Information Polity 27 (2022) 147–162
DOI 10.3233/IP-211524
IOS Press

Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance[1]

Irena Barkane
University of Latvia, Raina Blvd. 19, LV-1586, Riga, Latvia
Tel.: +37 129187564; E-mail: irena.barkane@lu.lv

Abstract. Artificial Intelligence (AI)-based surveillance technologies such as facial recognition, emotion recognition and other biometric technologies have been rapidly introduced by both public and private entities all around the world, raising major concerns about their impact on fundamental rights, the rule of law and democracy. This article questions the efficiency of the European Commission's Proposal for Regulation of Artificial Intelligence, known as the AI Act, in addressing the threats and risks to fundamental rights posed by AI biometric surveillance systems. It argues that in order to meaningfully address risks to fundamental rights the proposed classification of these systems should be reconsidered. Although the draft AI Act acknowledges that some AI practices should be prohibited, the multiple exceptions and loopholes should be closed, and in addition new prohibitions, in particular to emotional recognition and biometric categorisation systems, should be added to counter AI surveillance practices violating fundamental rights. The AI Act should also introduce stronger legal requirements, such as third-party conformity assessment, fundamental rights impact assessment, transparency obligations as well as enhance existing EU data protection law and the rights and remedies available to individuals, thus not missing the unique opportunity to adopt the first legal framework that truly promotes trustworthy AI.

Keywords: Artificial Intelligence Act, ban on mass surveillance, remote biometric identification, biometric categorisation, emotion recognition, prohibited artificial intelligence practices

Key points for practitioners:

- The article is intended to facilitate a discussion on the development of AI legal framework, recommend the improvements for the draft AI Act and provide guidance as to how fundamental rights-based approach could substantially support this process.
- The article explains the reasons why it is important to include clear prohibitions of certain uses of AI in the AI Act, in particular to counter mass surveillance practices.
- The article recommends to strengthen accountability and transparency mechanisms, enhance existing data protection rules and promote the rights and remedies of the individuals and groups in the draft AI Act.

1. Introduction

On 21 April 2021, the European Commission published a long-awaited proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, known

[1]This article received a correction notice (Erratum) post publication with DOI 10.3233/IP-229012, available at http://doi.org/10.3233/IP-229012.

as the Artificial Intelligence Act (the draft AI Act or AI Act) (European Commission, 2021) – the first legal framework on artificial intelligence (AI) that addresses the risks of AI systems.

A wide range of research has been published, including by the Council of Europe (Council of Europe, 2021), the European Parliament (Madiega & Mildebrath, 2021), the European Union Agency of Fundamental Rights (FRA, 2019) and academics (Veliz, 2020), revealing the negative impacts of biometric surveillance systems, such as facial recognition, emotional recognition and biometric categorisation, on a wide range of fundamental rights, in particular human dignity, the right to privacy and data protection, non-discrimination, freedom of expression and freedom of peaceful assembly, the rights to an effective remedy and to a fair trial as well as the rule of law and democratic values.

The draft AI Act introduces new rules for use of AI biometric surveillance systems to address these risks. The draft AI Act classifies these systems into different categories based on the risks they create, sets prohibitions on certain practices, and introduces new legal requirements. These new rules – in particular the proposed prohibitions and classification choices of AI systems – have sparked much discussion and have been heavily criticised by academics (Veale & Zuiderveen Borgesius, 2021; Malgieri & Ienca 2021), civil society (EDRI, 2021a) as well as the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) (EDPB & EDPS, 2021).

This article aims to question whether the draft AI Act meaningfully addresses risks to fundamental rights caused by use of AI biometric surveillance systems. Firstly, the article will underline the importance of the AI Act in terms of promoting trustworthy AI that, *inter alia*, requires a meaningful approach to the risks that AI systems pose to fundamental rights. Next, it will highlight the growing calls, in particular by international organisations and civil society, to introduce clear red lines in the AI legal framework. After that, the article will critically analyse the provisions of the draft AI Act with regard to the risk-based classification of AI biometric surveillance systems and the rules and legal requirements for use of those systems and reveal key challenges and opportunities not to be missed for the AI Act to efficiently counter risks to fundamental rights.

2. The objective of the draft AI Act to protect fundamental rightss

The draft AI Act puts fundamental rights at the core of Europe's AI approach. The need for a human rights-based approach to artificial intelligence has been increasingly recognised by academics (Mantelero, 2020) and the international community (OHCHR, 2021). Fundamental rights form the basis of AI regulation and play a key role in developing the international and EU AI regulatory framework, as has been emphasized in many AI ethics initiatives developed by international organizations, such as the Council of Europe (CAHAI, 2020), the EU (European Commission, 2020) and UNESCO (UNESCO, 2021).

There are many advantages of using a human rights-based approach in the context of AI. Over time, a broad human rights protection system has been established at the international, regional and national levels where individuals can seek legal remedies in the case of human rights violations. There is constantly evolving case law on how to interpret and apply human rights in specific situations. Human rights provide a universal language for global issues and they are internationally recognized.

At the same time, there are also challenges to implementing a human rights-based approach to AI. Human rights have been criticised for being more oriented towards states than private actors (Ben-Israel et.al., 2020). They are better suited to reducing significant harm to a small number of people than to preventing harm to the collective interest. AI biometric surveillance systems and their effects on human rights and freedoms are more difficult to challenge individually. Human rights are too abstract and thus it

may be difficult to interpret them in relation to AI systems. Moreover, they clearly do not address some issues related to AI (Smuha, 2021).

However, despite these pitfalls, human rights provide a sound normative framework to make AI systems work for the good of individuals and society and to prevent harm. The EU is founded on the values of human dignity, freedom, democracy, the rule of law and respect for human rights as set out in Article 2 of the Treaty on European Union and on unequivocal respect for fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union (the Charter). The Charter applies to EU institutions and to EU Member States when implementing EU law. However, international human rights law is legally binding on EU Member States. Rights considered as fundamental in the EU are universally recognised all over the world and universally applicable to all human beings regardless of any individual trait (Smuha, 2021).

The AI regulatory framework should further develop human rights norms by clarifying and contextualising their application to specific AI use cases (Mantelero, 2020). Implementing a human rights-based approach to AI also requires effective enforcement mechanisms as well as the realisation that all human rights are dependent on the underlying societal infrastructure (Smuha, 2021; Mantelero & Esposito, 2021).

The draft AI Act aims to pursue two parallel objectives. On the one hand, it fosters development, use and uptake of AI in the internal market. On the other hand, it creates an ecosystem of trust by seeking to ensure protection of safety, fundamental rights and EU values (Recital 1). These two objectives are distinct. The most advanced AI systems can pose serious threats to citizens' rights and social values. Likewise, effective protection against the risks posed by AI systems does not in itself provide the incentives that are needed to promote the uptake of AI (Sartor & Lagioia, 2020). At the same time, both objectives are compatible.

Although the draft AI Act aims to introduce a balanced and proportionate horizontal regulatory approach with a view to achieving both objectives, the proposed risk-based approach raises significant concerns. The draft AI Act is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for adoption of measures to ensure the establishment and functioning of the internal market. The exception is specific rules on protection of individuals with regard to processing personal data concerning restrictions on the use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement, which are based on Article 16 of the TFEU (Recital 2). Where the provisions of the draft AI Act entail 'maximum harmonisation', Member States' abilities to act in that area are disabled and they must disapply conflicting national rules that entail further questions. The supremacy of EU law accompanied by existing weaknesses of the proposed rules – the classification of AI systems in different risk categories, setting mandatory requirements for high-risk AI systems that will be further operationalised through harmonised technical standards and a conformity assessment system adapted from EU product safety law – raises concerns whether the draft AI Act would provide effective mechanisms to ensure effective enforcement of existing fundamental rights and whether Member States may be deprived of the right to take action in this regard (McFadden et.al., 2021; Veale & Zuiderveen Borgesius, 2021). Further analysis will discuss these provisions of the draft AI Act in more detail, though will not cover all contentious issues, for example, on the role of standards, that would require separate analysis.

AI systems do not operate in a lawless world. The draft AI Act seeks to ensure consistency and will complement existing EU legislation. AI systems are already subject to European legislation, in particular the Charter, the rules on personal data protection, notably the General data Protection Regulation (the

GDPR) (Regulation 2016/679) and the Law Enforcement Directive (Directive 2016/680), and non-discrimination law. However, existing legal norms are not sufficient to deal with the complexities of AI and address potential harms and negative impacts of AI systems (CAHAI, 2020).

The increasing use of AI biometric surveillance systems raises serious concerns as to fundamental rights. Remote biometric recognition is linked to deep interference with the right to privacy, including people's autonomy, their right to establish details of their identity and psychological integrity (Muller & Dignum, 2021). It negatively impacts freedom of expression, association and freedom of movement (EDPB & EDPS, 2021). Remote biometric identification and predictive tools may lead to discrimination, violate the values of equality and justice due to biased data sets and errors as well as undermine the rights to liberty and to a fair trial (OHCHR, 2021).

Moreover, biometric recognition systems, including those used for social scoring and predictive policing, may enable mass surveillance (Wendehorst & Duller, 2021). The clearest distinction between AI systems in authoritarian countries and AI systems in democratic countries is the use of facial recognition for mass surveillance (CAIDP, 2021).

The draft AI Act is an ambitious attempt to deal with the complexities of AI and adequately address both the benefits and risks of AI and to support the EU objective to be a global leader in the development of secure, trustworthy and ethical AI. In order to be trustworthy, AI systems should be (1) lawful – compliant with all applicable laws, (2) ethical and (3) robust (AI HLEG, 2019). Human rights as legally enforceable rights fall under the first component of trustworthy AI. Moreover, they form part of the second component as they are also bestowed on individuals by mere virtue of their status as human beings regardless of any legal enforceability. Ensuring that AI systems are robust from both the technical and social perspectives is closely intertwined with the first two components (Smuha, 2021).

The AI Act should effectively enforce existing laws on fundamental rights by addressing the risks created by AI systems, including by biometric surveillance systems. Respect, protection and promotion of human rights, within a framework of democracy and the rule of law, is essential throughout the life cycle of AI systems. This objective also requires introduction of prohibitions on certain AI practices that violate fundamental rights and democratic values.

3. Growing calls for red lines in the upcoming AI legal framework

The draft AI Act sets prohibitions on AI practices contradicting EU values and fundamental rights. Introducing these prohibitions is as such unequivocally a significant step forward in the intense debate at EU, international and national levels on the need to set red lines to AI practices violating human rights, in particular on the use of biometric surveillance systems.

Due to conflicting opinions, prohibitions of certain AI practices were not included in prior EU policy documents on the development of AI regulation. The European Commission's White paper on Artificial Intelligence, while emphasising that the use and gathering of biometric data for remote identification purposes carries specific risks to fundamental rights, contains no prohibitions (European Commission, 2020). However, a leaked version of this document contained a moratorium on facial recognition, controversially later removed from the final version (Access Now, 2020).

At the same time, the European Parliament has on a number of occasions urged the European Commission to consider a moratorium on the use of facial recognition systems (European Parliament, 2020). In 2021, a group of more than 100 members of the European Parliament has called on the European Commission to enshrine an explicit ban on biometric mass surveillance in public spaces in EU law (European Parliament, 2021).

International organisations involved in the debate on development of AI regulation increasingly and noticeably recognise the need to set red lines in AI regulation.

The UNESCO Recommendation on the Ethics of Artificial Intelligence adopted in 2021 provides that "AI systems should not be used for social scoring and mass surveillance purposes" (para 26) (UNESCO, 2021).

In September 2021, the United Nations High Commissioner for Human Rights, Michelle Bachelet, published a report stressing the urgent need to ban AI applications that violate human rights (OHCHR, 2021). The High Commissioner urges States to expressly ban AI applications that cannot be operated in compliance with international human rights law and to impose moratoriums on the sale and use of AI systems that carry a high risk for enjoyment of human rights, unless and until adequate safeguards to protect human rights are in place. The document also underlines the need to impose a moratorium on the use of remote biometric recognition technologies in public spaces. The High Commissioner emphasises that a risk-proportionate approach to legislation and regulation will require prohibition of certain AI technologies, applications or use cases, where these would create potential or actual impacts that are not justified under international human rights law, including those that fail the necessity and proportionality tests.

In 2020, the Council of Europe published a report prepared by the Ad hoc Committee on Artificial Intelligence (CAHAI) which indicates that red lines could be drawn for certain AI systems or uses that are considered to be too impactful to be left uncontrolled or unregulated or to even be allowed at all, including AI-enabled mass surveillance and social scoring (Ben-Israel et.al., 2020). The Council of Europe has also issued Guidelines on Facial Recognition that call for specific rules for biometric processing by facial recognition technologies for law enforcement purposes as well as to strictly limit or prohibit certain uses of these technologies (Council of Europe, 2021).

This direction of debates on the need to introduce red lines in the AI legal framework has been much influenced by national legislators, civil society, data protection authorities and academics (Veliz, 2020).

In contrast to the situation in the EU, in the last few years the use of facial recognition technology by government and law enforcement authorities has been banned in a number of USA cities, such as San Francisco, Oakland, Boston, despite the lack of strong federal data protection regulation (Access Now, 2020).

The debate has been strongly influenced by civil society organisations. In 2020, European Digital Rights (EDRI), an association of 115 civil and human rights organisations, launched the 'Reclaim your face' campaign and the European Citizens' Initiative, calling on the European Commission to ban biometric mass surveillance practices (EDRI, 2021b). In 2021 EDPB and the EDPS joined civil society in their call for a ban on automated facial recognition technologies (EDPB & EDPS, 2021).

National data protection authorities have also adopted the first decisions finding that use of facial recognition technologies, for example, to monitor attendance of students at school (EDPB, 2019) and to identify individuals by using *Clearview AI* (EDPB, 2021), violates data protection law. Currently their use is supervised on a case-by-case basis, raising the risk of their normalisation and legitimisation in individual Member States across the EU.

Despite recognition of the urgent need for a ban on certain AI practices contravening fundamental rights and democratic values, the EU, international organizations and national legislators still need to take courageous further steps to effectively introduce prohibitions in the legal framework, including in the draft AI Act.

4. Reconsidering the classification of AI systems

The draft AI Act follows a risk-based approach and proposes to categorise AI systems based on the four different risk levels they create: 1) an unacceptable risk (Title II); 2) a high risk (Title III); 3) limited risk (Title IV) or 4) minimal risk (Title IX). No limitations or requirements are set for use of AI systems creating minimal or low risk.

The draft AI Act prohibits certain AI practices that create unacceptable risk as they contradict EU values and fundamental rights. The draft Act proposes to prohibit four AI practices: 1) deployment of subliminal techniques beyond a person's consciousness, 2) exploitation of the vulnerabilities of specific vulnerable groups, 3) social scoring, and 4) use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement (Article 5 (1)).

Other AI systems that create an adverse impact on safety or fundamental rights are considered as high-risk. This includes AI systems that are product or safety components (Article 6 (1)) or systems used in the areas listed in Annex III of the draft AI Act (Article (6) (2)), including such areas as biometric identification and categorisation, education, employment, law enforcement, migration, asylum and border control. The draft Act sets specific requirements for high-risk AI systems and obligations for operators of such systems to mitigate the risks they pose.

For other AI systems that do not pose high risks, the draft AI Act imposes limited transparency rules. The draft Act classifies AI systems as limited-risk systems that are intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content (Article 52).

According to the proposed classification, AI biometric surveillance systems may fall into three categories and be seen as prohibited, high-risk, or limited risk AI systems. The draft AI Act defines and regulates three kinds of AI biometric surveillance systems – remote biometric identification systems, biometric categorization systems, and emotion recognition systems. However, only use of the first system – remote biometric identification systems – may be classified as prohibited AI practices. At the same time the first system may also fall into the high-risk AI system category. Biometric categorization systems and emotional recognition systems may fall into the categories of limited risk or high-risk AI systems depending on the area in which they are used.

Further analysis will critically assess the proposed classification of AI biometric surveillance practices and reveal the main concerns and shortcomings of the new rules.

4.1. Remote biometric identification as prohibited AI practices

The draft AI Act prohibits use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement (Article 5 (1) (d)). 'Remote biometric identification system' is defined as 'an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified' (Article 3 (36)).

Remote real-time facial recognition is increasingly deployed by authorities around the world. In Europe, the United Kingdom has been the most active in experimenting with this technology. A number of EU Member States have also conducted live facial recognition pilot projects, for example, at Brussels International Airport, during the Carnival in Nice, during Carnival 2019 in 's-Hertogenbosch's Korte Putstraat (the Netherlands), in Berlin Südkreuz train station or Mannheim city centre (Germany) (Ragazzi et. al., 2021; FRA, 2019). Their current deployment in public spaces across Europe is primarily experimental and

localised, although the technology coexists with a broad range of algorithmic processing of images being carried out on a large scale. Moreover, in the current creation of new biometric databases or upgrading existing databases to become facial recognition-readable, law enforcement authorities are building an infrastructure that poses significant risks for biometric mass surveillance (Ragazzi et. al., 2021).

The draft AI Act acknowledges that use of these systems is considered particularly intrusive into the rights and freedoms of the persons concerned, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade exercise of freedom of assembly and other fundamental rights (Recital 18).

However, the scope of the prohibition is strictly limited, thus allowing a wide range of biometric surveillance practices. In order for the prohibition to apply, several elements must be present, raising a number of concerns about their justification.

Firstly, the draft AI Act prohibits only "biometric identification systems", thus not covering other biometric systems that are used for other purposes than that of identifying natural persons, such as biometric categorisation, emotion recognition and behavioural detection and other techniques that are being used to an increasing extent by public and private bodies (Wendehorst & Duller, 2021).

Secondly, the prohibition applies only to 'real-time' biometric identification systems, thus allowing 'non-real time' or 'post' identification. The draft AI Act defines a 'real-time' remote biometric identification system as 'a system whereby capture of biometric data, comparison and identification all occur without significant delay, which comprises not only instant identification, but also limited short delays in order to avoid circumvention' (Article 3 (37)). Accordingly, real-time identification applies not only to instant identification but also to 'limited short delays'. However, it is unclear what should be understood by it. Biometric identification, even when not done in real time, but at a later stage, can have a similar negative impact on privacy, freedom of association and other fundamental rights. For example, remote biometric identification of political protesters creates a significant chilling effect on the exercise of freedom of assembly and association regardless of whether it is 'real-time' or 'post' (EDPB & EDPS, 2021).

Moreover, the 'real-time' and 'publicly accessible spaces' conditions allow law enforcement authorities to use recognition software services, such as *Clearview AI,* on previously recorded footages or images to identify individuals, track their movements, and attempt to link their behaviour to certain special categories. 'Publicly accessible spaces' means 'any physical place accessible to the public, regardless of whether certain conditions for access may apply' (Article 3 (39), draft AI Act). These include streets, government buildings, transport infrastructure, cinemas, theatres, shopping centres, and so on. The notion does not cover online spaces (Recital 9, draft AI Act). AI systems for large-scale remote identification in online spaces should be prohibited under Article 5 of the draft AI Act as they contravene EU data protection law and do not meet the strict necessity requirement established by the CJEU and the ECtHR (EDPB & EDPS, 2021).

Thirdly, the prohibition is limited to use of AI systems 'for law enforcement purposes', which means 'activities carried out by law enforcement authorities for the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties, including safeguarding against and prevention of threats to public security' (Article 3 (41)). Accordingly, the draft AI Act allows remote biometric identification by public authorities in publicly accessible spaces for purposes other than law enforcement as well as by private companies both in public and private spaces. These systems have been implemented by both public and private entities across Europe for different purposes, such as scanning shoppers entering supermarkets, controlling entry to stadiums, schools and transport and for crowd control or public health purposes, with severe effects on the populations' expectations of being anonymous in public spaces (Montag et.al., 2021; EDPB & EDPS, 2021).

In addition to the narrow scope of the prohibition, the draft AI Act provides an exhaustive list of exceptional cases in which the prohibition does not apply. Remote biometric identification systems may be still used for law enforcement purposes if strictly necessary for:

- targeted search for specific potential victims of crime;
- prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
- detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence for a wide list of criminal offences allowing issue of a European arrest warrant if those offences are punishable in that Member State by a custodial sentence or a detention order for a maximum of at least three years (Article 5 (1) (d)).

The draft AI Act acknowledges the essential requirement established by the case-law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) in mass surveillance cases, namely that use of these systems should be 'strictly necessary'. The further rules of the draft AI Act seem to be trying to include the following essential guarantees identified by both courts in mass surveillance cases:

- clear, precise and accessible rules;
- proportionality and necessity;
- an independent oversight mechanism; and
- effective remedies (EDPB, 2020).

The draft AI Act introduces extensive rules for the use of remote biometric identification systems in these exceptional situations. First, the draft AI Act states that two elements must be taken into account:

- the nature of the situation;
- the consequences of use for the rights and freedoms of all persons concerned.

In addition, the use of these systems must comply with necessary and proportionate safeguards and conditions, in particular regarding temporal, geographic and personal limitations (Article 5 (2)). Although the draft AI Act refers to 'personal limitations', the wording is too vague to ensure only targeted use of these systems.

Further, the draft AI Act states that each individual use of remote biometric identification systems should be subject to prior authorisation by a judicial authority or by an independent administrative authority, except in urgent situations, when authorisation may be requested during or after use. The authority will only grant authorisation where it is satisfied – based on objective evidence or clear indications presented to it – that use of the system is necessary and proportionate (Article 5 (3)). This provision, however, does not require an assessment of whether the use is 'strictly necessary'. Moreover, it allows authorisation of use of systems based on 'clear indications', i.e. without evidence. Evaluating whether use of surveillance measures is 'strictly necessary' requires evidence that they are effective in achieving the particular public interest objective and that there are no less restrictive means. Scholars have also indicated that it is unclear whether warrants can be thematic, i.e. issued for individual purposes, and that public scrutiny may be challenging as transparency over the number and types of authorisations issued is not required in the AI Act (Veale & Zuiderveen Borgesius, 2021).

The draft AI Act states that a Member State may decide to provide for the possibility to fully or partial authorise the use of biometric recognition systems for law enforcement purposes and must lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, such authorisations (Article 5 (4)). This allows Member States to choose whether they want to implement the exceptions for using these systems for law enforcement purposes in their national laws,

given that public security and national security largely remain within the exclusive competence of the Member States, although under the conditions and within the limits set in the draft AI Act (Christakis & Becuywe, 2021).

Thus, the draft AI Act requires Member States to introduce in national regulation detailed rules for authorisation. However, the draft AI Act does not require Member States to adopt rules on use of these systems, although the CJEU and the ECtHR case-law has emphasised that it is essential to have clear, precise and accessible rules governing the scope and application of mass surveillance measures. The draft AI Act also does not include any rules on remedies available to individuals as well as on notification about use of the systems, although these are acknowledged as essential guarantees in mass surveillance case-law (EDPB, 2020).

The use of biometric data for law enforcement is currently regulated by the Law Enforcement Directive. The draft AI Act – as far as it provides specific rules on protection of individuals with regard to processing of personal data concerning restrictions on use of AI systems for 'real-time' remote biometric identification in publicly accessible spaces for the purpose of law enforcement – is based on Article 16 TFEU, rather than Article 114 as is the rest of the draft Act. The AI Act would be *lex specialis* to the Law Enforcement Directive. The EDPB and EDPS have stressed that it is of utmost importance to ensure clarity of the relationship between the AI Act to existing EU legislation on data protection and have recommended clarifying in Article 1 of the draft AI Act that EU legislation for protection of personal data applies to any processing of personal data falling within the scope of the AI Act (EDPB & EDPS, 2021). Inclusion of this provision would ensure that the AI Act would not lead to a weakening of the EU's high data protection standards, for example as interpreted in the case-law of the CJEU.

Not only the scope of prohibition of the use of remote biometric identification systems, but also the other three prohibitions have been widely criticised for being too narrow. AI systems that deploys subliminal techniques beyond someone's consciousness (Article 5 (1) (a)), and that exploits the vulnerabilities of a specific group of persons due to their age, physical or mental disability (Article 5 (1) (b)) are prohibited only if used to 'materially distort a person's behaviour' and only if such practice 'causes or is likely to cause that person or another person physical or psychological harm' making it impossible to ban any manipulative practices. The draft AI Act also prohibits AI-based social scoring, though limits its scope to general purposes carried out by public authorities, and does not cover social scoring by private companies (Article 5 (1) (c)). The risks posed by social scoring, likewise the use of remote biometric identification and other forms of biometric recognition in public spaces, do not depend on their purpose or whether they are used by public or private actors (EDPB & EDPS, 2021).

The draft AI Act, unlike in the case of the other three set prohibitions, namely on social scoring and AI manipulation, only prohibits the use of remote biometric identification systems, but does not prohibit the placing on the market and putting into service of such systems, thus allowing sale to oppressive regimes of biometric systems whose use would be illegal in the EU (Veale & Zuiderveen Borgesius, 2021).

Many actors have urged for a ban in the AI Act on remote biometric recognition in public spaces, including but not limited to biometric identification, and any type of social scoring as well as to introduce new prohibitions on predictive tools currently classified as high-risk systems and biometric classification and emotional recognition classified generally as limited risk AI systems (EDPB & EDPS, 2021; Muller & Dignum, 2021; EDRI, 2021a; CAIDP, 2021; EPIC, 2021). These categories of AI systems will be assessed further.

4.2. Remote biometric identification as high-risk AI systems

AI systems intended to be used for 'real-time' and 'post' remote biometric identification of natural persons which fail to meet all the criteria described above would be considered as prohibited and classified

as high-risk systems, i.e. under the area of biometric identification and categorization of natural persons (Annex III, 1, draft AI Act).

The draft AI Act states that high-risk AI systems should only be placed on the EU market or put into service if they comply with certain mandatory requirements to ensure that they do not pose unacceptable risks to important EU public interests as recognised and protected by EU law (Recital 27). The draft AI Act sets out a wide range of legal requirements for high-risk AI systems (Chapter 3). These are connected to the obligations of providers and users of AI systems and other parties (Chapter 4). Most of the requirements will apply to providers of AI systems, i.e. those who develop an AI system and place it on the market or put it into service (Article 3 (2)). They must implement a risk management system, use high-quality data sets, draw up technical documentation, enable record-keeping, ensure transparency and provide information to users, ensure human oversight and an appropriate level of robustness, accuracy and cybersecurity (Articles 8–15).

In addition, providers of high-risk AI systems must ensure that their systems undergo an *ex-ante* conformity assessment through internal checks prior to their placement on the market or putting into service (Article 43). Conformity assessment means verifying whether the requirements described above (i.e. set out in Title III, Chapter 2 of the draft AI Act) relating to an AI system have been fulfilled (Article 3 (20)). Within the area of remote biometric identification and categorisation of natural persons, third-party conformity assessment by an independent body for AI systems is planned to be used (Chapter 3). However, once harmonised standards and common specifications covering these systems exist, only self-assessment is needed. All other stand-alone high-risk AI systems, e.g. emotion recognition systems used in high-risk areas, will be based on self-assessment, which does not provide for involvement of a notified body. EDPS, EDPB and many other organisations have recommended that there is a need for third-party conformity assessments for all high-risk AI systems as internal assessments could quickly devolve into meaningless box-checks (EDPB & EDPS, 2021, Muller & Dignum, 2021, EDRI, 2021a; CAIDP, 2021). Moreover, conformity assessments could be made available to increase transparency (EPIC, 2021).

The draft AI Act requires new *ex ante* re-assessments of conformity in the case of substantial modifications to AI systems (Article 43 (4)), in particular a change of the intended purpose for which the AI system has been assessed (Article 1 (23)). However, this assessment would not be required for high-risk AI systems that have already been placed on the market or put into service. The AI Act would apply only to those AI systems that were subject to significant changes in their design or intended purpose (Article 83 (1)). Clearer guidelines should be set in the AI Act for the obligation to undergo re-assessment as well as for assessment of AI systems that already operate within the EU.

After performing a conformity assessment, the provider should register this high-risk AI system in an EU database managed by the European Commission to increase public transparency and oversight and strengthen *ex post* supervision by competent authorities.

The requirements applicable to design and development of certain AI systems before they are placed on the market will be further operationalised through harmonised technical standards, raising significant concerns as to how they would reflect democratic values and respect fundamental rights (McFadden et.al., 2021). Although the draft AI Act sets an obligation to introduce risk management systems, it does not specify what kind of risks should be assessed (Article 9 (2) c). The draft AI Act calls for establishing common normative standards for all high-risk AI systems consistent with the Charter in order to ensure a consistent high level of protection of public interest in terms of health, safety and fundamental rights (Recital 13). However, the risks to fundamental rights are more challenging to identify in the field of AI than that of products. Not only are the use cases for AI harder to predict than those of physical objects,

but AI applications are typically embedded within complex systems so it is difficult for a provider of an AI application to predict all the ways in which that system could be used or could impact fundamental rights (McFadden et.al., 2021).

The draft AI Act does not require users, in contrast to providers, to conduct a risk assessment of AI systems, as they will simply follow the instructions for use supplied by the provider accompanying high-risk AI systems and monitor their operation on the basis of those instructions (Article 29 (1), (4)), although the risks to a large extent may depend on the way the systems are used.

Thus, the AI Act should not miss the opportunity to introduce impact assessments that would require users to identify and assess the impacts of AI systems on fundamental rights as well as on society, democratic values, the environment, and so on (EDRI, 2021a). Impact assessments of this kind have been suggested by international organisations as one of the main AI accountability mechanisms (UNESCO, 2021, para. 50, 51) as well as academics (Mantelero & Esposito, 2021; Reisman et.al., 2018).

No reference appears in the draft AI Act either to the rights of individuals, for example, when assessing whether an AI system poses a high risk to fundamental rights (Article 7 (2)), or to complaints and redress mechanisms available to individuals and communities affected by AI systems. EDPB and EDPS have recommended that the AI Act should also address the risks posed by AI systems to groups of individuals or society as a whole (EDPB & EDPS (2021) – risks that have also been recognized by scholars (Taylor et. al., 2017).

In addition to the requirements set in the draft AI Act, both providers and users of high-risk AI systems would be required to ensure compliance with existing data protection law. The draft AI Act only indicates that users of high-risk AI systems should use the instructions for use provided under Article 13 (setting transparency obligations and provision of information to users) to comply with their obligation to carry out a data protection impact assessment (Article 29 (6)). The EDPB and EDPS recommend setting compliance with data protection law as one of the requirements in the AI Act (EDPB & EDPS, 2021). Remote biometric identification systems should comply with data protection requirements that mandate a legal basis for processing biometric data and allow processing only under strict conditions (Madiega & Mildebrath, 2021). Data protection standards also apply to all other AI systems processing personal data and classification of AI systems. Moreover, the fact that AI systems are not classified as high-risk within the meaning of the draft AI Act does not mean that processing personal data by such systems could not be considered as high-risk when applying data protection rules, for example, in the case of biometric categorisation and emotion recognition.

The draft AI Act states that the fact that an AI system is classified as high risk should not be interpreted as indicating that use of the system is necessarily lawful under other EU norms or under national law, such as those on protection of personal data, on use of polygraphs and similar tools or other systems to detect someone's emotional state. The AI Act should not be understood as providing a legal ground for processing personal data, including special categories of personal data, where relevant (Recital 41, draft AI Act). The provision only refers to AI systems 'classified as high-risk', but not to AI systems classified as limited risk, such as emotion recognition systems.

The draft AI Act classifies certain AI predictive systems in law enforcement as high-risk, that is, systems used for:

- making individual risk assessments of natural persons in order to assess the risk of offending or reoffending (Annex III, 6 (a));
- predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons or assessing the personality traits and characteristics or past criminal behaviour of natural persons or groups (Annex III, 6 (e)).

Predictive tools carry an inherent risk of perpetuating or even enhancing discrimination, reflecting embedded historic racial and ethnic bias in the data sets used, such as a disproportionate focus on policing certain minorities (OHCHR, 2021).

Emotion recognition systems used in law enforcement and in the area of migration, asylum and border control management are also classified as high-risk systems, that is, AI systems used as polygraphs and similar tools or to detect the emotional state of a natural person (Annex III, 6 (b), (7 (a)).

AI systems coupled with biometric techniques have led to a re-emergence of lie detection and other predictive systems that analyse human behaviour. For example, the EU-funded iBorderCtrl project testing AI for facial "lie detection" to control immigration, which ended in 2019, raised major public criticism. The use of these systems is highly contested, as they are not based on sound science (Wendehorst & Duller, 2021).

Behavioural detection systems touch the essence of human dignity, deeply affect enjoyment of the right to privacy and carry inherent risks of discrimination and may undermine other human rights, such as the rights to liberty and to a fair trial (EDPB & EDPS, 2021, OHCHR, 2021). These concerns will be discussed further below.

Although the draft AI Act acknowledges that high-risk AI systems may be unlawful, each use case of these systems would be assessed on a case-by-case basis. This approach does not seem to provide effective protection against the significant risks these systems clearly pose.

4.3. Biometric categorization and emotion recognition – limited risk or rather prohibited AI systems

The draft AI Act classifies emotion recognition and biometric categorization systems as limited-risk AI systems. The draft Act provides definitions of both systems. 'Emotion recognition system' means 'an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data' (Article 3 (34)). 'Biometric categorisation system' means 'an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data' (Article 3 (35)).

The draft AI Act claims to lay down harmonized transparency rules for these systems (Article 1 (c)). Accordingly, users of an emotion recognition or a biometric categorisation system must inform those exposed to the operation of such a system. This obligation will not apply to AI systems used for biometric categorisation, which are permitted by law to detect, prevent and investigate criminal offences (Article 52 (2)). The obligations will not affect the requirements and obligations set for high-risk AI systems (Article 52 (4)).

These transparency obligations add no new requirements that are not already included in the existing data protection law, namely Article 13 GDPR. If this provision is for emotional recognition and biometric classification systems that do not process biometric data – an interpretation that brings with it many problems – this reasoning would see the European Commission implicitly legitimising a contentious and restrictive reading of the GDPR (Veale & Zuiderveen Borgesius, 2021).

Emotion recognition systems and biometric categorisation systems may also fall within the category of high-risk AI systems depending on the area where they are used, for example, if they are used in the areas of education, employment, law enforcement, or migration.

Moreover, the high-risk area – biometric identification and categorization of natural persons – refers to two kinds of system, with only remote biometric identification set as one of the sub-areas under this area. This could provide the opportunity later to expand the area to include biometric categorization. However,

it is unclear why these systems have not already been included in this area but rather categorized generally as limited-risk AI systems. The title of this area also does not include emotion recognition systems. The draft AI Act empowers the European Commission to expand the list of high-risk AI systems used within certain pre-defined areas already set in Annex III. However, it does not enable addition of new areas or amendment of existing ones, thus not enabling emotion recognition systems to be added as high-risk systems in the area of biometric identification and categorization of natural persons.

Classifying emotion recognition systems and biometric categorisation systems generally as limited-risk AI systems (although in some cases falling within the high-risk category), where risks can be sufficiently mitigated simply by transparency rules, while at the same time not acknowledging the need for any other limitations and requirements, will fail to meaningfully address the significant risks that these systems pose to fundamental rights.

Emotion recognition and biometric categorisation systems have been increasingly used by both private and public entities across multiple sectors within the EU, including for law enforcement and border control purposes (Wendehorst & Duller, 2021). They raise significant risks to human dignity, autonomy, the right to privacy and other fundamental rights. Biometric recognition systems analysing and predicting our behaviour and emotions through facial expressions, tone of voice, gait, and heart rate, affect our psychological integrity, deeply interfere with our personal sphere and severely limit our ability to freely express our personality, autonomy, and freedom of thought (AI HLEG, 2019; McStay, 2020; CAHAI, 2020; OHCHR, 2021; Ben-Israel et.al., 2020) AI systems categorizing individuals from biometrics into clusters according to ethnicity, gender or other grounds of discrimination prohibited under Article 21 of the Charter contradict fundamental rights and EU values (EDPB & EDPS, 2021).

Moreover, the scientific validity of emotion recognition and biometric classification systems is not proven (Heaven, 2020). There is no scientific evidence proving the abilities of AI systems that they claim, e.g. there is no proof that a person's inner emotions can be accurately 'read' from facial expressions, heart rate or tone of voice (Barrett et. al., 2019). These systems present severe problems of inaccuracy and bias leading to discrimination and social inequalities (Heaven, 2020).

EDPB and EDPS (2021) call for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces – such as faces but also gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals – in any context, recommend a prohibition on biometric categorisation, for both public authorities and private entities, as well as on the use of AI to infer the emotions of a natural person, except for certain well-specified use-cases, namely for health and research purposes. This opinion has been endorsed by many other actors (Muller & Dignum, 2021, EDRI, 2021a; CAIDP, 2021).

The proposed classification of emotion recognition and biometric categorisation systems as limited risk or high-risk AI systems in the draft AI Act, rather than prohibiting their use, could normalize or even legitimate the use of these scientifically unfounded systems contravening fundamental rights and democratic values.

5. Conclusion

The draft AI Act is the first initiative in the world that provides a legal framework to address the risks of AI systems and aims to promote trustworthy AI, at the same time requiring introduction of prohibitions on certain AI practices that violate fundamental rights.

Although introducing a ban on prohibited AI practices in the draft AI Act is as such a significant step forward in the debate on introducing red lines in the AI regulatory framework, EU legislators still need to

take courageous further steps to introduce clear prohibitions in the draft AI Act before it becomes law. Prohibiting the use of remote biometric identification systems in the draft AI Act is severely limited and would allow a wide range of surveillance practices. Use of these systems for law enforcement purposes, although permitted in exceptional cases, could almost always be justified. Moreover, the conditions for such uses are very vaguely worded and partly reflect essential guarantees for use of surveillance measures recognized by the CJEU and the ECtHR and would not be able to prevent use of AI systems for mass surveillance. The exceptions and loopholes with regard to all prohibited AI practices should be removed.

The proposed classification of biometric surveillance systems in the draft AI Act should be reconsidered in order to meaningfully address the risks they pose to fundamental rights. Classifying biometric systems as high-risk or limited-risk AI systems could normalise or even legitimatise their use. The draft AI Act should prohibit emotion recognition and biometric categorisation as these AI practices violate fundamental rights and are scientifically unfounded.

The draft AI Act should also strengthen legal requirements for accountability and transparency, enhance existing data protection standards, introduce third-party conformity assessments for all high-risk AI systems, complaints and redress mechanisms, and in addition not missing the opportunity to introduce impact assessment on users of high-risk AI systems to assess the impact of AI systems on fundamental rights as well as other impacts, including on democratic values and the rule of law.

Acknowledgments

The author wishes to thank Prof. Helene Oppen Ingebrigtsen Gundhus (University of Oslo) for her comments on the publication.

The Open Access publication of this paper was supported by the Panelfit project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Funding

The work has been funded under Nordforsk Research and Innovation Programme on Digitalisation of the Public Sector and is an output of the project No. 100786 Critical Understanding of Predictive Policing (CUPP).

References

Access Now (2020). *Europe's Approach to Artificial Intelligence: How AI Strategy is Evolving.* https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf.

AI HLEG. (2019). *Ethics Guidelines for Trustworthy AI.* https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Barrett, L. F., Adolphs, R., Marsella, S., Martinez, A. M., & Pollak, S. D. (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements. *Psychological Science in the Public Interest*, *20*(1), 1-68. doi: 10.1177/1529100619832930.

Ben-Israel, I. et.al. (2020). *Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law.* Council of Europe. https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a.

CAHAI. (2020). *Feasibility Study.* Council of Europe. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.
CAIDP. (2021). *Statement on Proposed EU AI Regulation.* https://www.caidp.org.
Council of Europe. (2021). *Guidelines on Facial Recognition.* https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.
Christakis, T., & Becuywe, M. (2021). Pre-Market Requirements, Prior Authorisation and Lex Specialis: Novelties and Logic in the Facial Recognition-Related Provisions of the Draft AI Regulation, *European Law Blog.* https://europeanlawblog.eu/2021/05/04/pre-market-requirements-prior-authorisation-and-lex-specialis-novelties-and-logic-in-the-facial-recognition-related-provisions-of-the-draft-ai-regulation/.
Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119.
EDPB, EDPS. (2021). *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en.
EDPB. (2019, 22 August). Facial recognition in school renders Sweden's first GDPR fine. https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en.
EDPB. (2021, 21 February). Swedish DPA: Police unlawfully used facial recognition app. https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_lv.
EDPB. (2020). *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.* https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_lv.
EDRI. (2021a). *European Commission adoption consultation: Artificial Intelligence Act.* https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf.
EDRI. (2021b, 17 February). New ECI calls Europeans to stand together for a future free from harmful biometric mass surveillance. https://edri.org/our-work/new-eci-ban-biometric-mass-surveillance/.
EPIC. (2021). *Feedback of the Electronic Privacy Information Center to the European Commission Regarding the Proposal for Harmonized Rules on Artificial Intelligence.* https://epic.org/apa/comments/EPIC-EC-Aug2021-AIA-Comments.pdf.
European Commission. (2021). *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence act) and amending certain union legislative acts.* (COM(2021) 206 final).
European Parliament. (2021, 8 March). MEP's Letter to the European Commission. https://edri.org/wp-content/uploads/2021/ropean Parli03/MEP-Letter-on-AI-and-fundamental-rights-1.pdf.
European Parliament. (2020). *Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL))* https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html.
European Commission. (2020). *White Paper On Artificial Intelligence – A European approach to excellence and trust.* https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.
FRA. (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law.
Heaven, D. (2020). Why faces don't always tell the truth about feelings. *Nature*, *578*(7796), 502-504.
McFadden, M., Jones, K., Taylor, E., Osborn, G. (2021). *Harmonising Artificial Intelligence. The role of standards in the EU AI Regulation.* Oxford Information Labs. https://oxcaigg.oii.ox.ac.uk/wp-content/uploads/sites/124/2021/12/Harmonising-AI-OXIL.pdf.
Madiega, T., & Mildebrath, H. (2021). *Regulating facial recognition in the EU.* European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf.
Malgieri, G., & Ienca, M. (2021, July 7). The EU regulates AI but forgets to protect our mind. *Eurioean Law Blog.* https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/.
Mantelero, A., & Esposito, M. S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, 41, doi: 10.1016/j.clsr.2021.105561.
Mantelero, A. (2020). Regulating AI within the Human Rights Framework: A Roadmapping Methodology. In Czech P., Hesch L., Lukas K., Nowak M., Oberleitner G. (Eds.). *European Yearbook on Human Rights*. Cambridge: Interesentia, Vienna: NWV Verlag GmbH. pp. 477-502. doi: 10.1017/9781839701139.020.
McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society*. doi: 10.1177/2053951720904386.
Montag, L., Mcleod, R., De Mets, L., Gauld, M., Rodger, F., Pełka, M. (2021). *The Rise and rise of biometrics mass surveillance in the EU. A legal analysis of biometrics mass surveillance practices in Germany, the Netherlands, and Poland.* EDRi – European Digital Rights. https://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf.

Muller, C., & Dignum, V. (2021). *Artificial Intelligence Act. Analysis & Recommendations.* ALLAI. https://allai.nl/wp-content/uploads/2021/08/EU-Proposal-for-Artificial-Intelligence-Act-Analysis-and-Recommendations.pdf.

OHCHR. (2021). *The right to privacy in the digital age.* https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E.

Ragazzi, F., Kuskonmaz, E.M., Z Plájás, I., van de Ven, R., Wagner, B. (2021). *Biometric and Behavioural mass surveillance in EU Member States*. http://extranet.greens-efa-service.eu/public/media/file/1/7297.

Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.

Reisman, D., Schultz, J., Crawford, K., & Whittaker, M., (2018). *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability.* AI Now. https://ainowinstitute.org/aiareport2018.pdf.

Sartor, G., & Lagioia, F. (2020). *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence.* European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.

Smuha, N.A. (2021). Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea. *Philosophy & Technology*, *34*, 91-104, doi: 10.1007/s13347-020-00403-w.

Taylor, L, Floridi, L., van der Sloot, B. (Eds.). (2017). *Group Privacy: New Challenges of Data Technologies*. Cham: Springer International Publishing.

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97-112, doi: 10.9785/cri-2021-220402.

Veliz, C. (2020). *Privacy Is Power. Why and How You Should Take Back Control of Your Data*. Bantam Press.

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence.* https://unesdoc.unesco.org/ark:/48223/pf0000380455?3=null&queryId=ade1add6-b32e-4243-ad62-fc213ed25f19.

Wendehorst, C., & Duller, Y. (2021). *Biometric Recognition and Behavioural Detection. Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces.* European Parliament. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2021)696968.

Author biography

Dr. Irena Barkane is a researcher at the Institute of Legal Science, Faculty of Law, University of Latvia. Her research interests cover the relationship between law and technology, artificial intelligence regulation, human rights, EU law, security, data protection and privacy issues. She leads research projects related to regulation, legal, ethical and social implications of new digital technologies and teaches Information Technology Law course. She also regularly participates at international conferences, such as ESIL and Riga StratCom Dialogue. Previously she was a Legal Adviser at the Ministry of Justice of the Republic of Latvia working with cases brought before the Court of Justice of the European Union. In 2020 Irena was appointed as one of 24 members of the UNESCO Ad Hoc Expert Group on the elaboration the first draft of the Recommendation on the Ethics of Artificial Intelligence and continued to represent Latvia as expert in the intergovernmental negotiations of the Recommendation in 2021.