/ Submission to the European Commission's Consultation on a Draft Artificial Intelligence (AI) Act

Draft AI Act: EU needs to live up to its own ambitions in terms of governance and enforcement

August 2021

AlgorithmWatch welcomes the European Commission's efforts to develop a framework for the governance of AI-based systems that is based on European values and the protection of fundamental rights. However, we fear that in its current version, the draft Artificial Intelligence Act would not reliably and comprehensively accomplish its stated objectives. We, therefore, call upon the Council and the Parliament to take appropriate measures to correct its shortcomings, clarify its ambiguities, and enhance its consistency, ultimately turning the Act into an effective means for using AI-based systems to the benefit of people—and not to their detriment.

Our Perspective

AlgorithmWatch is a non-profit research and advocacy organization that is committed to watch, unpack and analyze automated decision-making (ADM) systems and their impact on society. While the prudent use of ADM systems can benefit individuals and communities, they come with great risks to both individual autonomy and freedom as well as to society and the common good as a whole.

Therefore, guided by the principles of autonomy, justice, harm prevention, and beneficence, and oriented at the cornerstones of democratic societies and the protection of fundamental rights, we consider it crucial to make ADM systems transparent and hold them accountable to democratic control. Through our work, we aim at contributing to a fair and inclusive society and to maximizing and justly distributing the benefit of ADM systems for both individuals and the collective.

We submit the present **position paper** as part of the official public consultation on the proposed Artificial Intelligence Act (AI Act), commenting in detail on specific aspects without in any way intending or claiming to cover the entirety of this very complex regulatory proposal. The following reflections build upon AlgorithmWatch's contribution to the public consultation on the White Paper on Artificial Intelligence[1] as well as on our first analysis of the draft AI Act published shortly after its release.[2]

The Draft AI Act—Setting the Agenda Toward a Governance Framework on AI

The Commission's proposal will profoundly shape AI regulation in the next decades, not only in Europe but across the globe—through its direct legal extraterritorial effects as well as through its political implications. We appreciate the **agenda-setting character of the proposal**, which will likely stimulate the urgently needed debate on the governance of ADM systems. The fact that the EU is now proactively engaging in and promoting this debate presents an opportunity—both within the EU and beyond—for the development of consistent governance approaches.

As to its **overall substantial approach:** In contrast to the White Paper, whose narrative suggested a worrisome reversal of EU priorities by putting global competitiveness ahead of the protection of fundamental rights, the new proposal sets out with the prohibition of AI practices it declares to be in breach with Union values and fundamental rights protected under Union Law. At the same time, the draft Act is a complex piece of regulation with a variety of interdependencies with already existing norms, and it is not easy to foresee the effects it is going to have and the ways it is going to interact with these other regulatory frameworks. On closer inspection, many of the instruments it proposes turn out to be vague or risk becoming toothless or even self-defeating in practice, which very much contradicts the idea of a regulation that aims to increase legal certainty and that puts fundamental rights first.

- As AlgorithmWatch, we oppose the narrative that citizens' trust serves as a means to innovation, implicitly classifying the latter as the ultimate end. **While we very much agree with the importance and recognize the potential benefits of innovation, we regard individual autonomy and the common good as the ultimate benchmarks against which to set legal standards. It is now up to the Parliament and the Council to clarify the Act's ambiguities, correct its shortcomings, and enshrine reliable safeguards.**

Below you find our recommendations on selected issues in more detail.

1 Better Define the Far-Reaching and Broad but Porous Scope of the Act

The scope of the proposed Act is both far-reaching and broad—but at the same time porous in important respects.

I We welcome the proposal's focus on the *use* of AI-based systems as well as its broad take on what counts as such a system. At the same time, we stress that the need to regulate a system is not triggered by what specific type of technology it is, but by the impact it has on individuals and society. Thus, **impact should be the decisive factor in defining the scope of systems regulated by the Act**—rather than the way this impact came about. In our view, the concept of **automated / algorithmic decision-making systems** would more precisely capture this aspect, focusing on

[1] https://algorithmwatch.org/en/response-european-commission-ai-consultation/
[2] https://algorithmwatch.org/en/response-to-eu-ai-regulation-proposal-2021/

systems that are used to predict, prescribe, or make decisions with effects on human beings. It underlines the socio-technical nature of such systems, which are inevitably embedded in societal contexts that need to be taken into account when assessing the implications of their use.[3] We strongly agree with the European Center for Not-for-Profit Law's position that the risks and opportunities of AI systems should not be judged on a binary basis. Instead, it is necessary to account for the targeted population, context, and situation when considering the risks and opportunities of these systems.[4] In addition, the definition setting the scope of the Act focuses on the type of technology involved, which opens the door for operators to circumvent the scope of its provision by denying that their system falls under the respective definition.

II In general, the proposed Act covers uses by both **public and private actors**, which presents a critical opportunity to streamline requirements on uses where fundamental rights are concerned, regardless of the actors involved. However, specific provisions are limited to public authorities. Some of them explicitly mention that they also apply to private actors acting on behalf of public authorities or in the framework of Public-Private-Partnerships. At the same time, the absence of this key addition in other provisions indicates that the extension to such private actors does not automatically apply, creating potential loopholes public authorities could try to exploit by outsourcing the use of certain systems.

III Another aspect that is important for the effective protection of fundamental rights and that we welcome is the applicatory geographical scope of the proposed Act, which would apply whenever an AI-based system is used within the EU, regardless of where the operator is based—or whenever an output of such a system is used within the EU, regardless of where the system itself is based (Art. 2(1)). The **wide extraterritorial effects this implies ensure that geographical loopholes cannot be exploited to evade the Act's reach, guaranteeing protection across the Union.** At the same time, focusing on the location where a system is used implies that neither the development nor the sale and export of any systems are covered by the Act if they are put to use elsewhere—including systems whose use would be prohibited or classified as high-risk according to the Act. From a fundamental rights perspective, this creates a **protection vacuum for people in third states**, whose rights could be infringed by the uses of AI systems developed by EU-based providers.

IV A related loophole stems from excluding from the scope of the proposed regulation any systems used by public authorities in third states or international organizations in the framework of international law enforcement and judicial cooperation with the EU or its Member States (Art. 2(4)).

- **We call on the Council and the Parliament to clarify the applicatory scope of the AI Act with regard to the above aspects, making sure it is a coherent, consistent, and reliable instrument for protecting human beings from violations of their fundamental rights caused by the use of ADM systems—regardless of the specific technology or the type of actors involved.**

2 Mitigate the Self-Defeating Potential of the Risk-based Approach

It is a key achievement that the Commission **recognizes that the use of AI-based systems can come with serious risks for fundamental rights and that these risks need to be addressed by a governance framework**, and this is an important message by itself that should be recognized as such. We are relieved to see that the approach has improved compared to the White Paper, recognizing sensitive areas, such as when AI systems are used for recruiting, to evaluate creditworthiness, to determine access to social benefits, for predictive policing, to control migration, and to assist judicial interpretation. Furthermore, the misleading criterion 'sector' to determine high-risk AI practices has

[3] Following our definition, ADM systems encompass the design procedures to gather data, the collection of data, the development of algorithms to analyze the data, the interpretation of the results of this analysis based on a human-defined interpretation model, and the automatic action based on the interpretation as determined in a human-defined decision-making model.

[4] ECNL Position Statement on the EU AI Act, 23 July 2021, https://ecnl.org/sites/default/files/2021-07/ECNL%20EU%20AI%20Act%20Position%20Paper.pdf

been replaced by more appropriate criteria, including the extent of the use of the application and its intended purpose, the number of potentially affected persons and their vulnerabilities, or the dependency on the outcome and the irreversibility of harms (Art. 7(2)). However, we have **major doubts that the risk-based approach is appropriate** for several reasons.

I In general, while we support the approach of subjecting systems to transparency requirements, it should not be overlooked that the Commission, by introducing such a high-risk category, **explicitly allows and legitimizes the use of the systems belonging to that category**. However, many of these sensitive applications have not yet been the object of public debate. Before they are put to use, citizens should have the opportunity to discuss whether there are limits to what decisions should be automated in the first place. The Act precludes this opportunity by proactively permitting these systems to be put to use. Where implications for fundamental rights are uncertain, a precautionary approach could be the more appropriate option.

II A further critique concerns the way of **categorizing applications according to their risk levels**. Though the list of applications within these eight areas (Annex III) is amendable by the Commission, the eight areas themselves are not (Art. 7(1)(a)), which undermines the intention of the Commission to make the regulation future-proof. Moreover, it remains nebulous when the threshold of high-risk, as defined in Article 7(2), will be reached, i.e., when a system's risk count as "equivalent to or greater" than those of other systems already on the list. As a result, it is neither clear on what basis the current list of high-risk applications has been compiled, nor what will be considered as sufficient ground with respect to future risk classification. In addition, the clause "AI systems *intended* to be used", applied throughout Annex III, grants wide scope for interpretation—and wide opportunities for operators to evade being subjected to the requirements for high-risk systems by simply denying such an intention.

III Moreover, the idea of denoting eight areas of applications as high-risk does not seem to adequately consider the very likely possibility **that systems that were, from an ex-ante perspective, not classified as high-risk under the current proposal will turn out to have severe and detrimental impacts** on individuals and societies. First, the proposal leaves a major part of AI systems completely out of sight, stipulating ex-ante that they do not involve any risks and thus do not have to be subject to any scrutiny. Second, while there are some transparency obligations for specific limited risk systems in Article 52, namely for those interacting with natural persons (such as chatbots), emotional recognition and biometric categorization systems, as well as systems used to generate or manipulate content (such as 'deepfakes'), these obligations do not go far enough. Emotional recognition and biometric categorization systems as well as those involving deepfakes are all applications that are likely to come with a high potential of severe harm to individuals and democratic societies. What is more, the scientific basis, especially of emotional recognition systems, is highly disputed. The already minimal transparency obligations applying to this set of AI systems are further weakened by a range of exemptions (such as for the use of chatbots or biometric categorization systems for the prevention, investigation, or prosecution of crimes).

- **To address these concerns, we recommend that it be mandatory for every system deployed by public or private actors to conduct an impact assessment, allowing to determine their respective risk levels on a case-by-case basis**. Optimally, this could be done by means of a two-stage impact assessment procedure: At its first stage, a low threshold, non-bureaucratic checklist serves as a triage in order to detect risk signals a specific system comes with. If such risk signals are detected, then as a second step, a comprehensive transparency report should be provided, containing relevant information on how these risks are addressed and brought under human control.[5] Such a two-stage procedure would allow for a context-sensitive impact assessment, mitigating the danger that apparently harmless systems (that the draft Act would

[5] Cf. Loi, Michele / Mätzener, Anna / Müller, Angela / Spielkamp, Matthias: Automated Decision-Making Systems in the Public Sector – An Impact Assessment Tool for Public Authorities, 22 June 2021, https://algorithmwatch.org/en/adms-impact-assessment-public-sector-algorithmwatch/

classify as low-risk or no-risk) turn out to have major negative impacts on individuals and society. **We call on the Council and the Parliament to reconsider the specific approach of risk categories of the Commission's proposal in light of the above reflections.**

IV Moreover, the Commission's **harmonization efforts may have self-defeating effects**, undermining the initial intention of subjecting AI systems to greater—rather than less—scrutiny. On the one hand, the introduction of the high-risk category as the core of its proposal may unacceptably preclude Member States from introducing stricter or additional requirements in domestic law for systems beyond this category.[6] On the other hand, as soon as a high-risk system has the CE marking[7] affixed, Member States are no longer allowed to "create unjustified obstacles" on their use (para. 67), a requirement that urgently calls for clarification.[8]

/ **The Council and the Parliament must make sure that the Act's harmonization efforts do not result in ADM systems being scrutinized less thoroughly. Member States must have the right to subject such systems to additional requirements in order to mitigate their potentially harmful impact.**

3 Make Sure Risk-Assessment is More than a Fig Leaf

A further concern refers to the requirements to which operators (providers and users) are subjected. In general, AlgorithmWatch has long advocated for the instrumental role of transparency in furthering a responsible use of AI that benefits individuals and society. Against this background, we applaud the Commission for recognizing the instrumental value of **transparency,** and we support the approach of subjecting operators of AI systems to a variety of requirements in terms of transparency and risk-assessment, which creates an incentive to promote compliance-by-design approaches. Yet, it must be **ensured that these requirements do not end up as mere fig leaves**.

I Article 43 stipulates that only AI systems intended to be used for remote biometric identification are subject to third-party conformity assessment by notified bodies, while **for all other AI systems classified as high-risk, a self-assessment by the provider will suffice**, including systems used in sensitive areas such as predictive policing, migration control, or recruitment. Most requirements apply to the provider of a system (as opposed to its user, that is the one deploying it, who has fewer obligations). In most cases, providers of AI systems are **corporate actors**. In our view, it is unacceptable to leave such an important assessment solely to (mostly) corporate actors who have a great self-interest in the deployment of these systems. Systems that are likely to have consequential effects on individuals and society—or that threaten to come with special risks—should be subject to adequate third-party oversight.

II According to the proposal, the conformity assessment operators will have to conduct is the assessment of whether they are either in conformity with the essential requirements of the Act or with the standards developed on their basis. In the words of the Act, **systems in conformity with harmonized standards will be presumed to be in conformity with the requirements the Act sets for high-risk systems** (Art. 40). This raises a variety of questions: First, this presumption of conformity also seems to apply to biometric identification systems, the only use case for the assessment of which a third-party notified body would actually be foreseen. Thus, there is some uncertainty in the current proposal as to the role—and effective influence—of notified bodies, even where they are foreseen. Second, while the introduction of technical standards can be a valuable means toward regulating rapidly developing fields, standardization procedures tend to be opaque, prone to industry lobbying, and hardly accessible to all relevant stakeholders—especially not to civil

[6] Cf. Veale, Michael / Zuiderveen Borgesius, Frederik, «Demystifying the Draft EU Artificial Intelligence Act», in Computer Law Review International 22(4), 2021 (forthcoming), preprint available at https://osf.io/preprints/socarxiv/38p5f, pp. 20-23.
[7] The Conformitè Europëenne (CE) mark is the EU's mandatory conformity marking which regulates the goods sold within the European Economic Area.
[8] Cf. DGB, Initial Assessment of Issues Relevant to Labour Policy on the Draft of the EU Commission on a European AI Regulation, 21 April 2021, https://www.dgb.de/-/08J, p. 5.

society and those affected. What is more, technical standardization agencies often lack expertise on fundamental rights—the protection of which is the ultimate objective of the Act and must thus also foundationally guide any standards developed on it.[9]

III Likewise, the exceptional permission to derogate from the conformity assessment for public security reasons (Article 47) threatens to undermine the intention of the Commission's approach by opening up ways for authorities to circumvent the requirements.

/ **We urge the Commission—in its collaboration with standardization agencies—to ensure that the standardization procedures are conducted in a transparent, inclusive, and democratic way, including experts and civil society, in order to ensure they indeed do contribute to the protection of the values the Act is based on.**

/ **The Council and the Parliament should make sure that there is a comprehensive conformity assessment that is not rendered void, cannot be circumvented, takes place within an unambiguous governance structure, and adequately includes third-party oversight.**

In this regard, it is crucial to recognize that at all stages of the lifecycle of the system—from its development to its deployment—transparency, auditing, and control mechanism can be introduced: It is important to counter the misguided view that "self-learning" systems can, once they are in use, no longer be understood or controlled.

IV In addition, with respect to the substance of the **risk management requirements** to which the proposal subjects operators of high-risk systems, we stress that the issue of **discrimination, unequal treatment, and injustices** needs to be addressed more comprehensively. Discriminatory, unfair, and unjust effects do not always stem from bias in training data, and thus cannot merely be avoided by ensuring data quality. AI-based systems are socio-technical systems that are deployed in a certain societal context, the norms, values, and structural inequalities of which will inevitably influence the system's implications. Moreover, an aspect the requirements do not adequately consider is the enormous **resource consumption** that comes with the development and operation of AI-based systems.

/ **We, therefore, call upon the Council and the Parliament to include further and broader frameworks in the Regulation to address discriminatory and unjust effects of ADM systems and include explicit sustainability-related requirements.**

4 Make Use of the Potential of the EU Database as a Step Toward Greater Transparency

While we are concerned about the lack of clarity with respect to the high-risk classification, we welcome the introduction of an EU database for stand-alone high-risk AI practices that is accessible to the public. This is a promising first step toward greater transparency and corresponds to AlgorithmWatch's calls for **public registers** and improved **data access for public interest research**.

I However, in order to make full use of the transparency potential of publicly accessible registers, the database should **not only include high-risk systems** but—with regard to the public sector—be complemented by a list of all ADM systems in use by public authorities, regardless of their assigned risk level.[10] In addition, the register should include systems operated by private actors whenever their use has a significant impact on an individual, a specific group, or society at large.

II Moreover, the **information provided** must include the purpose of the system, an explanation of the model (logic involved), and details on the actors involved in developing and deploying the system, as well as the results of any algorithmic impact assessment / human rights impact

[9] Cf. Veale / Zuiderveen Borgesius, «Demystifying the Draft EU Artificial Intelligence Act», pp. 14-17.
[10] For further information on the idea of public registers of AI systems used by the public sector see our response to the European Commission's consultation on AI with Access Now: https://algorithmwatch.org/en/response-european-commission-ai-consultation/

assessment undertaken. In addition, these requirements should apply to all systems regardless of their purpose. We thus believe that exceptions for certain areas of application, such as those provided for in Annex 8(11), are not the right way to go. However, in cases where full public disclosure cannot be granted—for legitimate reasons that need to be clearly defined—the database should include information of the respective body to which such full transparency was granted (for example, the national supervisory authority).

III Furthermore, as to **format**, it is important that the information provided in the EU database is genuinely accessible to and useful for the public—to both researchers and those affected by the systems. Such data will not only enable public interest research and thus contribute to an evidence-based democratic debate on the use and impacts of ADM systems, but it will also give access to information for those affected—a necessary first step for them to be in a position to challenge systems' outputs.

/ **For it to be an effective means toward greater transparency and toward shedding light onto the black box, Council and Parliament must enhance the EU database accordingly. We call upon them to expand the scope of systems included in it to non-high-risk systems and to complement the information required in Annex VIII with the above-listed aspects. Article 60(3) should specify that the information must be provided in an easily readable and accessible manner, including structured digital data based on a standardized protocol.**

5 Clarify Enforcement Mechanisms and Equip Bodies with the Necessary Means

Transparency requirements are a necessary (though not yet sufficient) means toward a responsible use of ADM systems. However, for them to make a difference on the ground, they must be effectively enforceable.

I According to the proposal, its **enforcement** lies to a great extent with Member States. However, the interactions between the EU and Member States authorities are complex and their respective roles not fully clarified. The European Artificial Intelligence Board (EAIB) may importantly contribute to strengthening oversight and supervision, but it must be ensured it has the corresponding power, capacity, and independence to do so.[11]

II The same requirement applies to national authorities: They must be equipped with the expertise and resources to effectively fulfill their tasks. The number of 1 to 25 full-time equivalent positions, which the proposal foresees for national supervisory authorities, is clearly insufficient in this regard.

/ **The Council and the Parliament must take the opportunity and clarify the roles of the entities involved in enforcement. These entities must be sufficiently independent, adequately resourced, and have the relevant expertise—in both technology and fundamental rights—to fulfill the tasks assigned to them.**

6 Focus Accountability Frameworks on Those Affected

Moreover, transparency—as a mere instrumental means to an end—must be coupled with adequate and reliable **accountability frameworks**. The Commission set out with the claim to set up a human-centric AI Framework that puts people first. We regret that the current proposal insufficiently addresses the **perspective of those affected** by the output of AI systems by not including any guidelines on remedies for individuals. **A regulation that is based on the objective of protecting fundamental rights must equip the bearers of these rights with the respective means to defend themselves if they feel they have been treated unlawfully**.

[11] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

I On the one hand, if such systems have consequential effects on people's lives, they must be able to retrieve all **relevant information**[12] about what has led to the outcome of the corresponding decision. In the public sector, individuals who were subject to a decision by a public authority that is solely or significantly informed by the output of an AI system should be notified without delay. Inter alia, holding ADM systems accountable also requires making training data and data results accessible to independent researchers, journalists, and civil society organizations. We thus suggest introducing legally binding **data access frameworks,** focused explicitly on supporting and enabling public interest research and in full respect of data protection and privacy law.

II On the other hand, those affected must also have the possibility to legally challenge outcomes. Thus, there must be **easily accessible, affordable, and effective legal remedies** at hand for affected individuals and groups to contest such decisions and, where appropriate, to demand reversal, reconsideration through a different procedure, or compensation. Mere technological solutions do not suffice to ensure that AI systems are used to the benefit of the many, not the few.

III Though the Commission has deliberately omitted this dimension in the proposed AI Act, the question of **liability** for any harm related to the use of ADM systems is critical in order to ensure comprehensive responsibility and accountability mechanisms. The question of how and to what extent providers, vendors, and users can be made liable must be addressed, be aligned to the AI Act, and be based on the objective of fundamental rights protection. At the same time, it must be guaranteed that representative actions for the protection of the collective interests of consumers and end-users concerning systems governed by the Act will be possible and accessible to affected individuals and groups.

IV A related question concerns the role of the third-party **notified bodies.** In the current proposal, it remains unclear whether the foreseen **appeal procedure** against their decisions in Article 45 is (genuinely) accessible to affected individuals and civil society, what bodies decide on these appeals, and what the implications are in case such appeals are successful.

/ **We expect the Parliament and the Council to step up for the bearers of fundamental rights and to introduce effective accountability mechanisms for those affected by systems' outputs, ensuring that those with less bargaining power have a voice, too. This includes a right to information, data access frameworks for public interest research, and effective legal remedies. Article 45 and the role of appeals against notified bodies must be clarified. Moreover, upcoming legislative revisions and initiatives concerning the liability framework must be aligned to the goal of fundamental rights protection. Effective collective redress mechanisms must be ensured.**

7 Effectively Draw a Red Line on Biometric Mass Surveillance

There has been growing pressure on the European Commission to explicitly ban biometric mass surveillance technologies.[13] Unfortunately, these calls have not sufficiently been taken into account: Although the proposed Act provides in Article 5 for the prohibition of "real-time" remote biometric identification systems in publicly accessible spaces for law enforcement purposes, there are too many worrisome exceptions and catches. In our view, the narrow scope of this prohibition does not

[12] The only exception being Article 52, which foresees transparency requirements vis-à-vis natural persons for systems with limited risks.

[13] Dozens of civil society organizations and digital rights activists, among them AlgorithmWatch, urged the European Commission to substantively enhance fundamental rights protections in the upcoming AI regulation and to close existing loopholes, see https://edri.org/wp-content/uploads/2021/01/EDRi-open-letter-AI-red-lines.pdf and https://edri.org/wp-content/uploads/2021/04/Letter-from-51-civil-society-organisations-seeking-your-support-for-a-ban-on-biometric-mass-surveillance-practices.pdf. The general call—not explicitly limited to biometric mass surveillance—was furthermore supported by 116 Members of the European Parliament via an open letter to President von der Leyen, https://edri.org/wp-content/uploads/2021/03/MEP-Letter-on-AI-and-fundamental-rights-1.pdf. Meanwhile, more than 57,000 European citizens have signed a petition for a ban on biometric mass surveillance practices as part of the Reclaim Your Face campaign, and the number continues to grow: https://reclaimyourface.eu/.

sufficiently consider that the wide-scale use of such systems can enable **indiscriminate mass surveillance, which is inherently incompatible with fundamental rights, creates chilling effects, and undermines fundamental principles of democratic societies.**

I First, the prohibition of the use of these systems should not be triggered by any specific type of technology but depend on the impacts they have: **Whenever biometric recognition systems enable indiscriminate mass surveillance, arbitrarily-targeted or discriminatorily-targeted surveillance, the use of these systems is incompatible with fundamental rights and should be banned.** In its current version, Article 5 does not live up to that demand.

II Second, the prohibition of real-time remote biometric identification systems only applies to systems used for law enforcement purposes in publicly accessible spaces, thus neither to systems used by **other public authorities** nor to those used by **private actors that act on behalf of public authorities** or in the framework of Public-Private-Partnerships. Evidently, the major risks to fundamental rights associated with such systems are not limited to law enforcement purposes—a fact that the proposal does not sufficiently reflect.

III Third, in the same vein, the risks are not limited to real-time biometric identification systems: If, for example, **"post" biometric identification systems** are subsequently applied to video footage of an event, this may still enable mass surveillance.

IV Third, a **range of exceptions** to the prohibition creates a number of loopholes that authorities could try to exploit. For example, the use of real-time biometric identification can be allowed in relation to a wide range of criminal offenses (Article 5(3)), or for the "prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack" (Article 5(2)), the interpretation of which leaves wide discretionary power to the authorities. While judicial authorization is necessary for such exceptional uses, it can be postponed in cases of urgency.

/ As the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) have been interpreted controversially with respect to biometric identification and, thereby, do not reliably protect against such mass surveillance techniques, **the AI Act would provide an opportunity to comprehensively ban all uses of biometric recognition systems in public space that lead to mass surveillance and that are, therefore, inherently in conflict with fundamental rights. We urge the Council and the Parliament to take that opportunity and improve the effectiveness of the ban**.

V The **other prohibitions** listed in Article 5 exhibit similar ambiguities. The ban on AI systems used for social scoring purposes is limited to those deployed by public authorities (Art. 5(1)(c)). Private actors (that do not act on behalf of public authorities) are spared without any meaningful justification. The condition of causing "physical or psychological harm" necessary for the bans on manipulative systems (Art. 5(1)(a) and 5(1)(b)) raises the threshold enormously so as to unacceptably narrow the scope of this provision. Furthermore, Article 5 lacks a ban on AI systems used for predictive policing that clearly violate fundamental rights, which are only declared high-risk.

/ **We recommend that the prohibitions listed in Article 5 are better defined so as to reconcile them with the ultimate objective—the protection of fundamental rights.**

8 Guarantee Participation and Enhance Capacity to Protect Workers' Autonomy

We welcome the Commission's decision to include **AI systems relating to employment, workers management, and access to self-employment** in the catalog of high-risk AI systems. Complex computational systems are increasingly being used to monitor, score, manage, promote, and even fire employees. These systems have the potential to profoundly influence, alter, and redirect the lives of people at work and, therefore, impact their life chances in general. In order to protect workers' rights—and, first and foremost, their autonomy—there need to be mandatory provisions for transparency and participation.

We join the German union association DGB in criticizing the fact that the Commission's proposal **does not include any process requirements for participation and co-determination options** for the use of AI systems.[14] This is a regrettable step backward compared to the White Paper that held that "involvement of social partners will be a crucial factor in ensuring a human-centred approach to AI at work". We call on the Council and the Parliament to restore this objective and to undergird it with appropriate measures.

I First, workers must be guaranteed the **right to obtain information** about the purpose of systems covered under this Act, and how the system's purpose is intended to be achieved. This does not necessarily imply full disclosure of an algorithm, a model, source code, or data. An appropriate level of intelligibility can be achieved by providing information about key qualities of a system, e.g., using guidelines for reviewing essential features.[15] If such a level of understanding cannot be sufficiently achieved by these means, then there needs to be a procedure defined to compel providers and users to make satisfactory information available.

II Second, in line with the German union association DGB, we call for **independent agencies to be set up on the national level for the area of labor and employment**, to support company stakeholders in consultation, testing, evaluation, and complaints, and for these agencies to be equipped with sufficient resources. Furthermore, Member States should facilitate effective capacity building of workers representatives in relation to AI-based systems, either by providing training courses themselves, or allocating resources for third parties to do so.

III Third, with regard to "AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies", there needs to be an **update to anti-discrimination law** in line with technological developments. As we have shown, online platforms optimize ad delivery in discriminatory ways that very much affect the choice of job seekers.[16] These practices are not adequately addressed at the moment.[17] The AI Act offers an opportunity to address these challenges.

/ **We call on the Parliament and the Council to be more ambitious than the Commission with regard to workers' rights. In the face of the far-reaching effects AI-based systems (can) have on the power relationship between workers and employers, the European Union has a duty to safeguard and strengthen the values and practice of cooperation and balance of interests that are part of the Union's history of social partnership.**

Conclusion: Use the Opportunity to Make a Meaningful Step Forward

/ The intention of the above comments and recommendations is to contribute to making the AI Act an effective means to achieve the ultimate objective, which is to make sure that **the use of ADM systems contributes to individuals' enjoyment of fundamental rights instead of undermining them. It is our hope that all legislative bodies will be guided by this objective. We invite the Commission to continue with further public consultation mechanisms accompanying the co-legislative procedure and to ensure that these consultations are accessible to a broad range of stakeholders, including communities most affected by the use of the systems addressed.**

[14] Cf. Initial Assessment of Issues Relevant to Labour Policy on the Draft of the EU Commission on a European AI regulation, 21 June 2021, https://www.dgb.de/-/08J

[15] Cf. Stiller, Sebastian / Jäger, Jule / Gießler, Sebastian: Analysis Guideline for reviewing essential features of AI-based systems for works councils and other staff representatives, May 18, 2021, https://algorithmwatch.org/en/auto-hr/guideline-for-reviewing-essential-features-of-ai-based-systems-for-works-councils-and-other-staff-representatives/

[16] Kayser-Bril, Nicolas: Automated discrimination: Facebook uses gross stereotypes to optimize ad delivery, 18 October 2020, https://algorithmwatch.org/en/automated-discrimination-facebook-google/

[17] Fröhlich, Wiebke: Männer fahren LKW, Frauen erziehen Kinder – diskriminierendes Gendertargeting durch Facebook, 10 November 2020, https://algorithmwatch.org/de/diskriminierendes-gendertargeting-durch-facebook/