CIVIL LIBERTIES UNION FOR EUROPE

RECOMMENDATIONS ON THE COMMISSION'S AI REGULATION PROPOSAL

12 JULY 2021

BY CIVIL LIBERTIES UNION FOR EUROPE

Table of contents

Executive Summary

When used in a responsible way, artificial intelligence (AI) systems have the potential to contribute positively to our societies. They can help provide accurate medical diagnoses, detect wildlife poachers or prevent fatigue-related errors at work. But AI systems can also undermine our fundamental rights, by perpetuating bias in criminal justice, manipulating public opinion by facilitating the spread of disinformation and enabling mass surveillance practices. In the transition into a digital age, governments and corporations are increasingly making use of algorithms. Ensuring that their adoption respects our fundamental rights is key.

The Commission's proposal for a new Artificial Intelligence Act, published on 21 April 2021, is an improvement to last year's White Paper. The intention to make AI "a tool for people" and "a force for good in society with the ultimate aim of increasing human well-being" is spot on. Article 5, which bans AI systems considered "unacceptable as contravening Union values" and Article 60, which suggests the creation of a database for high-risk systems to increase transparency are much welcome initiatives. However, the proposal is still far from adequate. Liberties has identified six main issues:

First, the proposal's prohibition of remote biometric recognition technologies contains too many exceptions, so that it is de facto not a real prohibition. The vague wording leaves room for discretion: law enforcement authorities can justify the use of facial recognition technologies and circumvent the obligatory authorization by a judicial authority in "a duly justified situation of urgency". Further, the ban only concerns 'real-time' remote biometric identification systems, allowing law enforcement authorities to first collect the data and then mine it, using mass surveillance technologies, violating citizens' right to privacy and discouraging democratic participation. In addition, the ban only concerns law enforcement authorities. Other public authorities and private actors are exempt. Similarly, the ban on social scoring systems does not apply to private actors.

Second, the proposal fails to recognize the risks of predictive policing. These systems are built on biased data influenced by structural inequality and institutionalized racism. Multiple studies have shown that predictive policing systems are, by default, discriminatory towards marginalized communities. Furthermore, there is little evidence of the effectiveness of such systems and a lack of transparency as to where they are used and by whom.

Third, the proposal severely underregulates biometric categorization, emotion recognition and systems that manipulate image, audio or video content, such as deep fakes. Systems that group people according to their ethnic origin, gender and sexual and political orientation discriminate against non-binary people and minority groups and can be dangerous for people belonging to the LGBTQI+ community

or political dissidents. Systems that generate or manipulate content, such as deep fakes, are used to humiliate people, spread disinformation and interfere in democratic processes. Emotion recognition technologies are known for being unreliable and prone to bias. Allowing public authorities or businesses to use them for important decisions that have a major impact on a person's life and affect access to opportunities, such as testing a criminal suspect for signs of deception, recruitment and school performance, is unacceptable.

Fourth, businesses with high stakes in seeing their products make it to the market are allowed to self-regulate. This is an inappropriate solution because businesses have no incentive or inclination to proceed with caution and respect for fundamental rights, but are rather keen to downplay the risks and release their products as soon as possible. This will not only lead to variations in standards but also in lower levels of protection for citizens.

Fifth, it is not sure how the Commission wants to ensure enforcement. The proposal to create an AI board is sensible. However, it is not given sufficient autonomy to act independently from the Commission and not given sufficient resources to act effectively. The proposal further suggests that each Member State create their own national competent authority, which may come into conflict with existing authorities.

Sixth, the proposal fails to address power imbalances between providers of AI systems and consumers. It lacks clarity around citizens' rights to lodge complaints and access to a remedy for persons adversely affected by AI systems.

This paper provides an analysis of the key points of the proposal from a fundamental rights perspective. It serves to feed into the Commission's public consultation of the AI Regulation proposal. It includes six recommendations for how the Commission can make sure that the fundamental rights of EU citizens are protected. These are:

1. *Prohibit biometric mass surveillance systems and other AI systems listed in Article 5 without exceptions.*

AI systems that enable biometric mass surveillance, such as facial recognition technologies, have a chilling effect on our right to freedom of expression and assembly. Mass surveillance applications violate our right to democratic participation and our privacy, and they discriminate against marginalized groups. Furthermore, there is no evidence that these applications meet basic requirements of proportionality. The Commission must propose an outright prohibition, with no exceptions. The prohibition should be extended to include 'post' remote biometric identification systems and apply to all public authorities and private actors. The scope of the prohibition of AI systems used for social scoring must be extended so that it also applies to private actors.

2. All high-risk systems should be subject to a third-party conformity assessment.

The proposal suggests that providers of high-risk AI systems listed in Annex III should conduct a self-assessment. Liberties considers that this is not enough. These systems threaten to undermine a number of fundamental rights. Delegating risk assessment to profit-oriented businesses is unacceptable. Liberties therefore recommends that all high-risk systems be subject to a mandatory third-party risk assessment by an independent oversight body.

3. Prohibit predictive policing practices.

Evidence has shown that predictive policing technologies systematically discriminate against minority groups, perpetuate biases, are ineffective and inaccurate. Liberties recommends an outright prohibition of predictive policing systems.

4. Prohibit, with certain exceptions, emotion recognition technology, biometric categorization systems and systems used to manipulate content.

- **Emotion recognition systems:** Liberties recommends prohibiting emotion recognition technologies used for important decisions that directly affect a person's life chances and access to opportunities. To define 'important decisions' Liberties considers that these cover all systems that operate in the same areas as those of high-risk AI systems. In specific circumstances, for example when such systems can be used to treat a disease, the prohibition should be lifted, and the system moved to the high-risk category.

- **Biometric categorization systems:** Biometric categorization systems that group people according to their gender, ethnic origin, sexual or political orientation should be banned outright.

- **Systems that generate or manipulate image, audio or video content:** The speed at which AI systems that generate or manipulate image, audio or video content, such as deep fakes, propagate across the Internet has significantly increased in recent years. Given the harm they can cause to individuals' lives and democratic processes, Liberties recommends moving them to the high-risk category, where they will be

subject to stricter transparency and security obligations.

5. Extra scrutiny for public authorities.

Decisions made by public authorities can have a significant impact on our lives and, unlike with the private sector, people do not have the choice to opt-out of using public services. Thus, the public sector requires higher levels of transparency and accountability. Currently, we know too little about how the public sector uses AI systems. Liberties recommends that all AI systems used by public authorities, regardless of the risk level, be included in the EU database. This will build public trust in algorithms and public institutions and facilitate the work of investigative journalists and watchdogs. The database should inter alia contain information on who is using these systems and for which purpose.

6. Stronger enforcement and more opportunities for remedies

To ensure proper enforcement of the regulation, Liberties recommends giving more autonomy to the EU Artificial Intelligence Board and to designate national DPAs as the national competent authorities. This would require allocating more financial and human resources to national DPAs. In addition, the proposal should include more clarity on the possibilities of collective redress for persons adversely affected by AI systems.

1. Article 5: too many exceptions

The Commission's proposal bans several AI systems from the Union's market (Article 5). These include AI software that manipulate human behavior (e.g. children's toys using voice assistance), social scoring systems that rank people according to their social behavior, as is used in China and 'real-time' remote biometric identification systems in publicly accessible spaces. Article 5 is a step in the right direction, but it contains too many exceptions that will ultimately lead to abuses.

Particularly worrying are the exceptions for 'real-time' remote biometric identification systems in publicly accessible spaces for police or other government agencies engaged in law enforcement. These systems are designed to monitor and track the behavior of masses of people. Automated recognition technologies have become so precise and powerful that they are able to monitor our every move. The use of facial recognition technology in public spaces by government agencies has significantly increased in recent years. In France, CCTV images have been used illegally to fine protesters. In Italy, the police uses a facial recognition system that tracks and monitors people based on a database that contains 16 million mugshots. Mass surveillance technologies deter people from going to demonstrations. They have a chilling effect on our right to freedom of expression and assembly and violate our right to privacy. In addition, biometric mass surveillance systematically discriminates against minorities (e.g. reduced accuracy on darker skin tones) and there is no evidence that the aims pursued by the authorities using these applications could not be achieved through other means that are less invasive of privacy.

However, the Commission's proposal creates exceptions that allow the use of biometric mass surveillance systems when "strictly necessary", for example for the prevention of a terrorist attack or the localization and identification of a potential criminal. The necessary prior authorization of a judge or other independent authority can be circumvented "in a duly justified situation of urgency". The vague wording leaves room for abuse by law enforcement agencies to justify the use of such technologies. In addition, the prohibition does not apply to private actors (nor does the prohibition on social scoring), and could thus be used, for example, in shopping malls, nor does it apply to public authorities not engaged in law enforcement, such as local governments – although the use of biometric mass surveillance systems are equally intrusive when used by these bodies. Finally, the prohibition only applies to 'real-time' (as opposed to 'post') remote biometric identification, allowing the police and other law enforcement authorities to first collect the data and then mine it using mass surveillance technologies (e.g. the highly controversial ClearviewAI) to identify people.

The potential for abuses of biometric mass surveillance technologies is too high to allow for exceptions. In line with the Reclaim Your Face

campaign, the LIBE Committee, the position of the EDPB and the EDPS and over 175 civil society organizations, activists and academics around the world, Liberties advocates an outright prohibition of remote biometric recognition and facial recognition technologies. In addition, Liberties considers that the prohibition of AI applications used for social scoring should be extended to include private actors as it breaches EU fundamental values such as the right to privacy and the right to reputation.

2. Article 43: insufficient scrutiny of high-risk systems

Central to the Commission's proposal is the obligation for providers of high-risk AI systems (listed in Annex III) to conduct conformity assessments. The Commission is right to place these systems under increased scrutiny. But with the exception of AI systems used for 'real-time' and 'post' remote biometric identification of persons, none of the high-risk systems (not even those used for predictive policing or border control) will be subject to a third-party conformity assessment. Businesses don't have the necessary expertise, but they do have great interest to see their products land on the Union's market before their competitors' and to generate income. Requiring them to conduct conformity assessments could amount to a simple box-ticking exercise. This makes it an inappropriate solution to prevent the deployment of unsafe and rights-breaching algorithms.

The high-risk systems listed in Annex III have been proven time and again to be unreliable, to discriminate against minorities and to perpetuate social biases. The efficiency and accuracy of AI systems used for migration control (e.g. to calculate the likelihood of fraudulent asylum applications or to identify sham marriages) remain unproven, and they are likely to create unfair outcomes for asylum seekers and infringe fundamental rights. Similarly, algorithmic biases have been recorded in credit scoring, recruiting, systems used in the judiciary (e.g. to predict recidivism or determine length of prison sentences), education and the medical sector and systems used in predictive policing.

These systems are a threat to our individual freedoms, including the right to education, the right to a fair trial, the right to privacy and the right to freedom of speech. They often present a situation of severe power imbalance and have huge implications on people's fundamental rights. It is unacceptable to delegate their risk assessment to profit-oriented businesses who focus on obeying the rules when they have to and not on protecting fundamental rights. Liberties therefore strongly recommends that all high-risk systems be subject to a mandatory third-party risk assessment by an independent oversight body.

3. Risks of predictive policing systems are trivialized

Predictive policing systems are intended to help law enforcement calculate the likelihood of future crimes, using massive personal data sets. There is little evidence of the effectiveness of such systems. A lack of transparency and understanding about how these models work might lead to accountability problems whereby police officers fully rely on the algorithms and are unable to deduce biases. Instead, it has been amply demonstrated that predictive policing systems discriminate against ethnic and religious minorities. The main reason is that predictive policing systems learn from biased data influenced by institutionalized racism. Recently, the LIBE Committee warned that predictive policing systems "amplify existing discrimination".

Predictive policing systems are already used across the EU. In a pilot project in the Netherlands, police collected data on vehicles and movement patterns using cameras and other sensors. When the algorithm detected suspicious activity, the police would stop and check the individuals. One of the indicators to determine the "risk score" of a vehicle was whether the people inside were of Eastern European origin. This is not only unjust and discriminatory but also deeply humiliating for the affected communities and results in social alienation.

The proposal considers that predictive policing systems constitute a high risk, but not enough to impose an outright ban. Liberties is of the opinion that inaccurate technologies that systematically discriminate against minority groups and perpetuate biases should be prohibited. Instead of spending millions on new technologies that promise quick fixes, police should improve their relationships with local communities, as 'community-based' policing is often more efficient than data-driven solutions. Relationships built on mutual and genuine trust between the police and locals lead to information exchanges that can help prevent and solve crime.

4. Limited risk systems (supposedly)

AI systems that pose a limited risk have only minimal transparency obligations. Machines that interact with humans for instance must only clarify that they are machines. This is arguably sufficient for simple systems, such as chatbots. Extremely disturbing is that the same minimal requirements apply to emotion recognition technology, biometric categorization systems and systems used to manipulate content. Providers of such systems have no human oversight or technical documentation obligations. They do not have to ensure a minimum level of accuracy or robustness and there is no obligation to conduct a conformity assessment.

4.1. Emotion recognition technology

Emotion recognition technology uses biometric data, for example to find the "perfect" employee or identify inattentive students during lectures. It is known for being prone to bias. One study found that emotion-reading systems assign more negative emotions to people of certain ethnicities. Research has also shown that these systems are still inaccurate and thus unreliable, as the facial movements that express our emotions strongly vary according to our culture. Allowing public authorities or businesses to use them for important decisions (i.e. that have a major impact on a person's life and affect access to opportunities), such as recruitment or school performance, is unacceptable.

Liberties is of the opinion that the proposal should prohibit the use of emotion recognition technologies for important decisions. To determine what falls under the scope of 'important decisions', Liberties recommends that these cover systems that operate in the same areas as those of high-risk AI systems (listed in Annex III). These include: employment (e.g. recruiting), migration control (e.g. the EU-funded 'iBorderCtrl' project), access to essential private and public services and benefits (e.g. credit scoring), education (e.g. school performance), or law enforcement (e.g. testing a criminal suspect for signs of deception). Exceptions should be made in well-circumscribed circumstances, for example in medicine, when reading a patient's emotions is an important component of treatment.

4.2. Biometric categorization systems

Biometric categorization systems, which assign people to specific categories on the basis of their biometric data, also feature in the limited-risk category. They include systems that group people according to their observable data (e.g. hair color, foot size or age), but also according to their gender, ethnic origin, or sexual or political orientation. This is problematic in many ways. Algorithms

that can supposedly predict a person's gender based on their observable data can harm trans and non-binary people and any other person that does not fit the typical gender markers by denying them the freedom to express their own gender identity. Algorithms that pretend to predict a person's sexual and political orientation can pose huge risks for the safety of LGBTQI+ people and political dissidents, especially those living in less democratic countries – it is crucial to remember that the AI Act has a significant influence on how AI systems are applied across the globe. Further, AI systems used to identify a person's ethnic origin can be used for discriminatory practices, such as ethnic profiling. Liberties recommends that biometric categorization systems that group people according to their gender, ethnic origin, or sexual or political orientation should be prohibited outright.

4.3. *Systems that generate or manipulate content*

AI systems that generate or manipulate image, audio or video content, such as deep fakes, also feature in the limited-risk category. Thus, only limited transparency obligations apply, such as disclosing that automated means were used. This is very concerning, given the harm such technologies can cause. Deep fakes in particular have become widespread. It has become increasingly difficult to differentiate between real and fake content.

Most deep fake content circulating online is not used for society's general benefit. According to a study, 96% of deep fakes on the Internet are pornographic material. Celebrities, and in particular women, are often victims of face-swap technology. Deep fakes also have the potential to become a serious political threat. Fake videos are already being used to spread disinformation, distort reality, hurt a politician's reputation, manipulate voters and impact election results. In addition, deep fakes contribute to the existing mistrust of online content. Large online platforms, such as Facebook and Twitter, have banned or restricted the use of deep fakes. The fact that we have not yet seen in the EU a wide-scale use of deep fakes in political campaigning or fake videos of influential persons calling their followers to violence, should not lead to complacency. However, in certain contexts, deep fakes can also be of utility. They can for example be used in arts or to enable people suffering from Lou Gehrig's Disease to speak with their synthetic voice. Thus, instead of a complete prohibition, Liberties recommends placing systems that generate and manipulate images, videos and content in the high-risk category, where they will be subject to stricter transparency and security obligations.

5. Article 60: extra transparency for systems used by public authorities

The Commission's proposal to establish a publicly accessible database (Article 60) for all high-risk AI systems is laudable. However, it should be expanded to include all AI systems used by public authorities, regardless of risk level. Decisions made by public authorities can have far-reaching impacts on society and in particular its most vulnerable. Unlike with private companies, individuals are subordinated and exposed to public authorities. Therefore, the public sector requires higher levels of transparency and accountability. Currently, we know too little about how the public sector uses AI systems. It is not sufficient to know which high-risk systems are on the market. We need to know which ones are being used (e.g. if police are using predictive policing technology). Furthermore, public procurement procedures are regularly ignored. Taxpayers' money is spent on expensive technologies that do not necessarily provide the most efficient solutions. Including all AI systems used by public authorities regardless of the risk level in the EU database would increase trust in public authorities and facilitate the work of investigative journalists and watchdogs who hold governments accountable. In addition, the database should contain information on who is using these systems and for which purpose.

6. Governance: enforcement and remedies

Liberties welcomes the Commission's plans to establish an EU Artificial Intelligence Board (Article 56) to ensure a certain degree of harmonization. However, the board as it stands only acts as advisor and has too little autonomy to act effectively. In line with the EDPS and EDPB, Liberties recommends that the board be given adequate financial and human resources, as well as more autonomy to act independently from the Commission.

The proposal also requires Member States to create national competent authorities (Article 59) with between one and 25 full-time positions to oversee enforcement. The creation of new national authorities may come into conflict with existing authorities. Further, it is inconceivable that a single person would be able to oversee enforcement of the regulation. Instead, the national data protection authorities (DPAs) should be designated as national competent authorities, as they already enforce the GDPR on AI systems and have the necessary expertise. This would require allocating more resources to national DPAs, which are understaffed and underfunded. Liberties welcomes the initiative to increase the fines for non-compliance to six percent of a company's total global annual revenue. However, without sufficient resources, DPAs (or other competent authorities) will not be able to follow up on complaints, properly investigate and impose penalties. The proposal further designates the EDPS as competent authority for supervising Union institutions, agencies and bodies. However, it should clarify its role and how it would work with other competent authorities.

Finally, the proposal fails to address power imbalances between providers of AI systems and consumers. It lacks clarity around citizens' rights to lodge complaints (whether to the police, courts or Ombudspersons) and access to a remedy for persons adversely affected by AI systems. To protect citizens' and consumers' rights, the proposal should create or designate a complaint mechanism, similar to Article 77 and 78 of the GDPR. It should provide opportunities for collective redress in the form of a grievance mechanism to protect citizens from human rights violations, for example workers should have the right to take action against invasive AI systems used by their employer without fear of retaliation.

7. Conclusion

As with the GDPR, the EU has the potential to set a global standard on regulating AI. It carries a big responsibility, as it will also affect how AI systems are used in less democratic nations across the world. The EU has a responsibility to citizens to make AI work primarily for them in a way that enhances their quality of life and promotes equality. There is a temptation to embrace AI because it can deliver savings or because it will stimulate economic activity. But taking shortcuts in public services, like law enforcement, or deploying AI where it has no social benefit will end up damaging our way of life and the freedoms we value. As such, the EU institutions should be guided by the question of how we can use AI to bring fundamental rights to life.

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of 19 national civil liberties NGOs from across the EU.

Website:

liberties.eu

Contact info:

info@liberties.eu

The Civil Liberties Union for Europe

Ringbahnstrasse 16-18-20
3rd floor
12099 Berlin
Germany