

Amendment 12

Recital 76

Text proposed by the Commission	*CoR amendment*
In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. The Board should be responsible for a number of advisory tasks, including issuing	In order to facilitate a smooth, effective and harmonised implementation of this Regulation a European Artificial Intelligence Board should be established. The Board should be responsible for a number of advisory tasks, including issuing

opinions, recommendations, advice or guidance on matters related to the implementation of this Regulation, including on technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to and assisting the Commission on specific questions related to artificial intelligence.	opinions, recommendations, advice or guidance on matters related to the implementation of this Regulation, including on technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to and assisting the Commission on specific questions related to artificial intelligence. ***The members of the European Artificial Intelligence Board should reflect the interests of European society. The Board should be gender-balanced.***

Reason
The European AI Board should properly reflect the broad interests of European society. These interests include human rights, climate and the energy-efficient use of AI systems, safety, social inclusion, health, etc. Gender balance is a precondition for diversity in issuing opinions, drafting guidelines, etc.

Amendment 13

Recital 77

Text proposed by the Commission	***CoR amendment***
Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for the purpose of supervising the application and implementation of this Regulation. In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the public and other counterparts at Member State and Union levels, in each Member State one national authority should be designated as national supervisory authority.	Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more national competent authorities for the purpose of supervising the application and implementation of this Regulation. In order to increase organisation efficiency on the side of Member States and to set an official point of contact vis-à-vis the public and other counterparts at Member State and Union levels, in each Member State one national authority should be designated as national supervisory authority. ***Local and regional authorities shall be entrusted with supervisory or enforcement tasks where deemed appropriate by the Member State.***

Reason
In order to ensure the feasibility of the Regulation and its supervisory and enforcement framework, the Member State should be empowered to entrust, where necessary and where possible, local and regional authorities with carrying out supervisory or enforcement tasks.

Amendment 14

Recital 79

Text proposed by the Commission	*CoR amendment*
In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Where necessary for their mandate, national public authorities or bodies, which supervise the application of Union law protecting fundamental rights, including equality bodies, should also have access to any documentation created under this Regulation.	In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Where necessary for their mandate, national public authorities ***and, where applicable, local or regional authorities,*** or bodies, which supervise the application of Union law protecting fundamental rights, including equality bodies, should also have access to any documentation created under this Regulation.

Reason
This amendment takes into account the varying governance structures in the EU Member States.

Amendment 15

Recital 83

Text proposed by the Commission	*CoR amendment*
In order to ensure trustful and constructive cooperation of competent authorities on Union ***and*** national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.	In order to ensure trustful and constructive cooperation of competent authorities on Union**,** national**,** ***regional and local*** level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks.

Reason
This amendment takes into account the varying governance structures in the EU Member States.

Amendment 16

TITLE I, Article 3(1) – Definitions

Text proposed by the Commission	*CoR amendment*
'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or	'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed ***(non-exhaustively)*** in Annex I***, combined with social practices, identity and culture,*** and ***that*** can, for a given set of human-defined objectives, ***by***

decisions influencing the environments they interact with;	***observing its environment through collecting data, interpreting the collected structured or unstructured data, managing knowledge, or processing the information derived from these data,*** generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

Reason
An AI system consists of a combination of technical elements that link data, algorithms and processing power to social practices, society, identity and culture. The definition of such a dynamic socio-technical aggregate should therefore be future-proof and regularly updated to accurately reflect AI's ever-growing societal impact, while identifying fast changing AI-related challenges and opportunities, including the link between knowledge management and AI. In this context, an algorithm developed by another algorithm should also be subject to the Regulation.

Amendment 17

Article 5(1)

Text proposed by the Commission	***CoR amendment***
The following artificial intelligence practices shall be prohibited: (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm; (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm; (c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the	The following artificial intelligence practices shall be prohibited: (a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm***, infringes or is likely to infringe the fundamental rights of another person or a group of persons, including their physical or psychological health and safety, has or is likely to have a detrimental effect on consumers, including monetary loss or economic discrimination, or undermines or is likely to undermine democracy and the rule of law***; (b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group

trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, ***with the social score*** leading to ***either or both of the following:***	in a manner that causes or is likely to cause that person or another person physical or psychological harm;
i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;	(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons ***or groups of persons*** over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics**,** leading to ***AI-based social scoring for general purposes***;
ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;	(d) ***the placing on the market, putting into service or use of AI systems by public authorities or on their behalf, applying AI-based social scoring without human oversight for specific purposes, that is, in social contexts related to the contexts in which the data was originally generated or collected, for the evaluation or classification of the trustworthiness of natural persons or groups of persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;***
(d) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:	***(e)*** the use of 'real-time' remote biometric identification systems in publicly accessible spaces 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;	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;	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 Council Framework Decision 2002/584/JHA[62] 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.	

[62] 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).	iii) the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA[62] 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. [62] 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).

Reason
Subliminal techniques can, in general, undermine freedom, human rights and thus the functioning of the democratic rule of law. At the same time, artificial intelligence may undermine consumer rights. The purpose of the additions is to make this clear. Concerning social classification by public authorities or on their behalf, it should be banned if carried out for general purposes, given the dangers resulting from such practices, as explained in Recital 17. The generation or collection of data for specific purposes should only be allowed with human oversight and provided that it does not violate the right to dignity and non-discrimination and the values of equality and justice..

Amendment 18

Article 5(4)

Text proposed by the Commission	***CoR amendment***
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 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.	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 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. ***Those rules shall lay down the arrangements for***

	informing and consulting the local and regional authorities concerned. This consultation shall take place prior to the exceptional use of these systems in public spaces. In urgent situations where it would not be reasonable to await prior consultation, the local or regional authority concerned shall be immediately informed of the deployment of the relevant AI practice.

Reason
The political and administrative responsibility for managing and monitoring public spaces lies with local and regional authorities. They should therefore be put in a position to provide input prior to the deployment of such AI practices and be duly informed of the exceptional use of AI systems for the purpose of law enforcement. In urgent situations where it would not be reasonable to await prior consultation, the local or regional authority concerned shall be immediately informed.

Amendment 19

Article 13

Text proposed by the Commission	***CoR amendment***
Article ***13*** Transparency and provision of information to users 1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title. 2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users. 3. The information referred to in paragraph 2 shall specify: (a) the identity and the contact details of the	Article ***13a*** Transparency and provision of information to users 1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency ***and a comprehensible explanation*** shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title. ***The explanation shall be provided at least in the language of the country where the AI system is deployed.*** 2. High-risk AI systems shall be accompanied by ***publicly accessible and comprehensible*** instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users. 3. The information referred to in paragraph 2 shall specify:

provider and, where applicable, of its authorised representative; (b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including: i) its intended purpose; ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity; iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights; iv) its performance as regards the persons or groups of persons on which the system is intended to be used; v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system. (c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any; (d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;	(a) the identity and the contact details of the provider and, where applicable, of its authorised representative; (b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including: i) its intended purpose; ii) the level of accuracy ***(expressed in the relevant metrics for evaluating models)***, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity; iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights; iv) its performance as regards the persons or groups of persons on which the system is intended to be used; v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system. ***vi) parameters used to tune the model and measures taken to prevent overfitting and underfitting.*** (c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;

(e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates.	(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users; (e) the expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning of that AI system, including as regards software updates. ***13b Transparency and information to persons affected*** ***Persons or groups of persons for whom a high-risk AI system is intended to be used shall be informed in an appropriate, easily accessible and comprehensible manner, and have access to explicit, readily accessible and publicly available information of such use.***

Reason
In order to strengthen the ecosystem of trust, the instructions for use for high-risk AI systems should be made publicly accessible. These instructions should be written in a language of the country where the AI system is deployed, and should be comprehensible to the reader. With a view to the transparency and "explainability" of algorithms, it should be possible to explain with which parameters the model has been tuned and what measures have been taken to prevent overfitting and underfitting. Article 13b lays down an obligation for transparency and information vis-à-vis persons who interact with the AI system or who could be affected by the AI system.

Amendment 20

Article 14(4)

Text proposed by the Commission	***CoR amendment***
The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that	The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs

signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible; (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available; (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system; (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.	of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible; (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias') ***and of all other forms of bias***, in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available; (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system; (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure.

Reason
There are several forms of bias that may be problematic. Examples include the designer's or user's own bias (social bias), bias as to whether the AI system deployed is a suitable solution to the problem (technical bias) and statistical forms of bias.

Amendment 21

Article 14, new paragraph after paragraph 5

Text proposed by the Commission	***CoR amendment***
	Any decision taken by AI systems as referred to in Annex III(5) (a) and (b) shall be subject to human intervention and shall be based on a diligent decision-making process. Human involvement in these decisions shall be guaranteed.

Reason
Article 14 deals only with human oversight of high-risk AI systems. For government decisions, it is important to stress that human intervention, contact and due process are to be ensured.

Amendment 22

Article 17(1) new subsections after m

Text proposed by the Commission	*CoR amendment*
Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:	Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:
(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;	(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;
(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;	(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;
(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;	(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;
(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;	(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;
(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;	(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;

(f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems; (g) the risk management system referred to in Article 9; (h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61; (i) procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62; (j) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties; (k) systems and procedures for record keeping of all relevant documentation and information; (l) resource management, including security of supply related measures; (m) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph**.**	(f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems; (g) the risk management system referred to in Article 9; (h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 61; (i) procedures related to the reporting of serious incidents and of malfunctioning in accordance with Article 62; (j) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties; (k) systems and procedures for record keeping of all relevant documentation and information; (l) resource management, including security of supply related measures; (m) an accountability framework setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph***;*** ***(n) measures to prevent unjustified discrimination based on sex, ethnic origin, religion or belief, disability, age, sexual orientation, or on any other grounds;*** ***(o) an explanation of how ethical issues have been taken into account when designing the high-risk AI system.***

Reason
This addition stresses that inclusiveness and the fight against unjustified discrimination should be important elements of the quality system. The system should comply with the ethical values that a user of the AI system wishes to establish for that system or that the provider may reasonably expect to be established for a high-risk AI system. The provider must be able to explain how it has taken this into account.

Amendment 23

Article 19(1)

Text proposed by the Commission	*CoR amendment*
Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.	Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49. ***The providers of high-risk AI systems shall publish the EU declaration of conformity and a summary of the conformity assessment in a publicly accessible place.***

Reason
In order to strengthen the ecosystem of trust in AI systems, providers of high-risk AI systems must be open. The public should therefore be able to check that conformity assessment has been properly established in accordance with the rules of the Regulation.

Amendment 24

Article 29, new paragraph after paragraph 6

Text proposed by the Commission	*CoR amendment*
	Users of high-risk AI systems shall be responsible for making an ethical assessment before putting the system into use. They shall be able to explain the possible impact of the deployment of the technology on people and society. They shall specify their intended purpose in deploying the AI system, the overarching values, how those values have been weighted and whether or not they have been implemented in the system. They shall assess

	the actual impact of the system on people and society throughout the life cycle of the AI system.

Reason
Ethics is a broad concept. There are many ways of practising technology ethics, both in terms of theoretical underpinnings and practical methodologies, tools and design values. Values are matters that are considered important by certain (groups of) people; they may be more specific or more conceptual. It is important to keep open the range of possible moral values to be implemented and to continue evaluating the life cycle of the AI system.

Amendment 25

Article 52(1)

Text proposed by the Commission	***CoR amendment***
Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, ***unless this is obvious 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.	Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system. 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. ***The scope of options and legal position of natural persons interacting with AI systems shall not be limited by this interaction.***

Reason
Where technological tools are used as a medium for interaction with natural persons, there may be a risk of limiting the choices made by natural persons interacting with them. Natural persons should always be duly informed whenever they encounter AI systems and this should not be subject to interpretation of a given situation. Their rights should be guaranteed at all times in interactions with AI systems.

Amendment 26

Article 57(1)

Text proposed by the Commission	***CoR amendment***
The Board shall be composed of the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor. Other national authorities may be invited to the meetings, where the issues discussed are of relevance for them.	The Board shall be composed of the national supervisory authorities, who shall be represented by the head or equivalent high-level official of that authority, and the European Data Protection Supervisor. Other national***, regional and local*** authorities may be invited to the meetings, where the issues discussed are of relevance for them.

Reason
Local and regional authorities should be able to participate in the monitoring of AI systems and to report on their implementation on the ground.

Amendment 27

Article 58

Text proposed by the Commission	*CoR amendment*
When providing advice and assistance to the Commission in the context of Article 56(2), the Board shall in particular:	When providing advice and assistance to the Commission in the context of Article 56(2), the Board shall in particular:
(a) collect and share expertise and best practices among Member States;	(a) collect and share expertise and best practices among Member States***, regional and local authorities***;
(b) contribute to uniform administrative practices in the Member States, including for the functioning of regulatory sandboxes referred to in Article 53;	(b) contribute to uniform administrative practices in the Member States, including for the functioning of regulatory sandboxes referred to in Article 53;
(c) issue opinions, recommendations or written contributions on matters related to the implementation of this Regulation, in particular	(c) issue opinions, recommendations or written contributions on matters related to the implementation of this Regulation, in particular
i) on technical specifications or existing standards regarding the requirements set out in Title III, Chapter 2,	i) on technical specifications or existing standards regarding the requirements set out in Title III, Chapter 2,
ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,	ii) on the use of harmonised standards or common specifications referred to in Articles 40 and 41,
iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71.	iii) on the preparation of guidance documents, including the guidelines concerning the setting of administrative fines referred to in Article 71.

Reason
Local and regional authorities are closest to local residents and economies. They should explicitly feature when it comes to sharing their knowledge.

Amendment 28

Article 59(1)

Text proposed by the Commission	*CoR amendment*
National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks.	National competent authorities shall be established or designated by each Member State for the purpose of ensuring the application and implementation of this Regulation. National competent authorities shall be organised so as to safeguard the objectivity and impartiality of their activities and tasks. ***Local and regional authorities shall be empowered to carry out supervisory or enforcement tasks where deemed appropriate by the Member State.***

Reason
In order to ensure the feasibility of the Regulation and the given monitoring and enforcement framework, the Member State should be able to entrust, where necessary and where possible, local and regional authorities with supervisory or enforcement tasks. In this context, local and regional authorities must receive support and training in order to be fully empowered to carry out supervisory or enforcement tasks.

Amendment 29

Article 69(3)

Text proposed by the Commission	*CoR amendment*
Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.	Codes of conduct may be drawn up by ***national, local or regional authorities, by*** individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.

Reason
National, local and regional authorities should be given the legal power to draw up codes of conduct for the AI systems they develop or use.

Amendment 30

ANNEX I – Artificial intelligence techniques and approaches referred to in Article 3, point 1

Text proposed by the Commission	*CoR amendment*
(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.	***Having regard to the current state of science, AI includes the following techniques and methods:*** (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.

Reason
The definition and list of AI techniques should be future-proof. The list of specific techniques and approaches used for the development of AI systems should not be an exhaustive list and it must be clear that it is based on the current scientific state of play.

Amendment 31

Annex III, 1-5

Text proposed by the Commission	*CoR amendment*
High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas: 1. Biometric identification and categorisation of natural persons: (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons; 2. Management and operation of critical infrastructure: (a) AI systems intended to be used as safety	High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas: 1. Biometric identification and categorisation of natural persons: (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons; 2. Management and operation of critical infrastructure: (a) AI systems intended to be used as safety components in the management and operation

components in the management and operation of road traffic and the supply of water, gas, heating and electricity.	of road traffic and the supply of water, gas, heating and electricity***, and telecommunications, water and internet infrastructure***.
3. Education and vocational training:	3. Education and vocational training:
(a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;	(a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
(b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.	(b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.
4. Employment, workers management and access to self-employment:	4. Employment, workers management and access to self-employment:
(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;	(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behaviour of persons in such relationships.	(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behaviour of persons in such relationships.
5. Access to and enjoyment of essential private services and public services and benefits:	5. Access to and enjoyment of essential private services and public services and benefits:
(a) AI systems intended to be used by public authorities or on behalf of public authorities to ***evaluate*** the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;	(a) AI systems intended to be used by public authorities or on behalf of public authorities to ***evaluate and decide on*** the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
(b) AI systems intended to be used ***to***	(b) AI systems intended to be used ***to determine*** the creditworthiness of natural persons or their credit score, with the exception of AI systems

evaluate the creditworthiness of natural persons or ***establish*** their credit score, with the exception of AI systems put into service by small scale providers for their own use; (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.	put into service by small scale providers for their own use; (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

Reason
Telecommunications, water and internet infrastructure are an integral part of critical infrastructure. The classification of high-risk systems hinges on whether such systems could pose a real risk to citizens. The mere analytical and theoretical assessment of residents' claims to public services does not entail a high risk. Complementing "evaluate" with "decide on" emphasises that this risk effectively translates into decision-making, particularly for residents.

II. POLICY RECOMMENDATIONS

THE EUROPEAN COMMITTEE OF THE REGIONS

Ecosystem of excellence

1. stresses that the Commission's goal of making the EU a global leader in the responsible and human-centred development of AI can only be achieved if local and regional authorities have a significant role. Local and regional authorities are best placed to help create an environment propitious to boosting investment in AI in the coming years and fostering trust in AI;

2. highlights that besides involving local and regional authorities, it is important to provide support and training in order to enhance their competencies in the field, especially as they may receive supervisory and enforcement roles;

3. notes that EU funding is becoming available for the development of AI, but points to the fragmented approach here, due to the diverse range of programmes, which increases the risk of fragmentation and overlap;

4. calls, therefore, on the Commission to develop and connect strong and pluralistic common data spaces in which societal use-cases can be resolved with the use of public and private data. This also requires alignment with legislative initiatives under the European Data Strategy.

Ecosystem of trust

5. regrets that the proposal for a regulation does not refer to local and regional authorities, despite the fact that the legal framework will apply to both public and private players;

6. notes, to this effect, that AI systems can play an important role in local and regional authorities' interaction with citizens and service provision. Furthermore, AI systems have the potential, among other things, to improve public-sector efficiency and help local and regional authorities to respond to the adjustments that need to take place at local and regional level in the context of the green and digital transitions. It is therefore important that the experience gained by local and regional authorities is actively used in the ongoing revision of the Regulation;

7. calls for further clarification of the definitions of "provider" and "user", in particular in situations wherein companies, research institutions, public authorities and residents jointly develop and test AI systems in living labs. Due consideration should be given also to citizens or consumers affected by AI-driven decisions of systems employed by professional users;

8. stresses the need for prior consultation of the relevant local and regional authorities where AI systems are to be used for the real-time remote biometric identification of natural persons in publicly accessible spaces for law enforcement purposes;

9. welcomes the European Commission public consultation on the adaptation of civil liability rules to the specific challenges of digital age and artificial intelligence[1] and expects that this will result in an updated framework aimed at ensuring consumer redress for damage caused by AI applications;

10. wonders why AI systems used in democratic processes such as elections are not on the list of high-risk AI systems;

11. calls for high-risk AI systems to be subject to the same transparency and information requirements for natural persons as currently apply to users;

12. highlights the major human rights risks and implications associated with the use of social classification;

13. is highly sceptical here of the two scenarios set out in the Regulation[2] as grounds for determining when a social classification leads to detrimental or unfavourable treatment of individuals or groups of people, as it is extremely difficult to establish the existence of such grounds. In this context, the Committee urges for the clear formulation of strong safeguards in order to ensure that the ban on social classification practices is not circumvented;

14. notes the fact that the recitals of the Regulation address the risks to which individuals are exposed as a result of interacting with high-risk AI systems in the context of, inter alia, education, training, employment, human resource management, access to self-employment and access to and receipt of certain essential private and public services;

---

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en

2 Article 5(1)(c)

15. calls on the Commission to consider in greater depth the high-risk classification of AI systems intended for use by public authorities[3];

16. calls for an authority to provide substantial ex ante advice on the interpretation of provisions in the Regulation, also in relation to the General Data Protection Regulation. This will enhance legal certainty and reduce the costs of designing and implementing AI systems;

17. underlines to this effect the importance of clarity in the formulation of the Regulation, which is instrumental in building an ecosystem of trust and lifting legal uncertainty surrounding the development and use of AI systems. This would avoid misinterpretations of the proposed requirements and minimise the risks of subsequent mismanagement of AI applications, thus maximising the regulation's effectiveness and credibility of sanctions. At the same time, and in line with the European Commission's better regulation agenda, early detection and elimination of potential overlaps and/or conflicts with existing rules is of key importance;

18. notes that many local and regional authorities are using the same AI systems for similar tasks. The systems are designed by private companies in the vast majority of cases;

19. notes that the proposal for a regulation does not stand alone when it comes to guaranteeing citizens' rights and that it must be seen in the context of existing legislation. Member States are therefore encouraged to ensure that, on an ongoing basis, they take the necessary administrative measures to enable them to deal with the opportunities and risks posed by the use of AI in the public sector;

20. notes that this means that in conformity assessment, European and national rules are being interpreted by companies and notified bodies, and that this is having an impact on the practices of local and regional authorities using these AI systems. This makes it difficult to determine the extent to which local and regional policy is taken into account in these AI systems. Therefore, the Committee attention to the specific needs of local and regional authorities and to the fact that a “one-size-fits-all” approach may undermine the effectiveness of AI systems in responding to those needs. Besides, the Committee suggests that Member States should be empowered to regulate high-risk AI systems in the face of overriding and justified reasons of public interest;

21. calls, in this regard, for conformity assessments to be transparent and accessible to the public. Moreover, local and regional authorities should also be able to participate in the monitoring of AI systems, report on their implementation on the ground and make a formal contribution to the European Commission's evaluation of the application of the regulation;

22. stresses that the application of the regulatory sandbox requires the right legal, methodological and ethical conditions to be created to enable the development of technology and legislation and the evaluation of legislation. Clear criteria for allowing companies to participate in the regulatory sandbox should be established. To ensure that consumer organisations can enforce the provisions of the Artificial Intelligence Act, the latter must be added to Annex I of the

3 Annex III(5)(a)

European Directive on representative actions for the protection of the collective interests of consumers ((EU) 2020/1828);

Information campaigns

23. stresses the importance of public campaigns, so that the general public is informed about and familiarised with the existence and usefulness of AI systems as well as potential risks. Further underlines the urgent need for comprehensive information for consumers on Artificial Intelligence / machine-driven decision-making. Asks to this effect that the European Commission provide funding for such campaigns;

Administrative burden

24. expresses its concern about the potential administrative burden of the proposed Regulation. The administrative burden can hinder small and medium-sized enterprises and local and regional authorities in promoting innovation and deploying AI systems[4];

Proportionality and subsidiarity

25. considers that the draft regulation complies with the requirements of the proportionality and subsidiarity principles. The added value of EU action in this field and the appropriateness of the legal bases chosen by the Commission are clear and consistent. The impact assessment included a distinct section on subsidiarity. Moreover, no national parliament issued a reasoned opinion on non-compliance with the principle of subsidiarity by the deadline for submissions, set on 2 September 2021.

Brussels, 2 December 2021

The President
of the European Committee of the Regions

Apostolos Tzitzikostas

The Secretary-General
of the European Committee of the Regions

Petr Blížkovský

4 A recent study (*Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe*, p.12), supported by the European Commission, estimated that, on the basis of reasonable assumptions, obtaining certification for an AI system could cost on average between EUR 16 800 and EUR 23 000, roughly equivalent to 10-14% of development costs.

III. PROCEDURE

Title	European approach to artificial intelligence – Artificial Intelligence Act (revised opinion)
Reference(s)	COM(2021) 205 COM(2021) 206 OJ 2020/C 440/14
Legal basis	Article 307 TFEU
Procedural basis	Own-initiative opinion (under Rule 41(a) of the Rules of Procedure); revised opinion (under Rule 57 of the Rules of Procedure); see Bureau decision
Date of Council/EP referral/Date of Commission letter	24 June 2021
Date of Bureau/President's decision	4 May 2021
Commission responsible	Commission for Social Policy, Education, Employment, Research and Culture (SEDEC)
Rapporteur	Guido Rink (NL/PES)
Analysis	26 July 2021
Discussed in commission	23 June 2021
Date adopted by commission	1 October 2021
Result of the vote in commission (majority, unanimity)	Majority
Adopted at plenary	2 December 2021
Previous opinions	White Paper on Artificial Intelligence – A European approach to excellence and trust[5] Digital Europe for all: delivering smart and inclusive solutions on the ground[6] Artificial Intelligence for Europe[7]
Date of subsidiarity monitoring consultation	N/A

5 CoR 2014/2020

6 CoR 3332/2019

7 CoR 3953/2018