AI4Belgium

AI4Belgium Feedback Note on the European Commission's Proposal for an **Artificial Intelligence Act**

Key feedback points

1) Overall, the proposed regulatory framework is much appreciated and welcomed.
2) The proposal's "list-based" approach risks being incomplete, and it requires periodic assessments.
3) The scope of the proposal requires further refinement, and overlap with sectorial legislation that already covers AI needs to be more closely considered.
4) Further clarifications are needed for certain terms that are used throughout the proposal.
5) The requirement of ex ante third party conformity assessments could potentially be extended in certain cases.
6) Some open questions remain around the value of the proposed CE label.
7) Concerns about the regulation's enforcement mechanism should be addressed.
8) There is a need for guidance as to how the requirements should be implemented.
9) Additional efforts are needed to stimulate innovation.
10) More attention should be given to the impact of AI on societal interests and the environment.

Introduction

AI4Belgium is the Belgian coalition of key actors in AI from academia, the private sector, the public sector and civil society. It enables individuals and organisations in Belgium to capture the opportunities of AI while facilitating the ongoing transition towards the technology's increased adoption in a responsible and trustworthy manner. AI4Belgium has the ambition to position Belgium and its regions on the European AI landscape, drawing on the many assets vested in the Belgian AI ecosystem, from high quality researchers, excellent entrepreneurs and companies to innovative public entities, all the while being mindful of the ethical, legal and social challenges that this technology brings forth.

AI4Belgium welcomes the opportunity to provide feedback on the European Commission's proposed 'Artificial Intelligence Act' in the form of a new EU regulation (the 'proposed AI Regulation' or the 'proposal'), which was published on 21 April 2021.

The Commission's proposal was overall well-received by the AI4Belgium community, and is considered to be a strong starting point to ensure that AI systems are deployed in a manner that respects fundamental rights within an environment that is keen on socially beneficial innovation. There is, however, still some scope for clarification and specification throughout the proposed AI Regulation. Without aiming to be exhaustive, this feedback note provides an overview of the main considerations formulated by the AI4Belgium community.

This note was prepared in the context of a virtual workshop organised by AI4Belgium's Working Group on *AI Ethics & Law* on 18 May 2021 for the members of the AI4Belgium community, in

cooperation with the different regional AI hubs, including *Kenniscentrum Data & Maatschappij*, *CRIDS/NADI* and the *AI Institute for the Common Good* (FARI). During and after the workshop, feedback was gathered on the proposed AI Regulation's strengths and weaknesses from the perspective of the Belgian AI ecosystem. On this basis, a first draft note was prepared, which was subsequently circulated within the AI4Belgium community in order to give all members an opportunity to consult the document and provide further input. The end result comprises the consolidated feedback of the AI4Belgium members on the proposed AI Regulation.

In what follows, the key points of feedback that were raised by the AI community are described, with suggestions on how the proposal could be further improved. Given the rich diversity of AI4Belgium's membership, there are certain aspects of the proposal on which members disagreed. In those instances, we have reflected this variety of opinions in this document, in order to provide a comprehensive overview.

Overview of AI4Belgium's feedback

1) Overall, the proposed regulatory framework is much appreciated and welcomed

AI4Belgium commends the Commission's overall approach to the regulatory framework for AI that is being put forward in the proposal. The debate on an adequate ethical and legal framework for Artificial Intelligence has been ongoing for several years now, and the time was more than ripe to propose a number of binding rules to ensure that individuals and organizations can trust AI systems that are deployed across the EU through verifiable procedures rather than voluntary guidelines. These procedures to enable trust are not only important to ensure compliance with fundamental rights, but also to stimulate the adoption (and intra-EU trade) of AI, and to capture the benefits that this technology can generate. It can be hoped that the EU model will be adopted beyond the Union's borders, and provisions about the extraterritorial effect of the proposed regulation are hence also welcome.

The emphasis on regulating the use of AI rather than the technology itself is an advantage of the proposal. At the same time, given that AI systems can be repurposed for various uses, the Commission's proposed design, development and deployment requirements (in terms of risk-management, data governance, technical documentation, transparency, human oversight, and accuracy, robustness and cybersecurity) are essential, and will need to be translated into practice through various methods, which can also be adapted to the specific sectors in which the systems are used.

2) The "list-based" approach of the proposal risks being incomplete, and it requires periodic assessments

AI4Belgium members particularly appreciated the risk-based approach of the proposed AI regulation, and the important signposting of risk levels by way of the chapters' headings (namely a set of prohibited AI practices, a set of high-risk AI practices, a set of AI practices that require further transparency, and other AI applications).

Some members, however, rightfully remarked that this list-based approach risks being incomplete. Others pointed towards the risk of the list to become overly-inclusive. It is acknowledged that it is difficult to ensure the comprehensiveness of such lists from the outset. It is therefore crucial that the said lists are updated periodically and in a speedy manner, without the need to revisit the entire regulatory framework.

While such procedure is explicitly foreseen in the context of high-risk AI systems (through delegated powers granted to the European Commission), this procedure is currently lacking as regards the updating of the list of prohibited AI systems.

Some members therefore pointed out that it may be advisable to include such a procedure also for the list of prohibited systems, in order to enable its period review and revision, just as is the case for high-risk AI systems. Other members, however, disagreed, and noted that the line between prohibited systems and high-risk systems should remain in place, in particular by ensuring that the list of prohibited systems can only be revised through an amendment of the regulation itself.

In any event, when the Commission applies its delegated powers to update these lists, it is essential that it ensures full transparency during the entire process and involves a broad set of stakeholders, so that representatives of civil society, industry, academia and the public sector can have their voices heard. Furthermore, the Commission should ensure that the delegated acts come with adequate transition time as development and testing of certain AI systems may take a long time.

3) The Scope of the Regulation requires further refinement

The approach in the proposed AI regulation consists of providing a broad definition of AI, by including both new and old approaches to this technology (e.g. not only machine learning but also symbolic logic). Many members considered that this approach is helpful to evaluate as many AI innovations as possible, since the focus should lay on the potentially problematic use rather than the underlying technology. If the same harmful conduct can be enabled through a classical type of AI system, this is equally problematic from a fundamental rights point of view. The broad definition of AI is supplemented with an Annex of concrete technologies that fall under its scope. One downside to this list concerns the fact that the quality of the scope of this regulation is now largely influenced by this annex (and by the clarity and comprehensiveness of the concepts listed in there), which relies on efforts from the Commission who can review this list over time.

What is more, the list may ultimately lead to regulation shopping; innovations could be defined or framed by AI developers in a different way so as to fall inside or outside of the list, hence potentially leading to under-enforcement. The regulation's scope is, after all, mostly defined by whether or not a given application falls under any of the listed risk-categories (i.e., prohibited, high-risk, or requiring further transparency), and thereby excludes (AI) systems that do not fall under those problematic categories. Given the focus on the problematic use / consequences of technology rather than on the technology itself, many members propose keeping a broad definition of 'AI', which could, for instance, cover each practice or system that relies on automated processes, in particular where information is collected to make a choice among options. Hence, for each such practice or system it should be verified whether it falls under the risk categories covered by this regulation or not. Otherwise, the regulation risks having a bias towards problematic uses only by known/hyped AI systems, rather than by systems that potentially cause the same problematic impact but are not listed in Annex I.

At the same time, however, some members also considered that, instead, the current definition is overly broad and also captures software which are not AI systems. They propose instead that the scope should be limited to AI systems which generate outputs that are not predetermined by

the natural person developing the system. They stress that, in fact, some AI tools often have no broader purpose beyond serving as building blocks for various user-designed applications, which in turn serve more specific user-generated intended purpose; such general-purpose tools are not in and of themselves AI systems, but rather serve as components or precursors of AI systems. The text of the Regulation should hence be more explicit regarding the allocation of responsibilities when it comes to general purpose tools, as – in that case – it is the user who often ultimately decides on the intended use of the AI system rather than the provider.

Furthermore, the proposed definition also seems to focus on AI as a software exclusively. This can cause some concerns from the scientific community around the exclusion of AI as a hardware (e.g. in robotic devices). If the aim is to secure a broader definition of AI (which includes robotics), this should ideally be clarified in the text or through other guidance documents. Similarly, it would be beneficial to provide more clarity on whether and to which extent AI research is seen in scope of the AI Act, given that it is not directly related to putting an AI product in service or on the market.

Finally, attention can be drawn to sectorial legislation that already legislates AI systems, in particular the medical device and in-vitro diagnostic regulation. The potential legislative and standardization overlap brings a risk of conflicts and could increase costs for AI providers, which – in the area of AI in healthcare, for instance – may ultimately be transposed onto the healthcare system or the patient. Great care should hence be taken to align the definitions and requirements of the proposed regulation and existing sectorial legislation.

4) Further clarifications are needed as regards certain terms

*Putting on the Market/Into service***:** The proposal specifies that AI systems should comply with the regulation when “placed on the market” or “put into service”. This concept is already well-established and documented in existing legislation relating to physical products, but for digital products this concept is quite new. As digital systems often undergo multiple iterations and developments before they are considered fully implemented and ready to release, clarification is needed on when the AI system should be compliant. Some members pointed out that if, for example, compliance should already be ensured when a proof of concept is delivered to a client, this would significantly increase the costs of developing an AI business case while at that point there is no certainty the application will actually be purchased by the client.

Citizen Scoring: Public services already assign scores to citizens in numerous contexts (from verifying eligibility to social benefits, to the risk of recidivism, and from the need for intervention to protect / place children to the chances of easily finding a job). Further clarification about the practices that fall under the prohibition on general citizen scoring would hence be welcomed, as the language that is currently used in the proposed regulation, and the examples provided by the European Commission in its presentations, are not always clear.

Remote biometric identification system: The current definition is not entirely clear. Some may argue that “remote” is referring to cloud services, while others will consider this as referring to no-physical-contact identification systems (such as cameras). For reasons of legal certainty, it would be good to clarify this.

Task allocation: Annex III bullet 4(b) considers AI systems as high-risk if these are used for task allocation in the context of employment, workers management and access to self-employment. Already today, a lot of software is used to assign tasks in production plants, call-centers,

distribution and warehousing plants, repair and maintenance scheduling, worklist orchestrators for homecare providers, or even to assign testing and coding tasks in software development pipelines. Further clarification is therefore needed on which type of system falls in scope of this category.

Under their authority (user): Article 3(4) defines a user *as any natural or legal person […] using an AI system under its authority, except* […]. Given the importance thereof to understand the scope of the legal obligations for AI actors involved, the term "under their authority" should be clarified.

Deployer: Some members suggested that it could be useful to give a definition of 'deployer'. For instance, a 'deployer' could refer to the entity that makes the AI system available for use in a specific operational context. Sometimes (e.g., if the system is custom-built for the deployer by a developer) the deployer might be the same as the provider. But this may not always be the case, for instance if general purpose AI systems are being used.

Beyond these examples, several members pointed out - as overall comment on the Proposal - that its language is more generally too vague for a legislative document. As a result, a number of important terms are left undefined. Examples include terms such as 'state of the art', 'robustness', 'error' in the context of 'error-free datasets', 'entire-life cycle' of an AI system or 'impact on children'. The risk of using language which is too vague is that the obligations that flow from it may be under- of over-inclusive.

Furthermore, the explanatory memorandum (section 3) indicates that the Commission's survey highlighted the need to define the notions of 'risk' and 'harm'. However, neither is currently defined in the proposal and, throughout the Act, the term 'risk' is used in relation to many, often disparate meanings of harm. Some articles in the proposal relate to harm to health, safety and fundamental rights, others to breach of obligations to protect fundamental rights, or more vaguely 'other aspects of public interest protection', yet other articles refer to harm to critical infrastructure or harm to fundamental rights of data subjects. In addition, some articles point to the definition of 'product presenting a risk' in the market surveillance regulation, but that definition refers to risks at national level and may hence not be applicable to risks to the individual where the AI system is customized/trained on the data of one person. The market surveillance definition also does not apply to AI systems sold as a service and lacks a clear inclusion of harm to fundamental rights. It would therefore be advisable to more clearly define these terms in the proposal itself, and to align the different articles that relate to risk.

5) The requirement of *ex ante* third party conformity assessments could potentially be extended in certain cases

Currently, the proposal stipulates that only AI systems intended to be used for 'real-time' and 'post' remote biometric identification of natural persons will be subject to an *ex ante* third party conformity assessment. Other AI systems classified as high-risk, like those used in the context of recruitment or predictive policing, will be subject to self-assessment by the provider.

However, given the fact that such high-risk systems pose significant risks for individuals in terms of fundamental rights and societal impact, some members raised the need to consider whether the requirement of third-party conformity assessments should be extended to all high-risk AI systems. Such extension could be beneficial for all parties concerned, as it can enhance trust in

the fact that the AI systems meet the required standards. Moreover, this could also improve legal certainty by further reducing the risk of liability claims for unintended consequences of these high-risk AI systems. In such case, specific provisions about the status of auditors would be welcome.

Other members, however, disagreed on this point. They consider that the application of third-party conformity assessments would go against the goal of taking a risk-based approach. They also noted that the use of third-party conformity assessment for only one high-risk AI system makes sense because that system, in different circumstances, is prohibited.

6) The value of the proposed CE marking is questioned

The CE-marking for AI applications in Europe can help to create trust and assurance in technology that is complex to understand for users. However, with the CE-marking, certain risks arise such as a potential false flag for unreliable products being marketed in Europe. To achieve the trustworthiness of such a CE-marking, there is a big need to have standards to support organizations to comply with the requirements. As it is, these standards do not yet exist, and it will take a huge effort to ensure that they are published in time before this regulation comes into effect.

In this regard, when setting up these standards or best practices, it is also important to consider the views of various stakeholders, including civil society, so as to ensure that compliance with the requirements is not only claimed but can also be demonstrated and lead to *earned* trust.

Moreover, the CE-marking has been developed for 'hardware' and it is unclear how it would work for software, from the basics – of how it can be affixed – to the more complicated issue of how it would work in practice. This provision seems telling of the Commission's approach to AI coming from a 'product liability' perspective, which can present serious limitations in certain instances, given the nature of AI. Indeed, many of the obligations set out in the Regulation seem most appropriate for the products covered in Annex II, such as the requirement to comply with harmonized standards or to undergo a new conformity assessment every time there is a substantial modification. These obligations may, however, be less suitable for AI services, since these services can often be deployed in an almost unlimited range of scenarios, and are already frequently updated.

7) There is a need for guidance on how to implement the various requirements

As noted above, many of the requirements contain vague language, and will hence need to be clarified through guidance from the European Commission in order to ensure their implementation. In this regard, lessons should be drawn from the implementation of the GDPR, where a lack of guidance in combination with high potential fines prompted organizations to massively seek consent from data subject, leading to overflooding citizens with messages and legal uncertainty on how to comply. To avoid the difficulties in interpretation that seem to be prevalent with the GDPR, it is important that guidance be provided at the European level (including through the European Artificial Intelligence Board). Providers, importers and users of AI operate in different countries and do business across the EU – they hence need uniform guidance to implement these requirements, regardless of the member state in which they primarily operate.

Attention should also be given to the way in which different types of AI work, such as platform and general-purpose systems. These systems may not be high-risk in the form initially placed on the

market, but may nonetheless be caught by the Regulation if used in a high-risk context later on. Unlike standalone AI systems, it would not always be feasible or desirable for providers to prescribe specific intended uses of these systems, as this may unduly restrict the customer's ability to deploy the system in an innovate way.

Further, given that the user will often control how these systems are used – including whether they are used in high-risk scenarios – it may be appropriate to place certain compliance obligations on the user. At the moment, the way in which obligations are divided between providers and users can be confusing, which risks being an obstacle to innovation. While the proposal currently imposes the majority of its compliance obligations on the provider, on some occasions, and depending on the AI system at stake, the user may be better placed to ensure compliance with those obligations in practice. This can, for instance, be the case for some general purpose and platform AI systems, where the user may not only determine the intended use and context, but can often also provide the input data necessary to operate the system (which can have a substantial impact, for instance, on the system's accuracy or its potential bias). It should hence be considered whether additional obligations should be placed on the user from the outset, instead of only carving out circumstances in which a user may step into the shoes of the provider (Article 28(1)). In addition, it should be clarified whether (and if so, when) providers and organizational users of AI systems may contractually allocate their responsibilities under the proposal.

In addition, guidance is needed as regards compliance with Annex IV. Although the need to explication and/or documentation related to the AI system is clear, the technical documentation request is far from complete in order to protect individuals. The terms used are often too vague, and the description seems to be based on stand-alone AI systems, which profit from a human data entry for training input and older fashioned training techniques. This part should hence ideally be reviewed in order to avoid misunderstandings in the context of a serial or parallel AI system architecture, or the use of newer training techniques such as, for instance, single shot/few shot/incremental or transfer learning. Additional points such as the context in which the system has been trained could be very valid to include as well, in order to avoid unintentional misuse in another environment.

Finally, the Regulation should ideally also further clarify how providers of component parts should be treated (e.g., the provider of speech recognition technology in a broader AI system), since their position – including their responsibilities – are currently under-addressed.

8) Concerns about the regulation's enforcement mechanism should be addressed

The proposed regulation sets out various requirements that AI providers and users will need to meet, and establishes an enforcement structure to ensure compliance with those requirements. During the AI4Belgium feedback session, an overwhelming majority of members indicated their preference for a shared governance and enforcement approach, with a good balance between the national and the EU level. Currently, the regulation lays more focus on the national supervisory authorities who will be first in line to implement and enforce this regulation. However, lessons should in this regard be learned from the enforcement structure of the GDPR, where the guidance given by national DPA's was quite limited in the beginning. As an example, the first code of conduct was approved by the Belgian Data Protection Authority (DPA) 3 years after the GDPR came into effect. Moreover, enforcement of the GDPR is also the responsibility of national

authorities and – due to unequal investments in the various member states' authorities – citizen protection is not at the same level in each EU country.

Also in the context of this regulation, it should be considered that too much emphasis on the national level can lead to a risk of unequal implementation in different member states, at different speeds and potentially different interpretations. Belgium has, for instance, been lagging behind with regard to the implementation of the GDPR; this delay may affect innovation and a European level playing field, and the same risks to happen in the field of AI. Strong coordination at the European level will hence be crucial; also given the fact that many AI systems may be used transnationally and may be imported from third party countries. Moreover, given the importance of the risks attached to the use of AI as set out in this regulation, it will be essential that these authorities receive proper funding (and a sufficiently skilled workforce – which may be difficult in this field) so that they can provide adequate guidance for organizations and ensure a high level of citizen protection.

The issue of different implementation speeds will also affect the creation of codes of conduct that can be voluntarily applied to AI systems other than high-risk systems. If it is assumed that the creation of a code of conduct is roughly the same effort and cost for any sector or member state, this absolute cost will mean that there may be more codes of conducts for sectors and member states with a higher turnover. Smaller member states with smaller markets will thus likely have less means to create these codes of conduct. This is another reason why a common European approach would be preferential.

In this regard, the obligation to appoint an authorized representative established in the European Union in case an importer cannot be identified (recital 56 and article 25) is welcomed. Building on the experience with the GDPR, it is crucial to allow all organizations in charge of the implementation and enforcement of the regulation – be it the national competent authorities (NCAs), market surveillance authorities or other bodies – to be able to conduct all necessary steps towards the authorized representative, independently of where in the European Union it is established. Related to this point, it is essential that several NCAs can oversee the notified bodies and technical services performing the conformity assessment. In other words, not only the NCA of the country in which the notified bodies and technical services are established, but also NCA from other European member states should be able to do so, especially to ensure protection in case a specific NCA would be too under-resourced.

Furthermore, while currently not foreseen in the proposed regulation, citizens should be provided with measures for redress and a right to file a complaint with national authorities, since this will not only help closing the protection gap of the proposal, but it can also help national authorities to assess and establish potential breaches of the regulation. In this way, public and private enforcement can be more complementary, and citizens will have a more active role in ensuring the protection of their rights. In the same line of thought, the link between the GDPR and this regulation should be highlighted.

More than the fact that the Proposal does not, currently, foresee any mechanisms through which citizens can file a complaint, it seems to ignore the rights of citizens altogether. Despite the fact that the Recitals make numerous references to protecting "health, safety and fundamental rights," the conceptual structure of the proposal is built on existing market surveillance schemes known from product safety legislation. The proposal seems to combine two concepts that are

fundamentally distinct: AI systems that are high-risk in the context of safety and health under the product safety legislative framework and stand-alone high-risk AI-systems that may have otherwise an impact on people's live or pose risks to fundamental rights. It is questionable whether the same requirements designed for product safety will indeed result in the protection of those rights (such as non-discrimination, privacy, fairness etc.), especially without specific rights allocated to individuals. Individuals should therefore be provided with substantive rights in the proposal, such as the right not to be subjected to prohibited AI systems, or the right not to be subjected to high-risk AI systems that do not comply with the proposal's requirements.

In this regard, it should also be noted that the proposed AI Act prescribes human oversight, transparency and provision of information to users of high-risk AI systems. However, considering that Article 3(4) defines 'user' as a professional user, the unintended side effect is that non-professional users of AI systems do not benefit from a similar level of protection in the form of transparency and information. Such protection is however essential to not just create trust with professional users of AI systems, but also with citizens and consumers that use such systems or are otherwise affected thereby. It is therefore important to extend the transparency requirements towards all users of AI systems, including non-professional ones.

Finally, the creation of an EU database for high-risk AI systems deployed in Europe is a welcome development, as it provides for more transparency that can benefit both public and private enforcement of the regulation and of fundamental rights that can potentially be breached by the use of AI. Some members suggested, given the crucial task of the public sector and the importance to secure trust and transparency, to broaden this database to include all AI systems used by the public sector rather than only those that were explicitly listed as high-risk. At the same time, it should then be ensured that such extension does not unduly raise the administrative burden of civil servants.

9) Additional efforts are needed to stimulate innovation

The abovementioned issue of different member states' speeds of implementation of the regulation risks being even more prevalent with regard to regulatory sandboxes, as the Commission expects the initiative to be taken by national competent authorities and member states. However, these sandboxes will be crucial to stimulate innovation in AI and ensure that European citizens can also benefit from the opportunities of this technology. In order to mitigate this issue, additional measures should hence be taken to incentivize the establishment of regulatory sandboxes at member state level.

Indeed, while it is positive that the Commission urges Member States to set up regulatory sandboxes, this process should be further formalized. Regulatory sandboxes can only foster innovation if they are supported by adequate incentives. The relevant national authorities, like the national data protection authorities, need to build competences and experience in this area, and should be supported by the Commission on this. Adequate funding and skilled personnel are also essential. Sandboxes should be closely monitored, and information about regulatory sandboxing initiatives should be shared as openly as possible to provide learning opportunities and best practices for other member states, and transparency for all those who may be affected.

Finally, the measures to help small scale AI providers and users may need to be extended. While such providers and users have priority access to regulatory sandboxes, participating in them will

require a huge time and resource investment from their side. Hence, they may need to be financially encouraged to participate. While a reduction of the cost of third-party conformity assessment for small scale providers and users is welcome, this should be further extended to specific funding for organizations who undergo a self-assessment procedure. In Belgium and elsewhere, we see that start-ups, scale-ups and SMEs develop many of the most innovative AI applications. Without adequate incentives, this regulation may put them at a competitive disadvantage compared to bigger companies who already have a lot of experience with compliance mechanisms.

10) More attention should be given to the impact of AI on societal interests and the environment

While the proposed AI regulation certainly advances citizens' protection against AI's adverse impact by countering some of the risks posed thereby, many have raised that the attention to collective and societal interests is fairly limited (as opposed to risks to individual interests). For instance, the adverse effects that the use of AI can have on the rule of law or on the integrity of the democratic process, does not seem to be tackled through this regulation, nor is the environmental impact of AI systems. The focus is currently placed on individual human rights, yet AI might also affect groups of people, not only according the traditional criteria (race, political, religious or philosophical opinions) but also based on less traditional profiling criteria, as well as society at large.

There is hence further scope left to provide attention to these aspects, and grant the public a greater role to counter these risks. This can be done, for instance, by allowing individuals or associations to file complaints with supervisory authorities, providing for collective redress mechanisms, and stimulate public interest litigation against uses of AI that may breach public values – for instance through the cumulative effects of the use of AI systems on a wider scale. In addition, stakeholder consultations should be organized at a frequent basis in order to determine the extent to which the regulation needs periodic revision to effectively counter the risks of problematic AI practices.

Some members noted that this attention to societal risks of AI systems should be reflected in the list of high-risk AI systems (e.g. through the inclusion of AI systems present on the web that recommend content or that moderate content and generate risks for freedom of expression and information and therefore for democracy, as reflected in the EP resolution on an ethical framework for AI (2020/2012(INL))). In the same vein, some suggested this should be reflected in the list of prohibited AI systems. Notably, in their joint comment on the proposed regulation, the EBDP/EDPS advocated that all remote biometric identification in public spaces should be prohibited as it generates extremely high risks for non-democratic intrusion into individuals' private life. Similarly, emotion recognition systems might also pose an unduly high risk to societal interests that may not be justified in a democratic society.

Evidently, countering AI's societal (and individual) impact necessitates not only protective measures on the supply side, but also broader awareness and education initiatives to ensure that citizens are well-equipped to understand the potential risks that accompany AI's opportunities. Such increased awareness will also contribute to the enforcement of the proposed regulation.