Comments by the International Commission of Jurists

on the

proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts

A Briefing Paper

1. Introduction

This briefing paper provides analysis based on international human rights law on selected elements of the *proposal by the European Commission of a Regulation of the European Parliament Laying Down Harmonised Rules on Artificial Intelligence*, also known as the Artificial Intelligence Act.

This draft Regulation is the first attempt in the world to set a legal framework for AI technology at supranational level and one which takes significant account of the impact of AI on human rights. The ICJ welcomes efforts in this regard, as AI technology is going to be – and to a great extent, already is - one of the defining elements of human society globally. It is therefore critical for the protection of human rights and the rule of law that States and supranational public entities, such as the European Union, step in to design and implement regulatory frameworks in order to fulfil their duty under international law to secure the respect and protection of the human rights of all, both online and offline.

2. Artificial Intelligence and international human rights law

In order to comply with EU law, and in particular the Charter of Fundamental Rights of the EU, the Regulation must accord with the human rights provisions of the Charter.

Artificial intelligence and any regulatory framework addressing its development, deployment, functioning, use and impact have the potential to affect all human rights to varying degrees depending on scope and context. While international human rights bodies have carried out thorough assessments on the impact that AI may have on the freedoms of expression and assembly or the rights to privacy including in relation to data protection, a broader range of human rights may directly or indirectly be impacted by AI technology. For example, AI may be used for the implementation of measures interfering upon the right to liberty; freedom of torture or cruel, inhuman or degrading treatment; the right to a fair trial; the right to life and the right to an effective remedy, among others.

It is therefore critical that any regulation on AI be fully in compliance with all human rights law and standards. The EU legislator should therefore pay particular attention to the fact that certain human rights allow for no restriction of any sort: the right to life (in the Council of Europe space and outside of armed conflict); freedom from torture and other cruel, inhuman or degrading treatment or punishment; freedom from slavery and forced labour, the principle of non-retroactivity in criminal law; the right to recognition as a person before the law; the freedom of thought, conscience and religion; the right to hold an opinion; the freedom from discrimination[1] and the right to an effective remedy whenever needed to seek redress for violations or abuses of these rights. The rights to liberty

[1] AI technology has been considered at high risk of perpetuating or exacerbating discriminatory practices: CERD*, General Recommendation No. 36*, para. 31, and para 32: "There are various entry points through which bias could be ingrained into algorithmic profiling systems, including the way in which the systems are designed, decisions as to the origin and scope of the datasets on which the systems are trained, societal and cultural biases that developers may build into those datasets, the artificial intelligence models themselves and the way in which the outputs of the artificial intelligence model are implemented in practice." See also, the Consultative Committee of the Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Guidelines on Facial Recognition*, 28 January 2021, Doc. T-PD(2020)03rev4, p. 5.

and a fair trial, while allowing for certain adaptations in scope, equally do not allow for restrictions in their core elements.[2]

Finally, the rights to family life, a private life, to the freedoms of expression and impart, to assembly, and association, to political participation, and to exercise one's religion or belief, while allowing for restrictions, do so in very strict situations, must not be arbitrary, must be provided by law, and be necessary and proportionate to the aim pursued. It is against these principles that the Regulation on AI must be tested.

In the present contribution, the ICJ will provide analysis and recommendation on selected issues of concern with the draft Regulation to contribute to its amelioration through the legislative process.

3. Fully prohibited practices

The ICJ welcomes that the Regulation prohibits at the forefront certain practices that are at risk of undermining human rights protection, such as AI systems that deploy subliminal techniques to manipulate one's consciousness or that exploit "any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability" and cause or "are likely to cause that person or another person physical or psychological harm".[3] It is also welcome that the Regulation prohibits the use of AI by public entities or on their behalf for the purpose of social scoring.[4]

Indeed, the UN High Commissioner for Human Rights has called on States to "[e]xpressly ban AI applications that cannot be operated in compliance with international human rights law and impose moratoriums on the sale and use of AI systems that carry a high risk for the enjoyment of human rights, unless and until adequate safeguards to protect human rights are in place."[5]

The ICJ would however stress that the concept of vulnerability may be stigmatizing in certain contexts for the group in question and it would be preferrable to refer to persons at risk in a disadvantaged position.

This notwithstanding, **the ICJ considers that the list of groups that would qualify as "vulnerable" according to article 5.1.b is excessively restrictive and risks to leave out groups that, according to human rights law and the EU Charter, would require such a specific protection.** The Commission's approach appears to be addressing situations of alleged "diminished" cognitive or emotional capacity. However, that would be insufficient to address all situations of disadvantage that could be exploited by AI to distort a person's behaviour. Just to cite article 21 of the Charter, this Regulation leaves out discriminatory impact that may occur based on sex, race, ethnic and social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth or sexual orientation. Contemporary human rights law includes also gender identity, marital and family status, health status, and economic and social situation.[6] An open-ended clause would likely provide public officials and judiciaries

[2] See, CCPR, General Comment No. 29, UN Doc. CCPR/C/21/Rev.1/Add.11, 31 August 2001. See articles 4 ICCPR and 15 ECHR and the European Court of Human Rights' jurisprudence here: https://www.echr.coe.int/documents/Guide_Art_15_ENG.pdf .
[3] Article 5,1.a-b.
[4] Article 5.1.c.
[5] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age,* UN Doc. A/HRC/48/31, 13 September 2021, para. 59
[6] CESCR, *General Comment No. 20*, UN Doc. E/C.12/GC/20.

with more capacity to interpret effectively such a prohibition to cover all affected groups.

4. Partially prohibited practices: real time remote biometric identification systems

The Regulation purportedly prohibits the use of "the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement."[7] However, the extent of the exception to such a prohibition makes it apparent that, in reality, it is at best a partial one that is vulnerable to abuse. Furthermore, it allows the use of remote biometric identification systems that are not "real-time".

This is already an issue of concern since several international authorities, including the UN High Commissioner for Human Rights, have called for a moratorium on the use of potentially high-risk technologies such as remote real-time facial recognition unless and until it is ensured that their use cannot violate human rights.[8]

According to article 5 of the draft regulation, law enforcement authorities can resort to these systems only and in as far as their use "is strictly necessary for one of the following objectives:

i. the targeted search for specific potential victims of crime, including missing children;
ii. the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;
iii. the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.

The offences under Framework Decision 2002/584/JHA, i.e. the European Arrest Warrant, are: participation in a criminal organisation, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in weapons, munitions and explosives, corruption, fraud, including that affecting the financial interests of the EU, laundering of the proceeds of crime, counterfeiting currency, including of the euro, computer-related crime, environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties, facilitation of unauthorised entry and residence, murder, grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, racism and xenophobia, organised or armed robbery, illicit trafficking in cultural goods, including antiques and works of art, swindling, racketeering and extortion, counterfeiting and piracy of products, forgery of administrative documents and trafficking therein, forgery of means of payment, illicit trafficking in hormonal substances and other growth promoters, illicit trafficking in nuclear or radioactive materials, trafficking in stolen vehicles, rape,

[7] Article 5.1.d.
[8] UN High Commissioner for Human Rights*, op. cit.* fn 5, para. 45. See, also, para. 59; Consultative Committee of the Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Guidelines on Facial Recognition*, 28 January 2021, Doc. T-PD(2020)03rev4, p. 5. See also, CAHAI Feasibility Study, para. 43.

arson, crimes within the jurisdiction of the International Criminal Court, unlawful seizure of aircraft/ships, and sabotage.[9]

Member States will need to declare if they avail themselves of this exception and, in that case, lay down national law rules for the request, issuance, exercise, supervision of authorisation to use real-time biometric identification systems. They will also be able to select which of the offences above may be amenable to the use of this law enforcement measure.

The use of these measures will have to be authorised by a judicial authority or by an independent administrative authority that must be "satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives".[10] It must issue a reasoned decision and take into account "the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system [and] the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences."[11] However, this requirement does not apply "in a duly justified situation of urgency, [where] the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use."[12]

Finally, the use of these biometric identification systems has to comply with unspecificed "necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations."[13]

4.1. Assessment

A real-time remote biometric identification system is 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, without prior knowledge of the user of the AI system whether the person will be present and can be identified, and whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay.[14] It is, depending on the use done and the data used, a surveillance system, whether on a massive or targeted scale. It is therefore crucial that the human rights framework related to surveillance and wiretapping be respected, with the additional consideration that certain steps will be undertaken by artificial intelligence.

4.1.1. Human Rights Law and Standards

Under international human rights law, any measure that entails an interference with the rights to freedom of opinion and expression, freedom of assembly and association and the right to privacy, under articles 7, 8, 11, and 12 of the EU Charter, articles 8, 10 and 11 of the European Convention on Human Rights (ECHR)

[9] Article 2.2. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584
[10] Article 5.3.
[11] Article 5.2
[12] Article 5.3.
[13] Article 5.2.
[14] Article 2.36-37.

and articles 17, 19, 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR), can only be justified

- if it is provided in law and consistent with the principles of legality;
- pursues one of the legitimate aims in the exhaustive provided under these articles, is necessary to achieve that aim;
- is proportionate, in that it is the least intrusive measure necessary to achieve the legitimate aim and does not imperil the essence of the right;[15] and
- is not discriminatory.[16]

Along similar lines, article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

With regard to the requirement of prescription by law, the European Court of Human Rights has held that the domestic law authorising the restriction "must also be compatible with the rule of law[,] be accessible to the person concerned and foreseeable as to its effects."[17] In consonance with the principle of legality, the law must be "formulated with sufficient precision to enable the [individual] to regulate his conduct; he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[18]

The UN Human Rights Council's Special Rapporteur on freedom of opinion and expression has further affirmed that "the standards of legality[mean] that [restrictions to human rights] are interpreted by independent judicial authorities"[19]

Any regulatory framework must clearly determine the purpose of the use of AI by law enforcement officials and regulate "as accurately as possible the parameters and guarantees that prevent breaches of human rights."[20] The CJEU has ruled that "EU legislation … must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data [and the] need for such safeguards is all the greater where … personal data are subjected to automatic processing and where

[15] *Big Brother Watch and Others v UK*, ECtHR, GC, Applications Nos. 58170/13, 62332/14 and 24960/15, 25 May 2021, para. 332. See, *Roman Zakharov v. Russia*, ECtHR, GC, Application No. 47143/06, 4 December 2015, para. 227; *Kennedy v. UK*, ECtHR, Application No. 26839/05, 18 May 2010, para. 130. See also, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the General Assembly,* UN Doc. A/74/486, 9 October 2019, para. 34; *Annual Report to the General Assembly*, Un Doc. A/73/348, para. 28. See also, among others, Judgment of 9 November 2010 (Grand Chamber), *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662) 11, para. 65.

[16] See, among other sources, CCPR, General Comment No. 34, UN Doc. CCPR/C/GC/34; CCPR, General Comment No. 37, UN Doc. CCPR/C/GC/37, and the Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights at https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf .

[17] *Big Brother Watch and Others v UK*, *op.cit.,* para. 332. See also, Heglas v. the Czech Republic, ECtHR, Application No. 5935/02, 1 March 2007, para. 74; *Roman Zakharov v Russia*, *op. cit.*, § 228; *Delfi AS v. Estonia*, ECtHR, GC, Application No. 64569/09, 16 June 2015, para. 120.

[18] *Delfi AS v. Estonia*, *op. cit.*, para. 121; *Ahmet Yildrim v. Turkey*, ECtHR, Application No. 3111/10, 18 December 2012 , para. 57.

[19] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the General Assembly,* A/73/348, para. 28.

[20] CERD, *General Recommendation No. 36*, para. 58.

there is a significant risk of unlawful access to those data."[21] The standard is that of "strict necessity".[22] The Court required that there be objective criteria for the identification of the seriousness of the offences or activities for which data retention could apply. In *Schrems*, the CJEU held that any EU legislation must lay down clear and precise rules governing the scope and the application of the measure, and impose minimum safeguards.[23]

When dealing with wiretapping of communications in criminal investigations and situations of national security, the European Court has set minimum requirements for what should be set out in law, to ensure that any interference with private life rights meets standards of prescription by law, necessity and proportionality. These require that the law should set out : "(i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed."[24]

When dealing with secret surveillance, the Court has affirmed that, while "the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge, [in] a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, … it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."[25] Once surveillance is terminated, notification to the individual is of the essence to ensure effective access to justice against any potential violation.[26]

4.1.2. ICJ Assessment

A biometric identification system will likely have to work by scanning and sorting out massive amounts of data to identify an individual based on AI technology and will therefore be part of a surveillance or interception system.

The proposal by the Commission makes important references to the requirements of necessity and proportionality and provides welcome criteria for reasoned decisions. However, in light of the international and EU human rights obligations of the EU and its Member States, the proposal still raises serious concerns.

First of all, **the proposal does not respect the requirement that a restriction be strictly necessary and proportionate to a legitimate aim pursued and be clearly defined by law.** The search for victims of crimes, as a component of public order, may be a necessary and legitimate purpose and the second priority is very clearly defined both by the imminence criterion and by the identification of the seriousness of the harm, i.e. the threat to life or physical safety.

[21] *Digital Rights Ireland Ltd* (C-293/12), para. 54-55. See also *Tele2 Sverige AB (C-203/15),* paras. 118-122*, Schrems (C-362/14),* para 91.
[22] *Ibid.*, para. 56; *Schrems, op. cit.,* para. 92.
[23] *Schrems, op. cit.,* para. 91.
[24] *Big Brother Watch and Others v UK*, *op.cit.,* para. 335. See also, *Roman Zakharov v. Russia*, *op. cit.*, para. 231.
[25] *Ibid.*, para. 336
[26] *Ibid.*, para. 337.

The ICJ has, however, **serious concerns with regard to the third priority encompassing criminal offences that**, depending on the level of maximum punishment foreseen in national laws, **are not effectively serious in terms of the human rights they protect**, such as counterfeiting and piracy of goods. Based on this article, AI may be used, for example, for the biometric identification of teenagers copying movies online in infringement of copyright rules. It is particularly concerning that the grounds of implementation of such an intrusive AI measure are done via a cross-reference to the European Arrest Warrant that has been demonstrated to have already been abused by several States because the offences listed in it are not all "serious" in nature and have different definitions in different member States.[27]

Furthermore, the requirement of the three years of maximum punishment coupled with States' discretion, instead of providing any guarantee, further increases the **unforeseeability** of the use of AI, as it would be unclear to any person which country will resort to it and in which situations.

Secondly, while the requirement of prior judicial authorisation is in line with human rights law, the possibility to resort instead to independent administrative authorities falls short of it. International human rights standards require that such a decision be taken by an order by a judicial authority or other independent administrative authority, whose decisions are subject to judicial review.[28] **It is important therefore that the Regulation ensures the possibility of judicial review in all circumstances.**

Thirdly, **the possibility of skipping the prior authorisation requirement "in a duly justified situation of urgency" is prone to arbitrary application.** The Regulation contains a definition of urgency that refers to "situations where the need to use the systems in question is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use."[29] While it limits the use to the "absolute minimum necessary", the focus remains on the maintenance of the possibility to resort to AI and not on the content of the urgency itself. The Regulation does not even address who should decide what constitutes urgency, but instead leaves this to national law. This vagueness is insufficient to respect the principle of legality, which is a key requirement for any restriction or derogation under international human rights law.

The ICJ finally notes that a concerning element lies in the very definition of law enforcement authorities that includes "any public authority competent for - or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of - the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[30] This inappropriately may include intelligence services and private entities, such as private security contractors, if so entrusted by the State, and it is apparent that

[27] See, ICJ, Transnational Injustices, 2017, p. 33; European Arrest Warrants, Ensuring an effective defence, a JUSTICE Report, 2012, p. 35. JUSTICE is the UK Section of the International Commission of Jurists; Gisele Vernimmen-Van Tiggelen, Laura Surano and Anne Weyembergh, The future of mutual recognition in criminal matters in the European Union, Institut d'Etudes Européennes, Université de Bruxelles, 2009; European Commission, On the implementation since 2007 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, EU Doc. COM/2011/0175 final; Council of the EU, Issues of proportionality and fundamental rights in the context of the operation of the European Arrest Warrant, EU Doc. 9968/14, 20 May 2014, p. 2.

[28] Appendix to Recommendation CM/Rec(2018)2, Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities, paras. 1.3.1 – 1.3.2; para. 2.1.3.

[29] Recital 21

[30] Article 3.1.40.

forces tasked with prevention of criminal offences or threats to public security may use AI.

5. Definitions and scope

5.1. Definition of AI

The Regulation is affected by a critical weakness at its core: the lack of definition of what is artificial intelligence. Instead of providing a definition, recital 6 and article 3 list specific techniques and approaches amounting to AI. This list is to be established and kept up to date by the Commission under delegated acts.[31]

Recital 6 affirms that the "notion of AI system should be clearly defined to ensure legal certainty, while providing the flexibility to accommodate future technological developments. The definition should be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension. AI systems can be designed to operate with varying levels of autonomy and be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded). The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to–date in the light of market and technological developments through the adoption of delegated acts by the Commission to amend that list."

Article 3.1 defines AI systems as "'software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

The text of these articles provides for no specific constraint on what the Commission can consider to be AI as nowhere is it specified that these techniques and approaches must be within an overall AI definition apart from a generic capacity to "generate outputs … or decisions influencing the environment they interact with".

The vagueness and overbreadth of this definition is not in line with the requirement of legality for any restriction of human rights that may be contemplated by this Regulation. While the Commission will hopefully provide for more clarity in delegated legislation, it will be difficult to evaluate the necessity and proportionality of measures based on technologies that will be considered AI only ex post facto, and for which tailored considerations may not be possible but that will simply inherit the AI regime of the Regulation. Furthermore, it is of concern that the very object of the Regulation will be defined effectively only by the Commission, without a meaningful involvement of the co-legislators.

[31] A3.1 that delegates the very definition to the Annex 1 modifiable by the Commission under article 4 and 73

5.2. Definition of high-risk AI

In a manner similar to the deficient definition provided for AI, articles 6, 7 and 8 give wide discretion to the Commission to assess what are high risk AI systems, that are allowed to be put on the market under certain conditions. However, here the Commission would operate under quite detailed criteria. This is a better system that could be adopted also for the more general AI definition.

It is, however, of concern that centrality in the definition of "high risk AI systems" is given to the element of intention of the producer of the AI application instead of its actual impact on human rights. According to Article 3.12 the "'intended purpose' means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation."

In a system where AI may be self-learning and adaptative, it is unwise to centralise the system on the "intention" of the producer and not on the most traditional category of harm under tort law, or on responsibility of private entities to exercise human rights due diligence under the UN Guiding Principles on Business and Human Rights, and the effective capacity of such technologies to be used for – or being cause of - violations and abuses of human rights.

5.3. Scope of application of the Regulation

The ICJ is further concerned that the Regulation does not apply to "AI systems developed or used exclusively for military purposes"[32] nor to "public authorities in a third country nor to international organisations ..., where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States."[33]

With regard to the military purposes, while it is understandable that the sphere of defence is not yet under EU regulatory competence, it is very problematic to exclude systems "developed" for military purposes, even if exclusively. Technological advances are often carried out at first for exclusive military purposes that later find a civilian use, sometimes unexpected.

With regard to the third countries or international organisations, this exception this is highly problematic as it relates to the field of law enforcement and judicial cooperation where a high level of interference with human rights, including even the right to liberty, is possible. The increasing relevance of international cooperation in this field militates against an exclusion of such entities unless covered by a current immunity agreement, as is often the case for international organisations and for which, therefore, a specific clause in this Regulation would be redundant. The current clause would allow third States to make use of AI systems banned in the EU and then to provide results of its functioning to EU institutions, Member States or private entities in disregard of this Regulation. In a

[32] Article 2.3.
[33] Article 2.4.

globalised digital world such as the present, it would provide a safe haven from the reach of this Regulation's guarantees.

6. Oversight authorities

The Regulation introduces a complex system of oversight, based on compliance assessment bodies, also referred to as notified bodies, doing third-party compliance assessment activities, including testing, certification and inspection; and notifying authorities, responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of compliance assessment bodies and for their monitoring. The Regulation identifies the task of applying and implementing the Regulation upon national authorities appointed by the State and that should be objective and impartial. From among them will be selected the notifying authority for the country.

It institutes a European Artificial Intelligence Board to provide advice and assistance to the Commission in order to contribute to the effective cooperation of the national supervisory authorities and the Commission with regard to matters covered by the Regulation; coordinate and contribute to guidance and analysis by the Commission and the national supervisory authorities and other competent authorities on emerging issues across the internal market with regard to matters covered by this Regulation; and assist the national supervisory authorities and the Commission in ensuring the consistent application of the Regulation.

The UN Human Rights Committee, OHCHR and the Committee of Ministers of the Council of Europe have called for independent and transparent scrutiny over decisions affecting data and the use of algorithmic systems.[34] The UN Special Rapporteur on freedom of opinion and expression has recommended that the independence of oversight bodies or regulators must be assured and scrupulously respected.[35]

The Court of Justice of the EU has ruled that "supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task of establishing a fair balance between the protection of the right to private life and the free movement of personal data. The mere risk that the scrutinising authorities could exercise a political influence over the decisions of the competent supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks."[36]

[34] CCPR, *General Comment No. 37*, para. 62; A/HRC/39/29, para. 33; A/HRC/48/31, para. 47. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, ad*opted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies, para. 4.4.* ee also, CAHAI Feasibility Study, para. 43

[35] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Annual Report to the UN Human Rights Committee,* A/HRC/47/25, paras. 59, 60.

[36] Judgment of 9 March 2010 (Grand Chamber), Commission v Germany (C-518/07, EU:C:2010:125) 5. See also, Judgment of 16 October 2012 (Grand Chamber), Commission v Austria (C-614/10, EU:C:2012:631): "The fact that such an authority has functional independence in so far as its members are independent and are not bound by instructions of any kind in the performance of their duties is not by itself sufficient to protect that supervisory authority from all external influence. The independence required in that connection is intended to preclude not only direct influence, in the form of instructions, but also any indirect influence which is liable to have an effect on the supervisory authority's decisions."

The ICJ is concerned that the regulation does not prescribe a requirement of independence for notifying authorities nor for notified bodies, even if the latter are called upon to "act independently". Article 59 on national competent authorities should clearly include a requirement of structural independence.

While it is welcome that there must be an appeal from decisions of notified bodies, it is not clear whether that should be to any independent body, possibly an administrative authority or a judicial body. Furthermore, the Regulation gives standing for such a legal action to those with "legitimate interest" leaving unclear whether civil society could fit into the definition or collective actions are contemplated.

Likewise, it is of concern that the European Board has a merely advisory role and leaves all supervisory power in the hands of the European Commission, i.e. an executive body. **Article 57 should make clear that the Board shall be independent of Member States, any executive authority and the European Commission and Council.** It is problematic that the European Commission, an executive body, chairs the Board. While it is welcome that observers may be invited, the impact on AI on human rights is so strong that more expertise in the field should be guaranteed. For that reason, **the ICJ considers that the FRA should be a member of the Board and that a meaningful participation by civil society should be ensured.**

7. Remedies

The ICJ notes that the draft Regulation misses the opportunity to provide much needed standards and rules for States and EU institutions to provide effective remedies[37] for human rights violations and abuses committed via the use of AI or by AI technology.

International human rights law provides that individuals must be able to access effective remedies and redress for their human rights violations occurring both online and offline.[38]

The Council of Europe Recommendation on the human rights impacts of algorithmic systems[39] affirms that "States should ensure equal, accessible, affordable, independent and effective judicial and non-judicial procedures that guarantee an impartial review, in compliance with Articles 6, 13 and 14 of the Convention, of all claims of violations of Convention rights through the use of algorithmic systems, whether stemming from public or private sector actors. Through their legislative frameworks, States should ensure that individuals and groups are provided with access to effective, prompt, transparent and functional and effective remedies with respect to their grievances. Judicial redress should remain available and accessible, when internal and alternative dispute settlement mechanisms prove insufficient or when either of the affected parties opts for

[37] Article 47 EU Charter, article 2.3 ICCPR and article 13 ECHR. A thorough analysis of the right to a remedy is to be found in, ICJ, Practitioners' Guide No. 2, available at https://www.icj.org/wp-content/uploads/2018/11/Universal-Right-to-a-Remedy-Publications-Reports-Practitioners-Guides-2018-ENG.pdf .

[38] See, UN Special Rapporteur on the promotion and protection of the right to freedom of assembly and association, *Annual Report to the UN Human Rights Council,* UN Doc. A/HRC/41/41, para. 15.

[39] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, a*dopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies.*

judicial review or appeal."[40] Remedies should be provided as well by the private sector that should also allow for collective redress mechanisms, both offline and online and that should not foreclose access to national judicial bodies.[41]

While national legal systems may provide judicial remedies via their tort law and civil liabilities systems, as well as regulations on the responsibility of the producers, AI technology gives rise to complex questions of jurisdiction, choice of the judicial forum, as well as the causality chain in tort law that would require regulation at European level to be able to address the global complexity of the phenomenon. **The ICJ urges that these concerns be addressed in this Regulation or, if this is not possible, that the European Commission urgently presents a legislative proposal in this regard.**

[40] *Ibid., 4. 5*
[41] *Ibid., 4.4 on Private Entities*. The same is affirmed in paras 1.5.1 – 1.5.2 and 2.5.1 – 2.5.3., Appendix to Recommendation CM/Rec(2018)2, Guidelines for States on actions to be taken vis-à-vis internet intermediaries with due regard to their roles and responsibilities