EU biometric data regulation: Part 2: the AI act

Kindt, E.J.

LECTURE NOTES

EU BIOMETRIC DATA REGULATION, Part 2: The AI Act

By Els J. Kindt, Center for Law and Digital Technologies of Universiteit Leiden, The Netherlands

Els J. Kindt is an associate professor and affiliated senior researcher with, respectively, eLaw, and the Center for Law and Digital Technologies of Universiteit Leiden, (https://www.universiteitleiden.nl/en/law/institute-for-the-interdisciplinary-study-of-the-law/elaw), The Netherlands, as well as the Centre for IT and IP Law (CITIP) of KU Leuven, Belgium (https://www.law.kuleuven.be/citip/en/). She also has her own research and advice company, RADL. Kindt has worked in law and biometric-related projects for more than 20 years, resulting in many publications, teaching posts, and conference presentations. In 2020, she set up the Biometric Law Lab (BLL) to consolidate research on the legal aspects of biometrics.

Abstract: In Part I of our **Lecture Notes** article on biometric data regulation, which ran in the December 2023 issue of this newsletter, we explained the EU data protection regulations found in the General Data Protection Regulation (GDPR) that are applicable to biometric data processing. We also focused primarily on the context of research activities. In Part II presented here, we discuss the EU Artificial Intelligence Act and the biometric data regulations it contains. We touch upon the distinct definition of biometric data for AI systems within this Act, and briefly explain its tier based structure. We also examine the Act's prohibitions of untargeted facial image scraping, biometric categorization, emotion identification or inference based on biometric data, and "real time" remote biometric identification of AI systems. We will also mention the possible impact these new provisions could have on research and development activities.

General Information

The AI Act of 13 June 2024, also known as AIA, was adopted and published in the summer of 2024 after much debate and many negotiations.[1] Application of the AI Act will phase in gradually. The prohibitions of Article 5 discussed below apply as of February 2, 2025. The high-risk obligations of AIA Article 6 apply as of August 2, 2027, when the whole act becomes fully applicable.

AIA is a comprehensive set of rules for AI systems placed in the market, put into service, and/or used in the EU. The Act demonstrates a particular sensibility for biometrics. One of the core objectives of the AI Act is to provide *a consistent and high level of assurance* that *AI technologies*

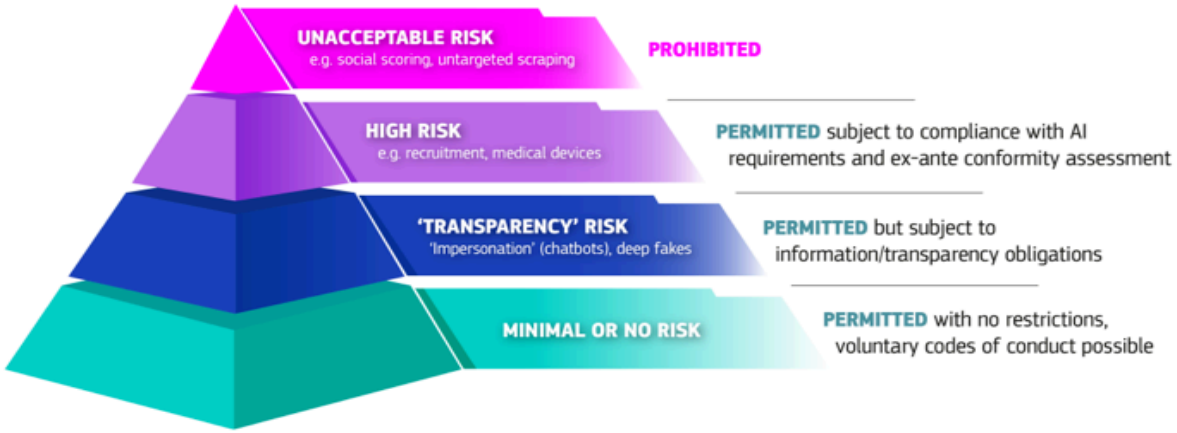


Figure 1. Illustration of how the EU AI Act follows a risk-based approach to setting regulations. Drawing © EU Commission. See the EU Commission, Digital Strategy, *The AI Act.* https://digital-strategy.ec.europa.eu/en/factpages/ai-act.

and tools are trustworthy and safe, and *have been developed and used in accordance with European Union (EU) fundamental rights obligations*.[2] The AI Act is based on constitutional values, such as respect for human dignity, freedom, and democracy, non-discrimination, the rule of law and respect for human rights, including the right to not be discriminated against and to have data protection, the latter also being a fundamental right.

The AI Act is a specific law, a "*lex specialis," filling up the gaps of more general legislation* for AI systems, including the *data protection regulations*. It affects the development and use of AI systems as defined, [3] including those related to research and development. The Act establishes a tiered, risk-based framework for AI systems. Some are *prohibited*, as delineated in Article 5, and others are regarded as *high-risk* AI systems (HRAIS), as explained in Article 6 and following articles.

A third category includes systems considered *low risk but for which particular transparency* obligations exist (Article 50), and a fourth category are deemed *minimal or no risk AI systems*. General-purpose AI models (GPAI) are also regulated under Article 51 *et seq*. Finally, the AI Act intersects with various other pieces of legislation.

The AI Act is very important for particular biometric applications and their related research activities. We discuss this briefly below.

Biometric Data: A Distinct New Definition

Article 3 of the AI Act introduces several new definitions, including for “biometric data”, “AI system”, “providers”, and “deployers”, as well as for concepts such as “placing on the market", “putting into service”, and “the use” of such systems. These definitions are important for both developers and users of AI systems. As will be discussed, a few of these definitions and prohibitions have been further interpreted by the EU Commission in its *Guidelines* on prohibited artificial intelligence practices issued on 4 February 2025. [4]

It is noteworthy that the definition of biometric data found in Article 3(34) of the AI Act differs from the one used in the 2016 EU General Data Protection Regulation 679 (GDPR). Biometric data is defined in the AIA as “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data.” [5] This is contrary to the definition of biometric data in the GDPR, as the AI Act definition does not include the wording “which allow or confirm the unique identification,” two specific functional uses of biometric data.

This new definition was adopted for the regulation of specific AI systems, such as emotion and biometric AI categorization systems, as explained below. The GDPR definition of biometric data will apply under data protection rules with regard to the processing of personal data as an

additional layer. For example, when the AIA would not apply to biometric data processing, Articles 6, 9(1) and 9(2) of the GDPR would be applicable. [6-7]

Four New Prohibitions on AI Systems Related to Biometric Data

Article 5 of the AI Act mentions four new system prohibitions that explicitly involve biometric data. Three of these prohibitions also affect distributors, importers, and developers of AI systems if they place the system "on the market" or put it into service, whether for free or for a fee. Member states have the responsibility to adopt proper national laws governing various provisions, including any exceptions for law enforcement purposes to the prohibition on the use of real-time remote biometric identification in publicly accessible places.[8] It is important to note that even in cases where an AI system would not qualify for one of the specified prohibitions, such an AI system is likely to nevertheless fall into the category of high-risk AI systems for which very specific obligations apply.

As of August 2, 2025, violations of Article 5 of the AI Act will trigger significant fines. The four previously mentioned prohibitions are briefly analyzed below.

Identification or inference of emotions or intentions based on biometric data in the workplace or educational settings: AI systems analyzing physical traits, such as facial images, eyes and body movement, speech and voice, as well as "inner biometrics" like electroencephalography (EEG) and electrocardiograms, may identify or infer emotions or intentions.[9] The AI Act defines "emotion recognition systems" in Art. 3(39) of the AIA as "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data".

The AI Act prohibits placing into the market, putting into service for this specific purpose, and using *AI systems to identify or to infer emotions of a natural person in area(s) of workplace (and education)*, unless the exceptions for medical or safety reasons are applicable.

Biometric categorization AI systems for individually deducing or inferring "sensitive" information: Biometric technologies and their use are especially prone to various kinds of discrimination. This is because biometric information contains "sensitive" data about peoples' race, health, or age. Biometric technologies can also reveal which (public) places a person may frequent, or the type of events in which he or she may participate (e.g., attendance at political protests).

This type of sensitive data is inherent to the gathering of biometric data, and can lead to unjust and discriminatory uses of biometric applications and technology, including facilitating arrests. [10] For example, in a 2018 study Buolamwini and Gebru demonstrated that gender recognition works considerably less well for

darker skinned females, compared to white males, and pointed to the need to tackle gender and racial bias in AI systems. [11]

The AI Act now requires that AI systems shall not be used to infer from biometric data (for example, voice recognition data), "sensitive characteristics" that assign persons to specific categories, as this action reinforces discrimination. Article 5(1) (g) prohibits placing on the market, putting into service (for this specific purpose) or using biometric categorisation AI systems *that categorise individual* natural persons *based on their biometric data, when th*e purpose is to *deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation*.

The prohibition does not cover any labeling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data, or categorising biometric data *in the area of law enforcement*. The latter shall, at the same time, meet the requirements of the Directive EU 2016/680 about data processing by law enforcement authorities, and will likely be categorised as a high-risk AI system.

Even if all three cumulative conditions are fulfilled, an AI system *is not considered a biometric categorisation* if the biometric categorisation AI system is (i) just an additional aspect to another application; (ii) the application in question is a commercial product; ànd (iii) the biometric categorisation is strictly necessary for objective technical reasons. Examples of individually categorizing as an ancillary feature deemed strictly necessary includes filtering facial or bodily features used in marketplaces to preview a product, if the filter can only be used in relation to the principal commercial purpose. [12]

Untargeted scraping of facial images from Internet or CCTV footage to create or expand facial recognition databases: Article 5.1(d) of the AIA also explicitly bans the (unauthorized) untargeted harvesting (scraping) by AI systems of facial images from social media or surveillance cameras, such as CCTV footage, to create or enrich databases. This applies to both private and public entities, including law enforcement authorities. The imminent threat and risks of the use of such practices was exemplified by the licensing of the Clearview AI facial recognition technology by the US-based company Clearview AI to law enforcement entities throughout the EU for recognizing individuals, while not respecting the rule of law, along with the use of such images and further identifying information. Several data protection authorities, including those from the Netherlands, France, Greece and Italy have, after an investigation, imposed fines on Clearview AI.

Real-time Remote Biometric Identification in Publicly Accessible Places for Law Enforcement (RRBI PAS LE): The AI Act forbids *the use* of Real-time Remote Biometric Identification in Publicly Accessible Places for Law Enforcement (RRBI PAS LE). The concepts of a real-time remote biometric identification system and a post-remote biometric identification system are defined, but may still evoke discussions. [13}

There are three narrowly defined exceptions to RRBI PAS LE: a targeted search of victims or missing persons, a qualified threat to life or safety or of terrorist attacks, and localization or identification of a suspect or perpetrator of a specific serious crime for investigation, prosecution, or execution of penalty.

Member States, if they democratically decide to provide exceptions to the prohibitions in case of "open clauses" in the AI Act, such as for RRBI PAS LE, *shall establish "law"* providing for the need of *prior authorization* by a judicial authority or an independent administrative authority for each use of RRBI PAS LE, and notification to the authorities. The law shall also specify the legitimate aim *within the limits of the three exceptions* mentioned above that are set forth in the AI Act, and provide specific and sufficient *safeguards* for assessing and applying the *strict necessity* and *proportionality* criteria *within the boundaries set by the AI Act*.

Use of RRBI in a publicly accessible place by public or private entities other than for law enforcement is not banned by the AI Act. But, in principle, its use would fall in the high-risk category.

High Risk Biometric AI Systems

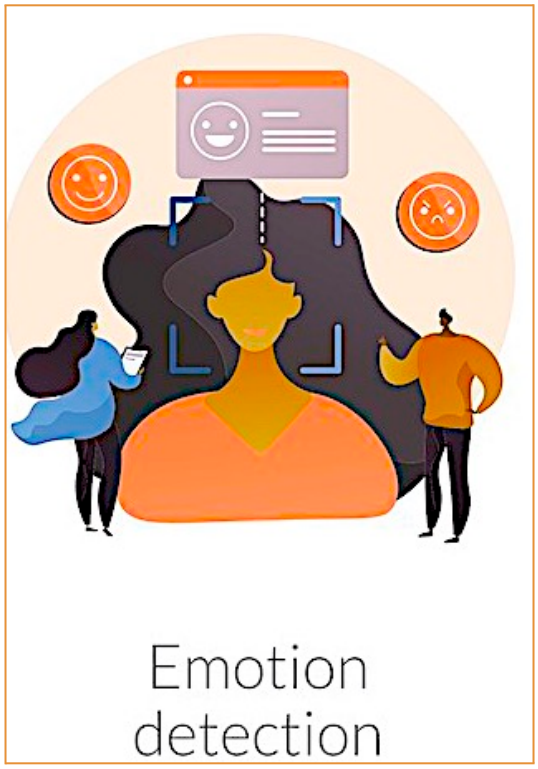
As mentioned, if an AI system would qualify as prohibited under Article 5, such systems are likely to fall in the category of high-risk (biometric) AI systems. For example, an AI system for identifying or inferring emotions which is *not* placed and used in the *workplace or for education*, will not fall under the Article 5 ban. But, if such an AI system is "intended for emotion recognition," it *will fall in the category of high-risk AI.* Article 6 of AIA states the conditions high-risk AI systems must fulfill, and also refers in paragraph 6.2 to Annex III, which lists AI systems considered to be high-risk (save the exceptions, as mentioned in para 6.3 AIA).

As a result, for any high-risk AI system, several new obligations will apply, including overall obligations like the need for an established, implemented, documented, and maintained continuous *risk management system*, *data governance*, *accuracy, robustness and cybersecurity*. Such systems also require making and maintaining *technical documentation*, *record keeping*, *transparency*, and *human oversight.* [14] There will also be obligations specific to providers and deployers, such as establishing *quality management and documentation systems*, automated *logging*, *corrective actions* and *information* duties, and *cooperative efforts* with the authorities. [15}

Many of these obligations are also very relevant to the activities undertaken during the research and development phase of AI systems. Other additional obligations specific to importers and distributors exist as well. These high-risk AI systems must also take into account the *European Declaration on Digital Rights and Principles for the Digital Decades*, and the *Ethics Guidelines for Trustworthy AI* of the

High-Level Expert Group on Artificial Intelligence [16].

For specific high-risk AI systems, including AI system safety components of critical infrastructures, and essential private and public services noted in Annex 5(b) and (c),



deployers shall also make *a fundamental rights impact assessment (FRIA)* according to specific requirements set out in Article 27. For example, if a city council installs remote biometric identification in publicly accessible places for public security, such systems threaten fundamental rights and freedoms essential to democratic societies. FRIA assessments shall complement any other impact assessment needed under general data protection legislation, such as the GDPR.

It shall be noted that *verification biometric systems* are to be distinguished from identification systems. Annex III of the AIA 1(a) states that, "AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be" shall *not* be considered high-risk. For such systems, GDPR shall remain the main text to comply with. [17]

Low Risk Biometric AI Systems Subject to Transparency Obligations

For biometric systems considered *low risk*, Article 50 of the AI Act sets *transparency obligations* that require information be presented "in a clear and distinguishable manner by, at the latest, the time of the first interaction or exposure," in conformity with the accessibility requirements. [18]

When deploying an (allowed) emotion recognition system, or a system that performs as a biometric categorisation system, any natural persons exposed to such a system *shall be informed* of the operation of the system.[19] In addition, in case of use by law enforcement, deployers of an AI system that generates or manipulates image, audio, or video content *constituting a deepfake,* shall *disclose* that the content has been artificially generated or manipulated. Article 50.2 further requires that providers of AI systems that generate *synthetic* audio, image, video or text content, including general-purpose AI systems, *mark the AI outputs in a machine-readable format,* and make them detectable as artificially generated or manipulated.

Addressing General-purpose AI Models with Systemic Risk

Under Article 51, general-purpose AI models may further qualify as being with "systemic risk" if they are evaluated as having high impact capabilities. Such an evaluation could be based on computation used for training that is higher than 10^{25}, or models that are qualified as such *ex officio* by the Commission based on criteria listed in Annex XIII. The additional obligations would include managing the related risks, monitoring serious incidents, performing model evaluations, adversarial testing, and cybersecurity obligations. These obligations could be implemented through codes of practice.[20]

Regulatory Sandboxes

The AI Act provides for the concept of "regulatory sandboxes" in which prospective AI providers can receive guidance from competent authorities on regulatory expectations and the requirements and obligations of the AI Act.[21] Hence, research and development activities can be tested under this framework with the new requirements of the AI Act.[22]

What does the AI Act and its Prohibitions Mean for Research and Development ?

The AI Act states that its provisions do not apply to systems or models—including the output of such systems—if they are "*specifically developed and put into service for the sole purpose of scientific research and development.*" [23] There is also an exception for systems used for "personal non-professional activity." Furthermore, the AI Act expressly states it will not apply "to any research, testing and development activity (…) prior to (…) being placed on the market or put into service (…)", while this does not apply to testing under real world conditions."[24]

AI technology, techniques, and systems are used for research and development, for example, to build databases, develop benchmarks or develop and/or fine-tune algorithms. But, they are also used to design and develop new AI systems to put on the market. So, what does this mean?

We explained in Part I of this tutorial, which was published in the December 2023 issue of this newsletter, that the use of biometric data for research purposes is subject to the GDPR. This is because biometric data, in principle, is personal data and, in principle, cannot be anonymized.

At the same time, the GDPR provides an explicit legal exception to the overall prohibition on the processing of sensitive data for research (Art. 9.2 (j) GDPR, if minimization and technical and organizational safeguards are applied).[25] [26] In our opinion, this exception should also be relevant to research and development leading to AI systems.

Furthermore, the AI Act is somewhat aligned in that it *also* provides for an exemption to AI systems and models *specifically developed and put into service solely for scientific activities,* as long as

such AI systems are solely used for scientific research and development, and not put on the market or in service.

The AI Act will affect researchers and developers involved in the making of *AI systems* that meet the criteria of article 3(1) of the AI Act, but are going to be used and/or placed on the market ("product-oriented research, testing and development activity"). It is sensible then that such research and development activities should duly take into account the many potential future obligations and user prohibitions should the system end up on the market.[27] For example, if deployers will need to meet obligations for record keeping, technical documentation, and providing information, preparing for this may well be taken into account during the development phase. These needs will be different than those of entities that are solely engaged in basic research, use in scientific fields, and/or in the scientific testing of AI systems with no specific real-world purpose or application sometimes conducted by universities (the so-called research privilege) [28] as these activities fall outside the scope of the AI Act.

Any liability under these regulations will generally not fall on the individual researchers or developers engaged under an employment contract, but instead will fall upon the company or establishment that employs them, unless national or contract law provides for individual liability, such as in cases of fraud, serious fault, repeated minor fault or intentional or willful misconduct by the researcher or developer.

Conclusion

The AI Act will have considerable impact on AI systems, including biometric AI systems. Therefore, an understanding of the new provisions, obligations, and compliance standards will be crucial prior to the design and the development of such systems. This approach applies to research and development activities as well, unless the AI systems are *specifically developed and put into service for solely scientific activities.* All other research and development activities for AI systems that will be used, placed on the market, and/or put into service should begin to take into account the obligations mandated by AIA during the research and development stages.

Parts of the AI Act have gone into effect already. The prohibitions and AI literacy requirements, that is the obligation of having skills, being able to understand, use, monitor, and critically reflect on AI use, have been mandatory since 2 February 2025. The AI Act further provides for governance, the monitoring of compliance, and enforcement through penalties. The latter can be considerable. For example, refusing to respect the prohibitions can result in fines up to €35 million, or 7% of a company's global annual turnover, whichever is higher. These penalties will go into effect as of August 2025.

Endnotes and References

1) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laid down

harmonised rules on artificial intelligence and amended Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), *OJ* L, 2024/1689, 12.7.2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

2) *AI Act*, Recitals 3, 5, and 7. Fundamental rights are the "red thread," especially with regard to biometric technologies. See also E.J. Kindt, "Biometric data processing: Is the legislator keeping up or just keeping up appearances ?" In G.G. Fuster, R. Van Brakel and P. De Hert (eds.), *Privacy and Data Protection Law: Values, Norms and Global Politics,* Chapter 18, Edward Elgar Publishing, Cheltenham, UK, and Massachusetts, USA, p. 389, 2022. An argument is made here for the use of a double framework of both GDPR and fundamental rights for assessing biometric data processing. And, E.J. Kindt, *Privacy and Data Protection Law: A Comparative Legal Analysis,* Springer, Dordrecht, pg. 570-571, 2013.

3) As defined in Article 3 (1) of the AI Act, an AI system is "a machine-based system that is designed to operate with varying levels of autonomy, may exhibit adaptiveness after deployment, and, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." By contrast, basic data processing activities that follow predefined, explicit instructions or operations "without learning, reasoning or modelling" at any stage of the system lifecycle, based on fixed human-programmed rules, without using AI techniques, or simple prediction systems, would not be considered AI systems under the AI Act. See also EU Commission, AI Office, C(2025) 924 final, 6.2.2025, p. 8. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application.

4) EU Commission, *Annex to the Communication to the Commission – Approval of the Content of the Draft Communication from the Commission – Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act), 4.2.2025, C(2025)* 884 final, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-

guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act. Note these Guidelines are currently only approved in draft.

5) *AI Act*, Art. 3(34).

6) For more background, see also C. Jasserand, *Guidance Study on Article 5(1)(h) Prohibition and its Three Exceptions (Article 5(1)(h)(i)-(iii)),* the procedural requirements laid down in *Article 5(2),* and the prohibition of *Article 5(1)(e) of the AI Act,* Study for the EU Commission per invitation to Tender, 2025; E. J. Kindt, *Study Concerning the Prohibitions of Article 5.1(c) (social scoring), Article 5.1(d) (predictive policing), Article 5.1(f) (emotion recognition), and Article 5.1(g) (biometric categorisation),* and the procedural requirements for the exceptions to the real-time remote biometric identification prohibition in Articles 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8 of the AI Act.

7) For the EU Commission per invitation to Tender EC-CNECT/2024/VLVP/0039 *Study on Guidance Art. 5 AI Act, multiple prohibitions,* 24 January 2025, to be published by the EU Publication Office, pp. 61-63.

8) For an overview of the timing of action by Member States under the AI Act, see *EU Artificial Intelligence Act*, Future of Life Institute, available at https://artificialintelligenceact.eu/responsibilities-of-member-states/

9) La Agencia Española de Protección de Datos (EDPS), *TechDispatch 1/2024 – Neurodata, 3.6.2024*, https://www.edps.europa.eu/system/files/2024-06/techdispatch_neurodata_en.pdfi. This technical report discusses the use of brain data and related technology, including the legal implications.

10) See also the widely cited 2019 study by the US National Institute of Standards and Technology (NIST) that established that the accuracy rates of facial recognition systems from well-known vendors contained biases based upon the sex, age and race, or country of birth of the subjects. The study showed false positive rates and biased outcomes often by factors of 10 to beyond 100 times, especially for African people and for women.

11) J. Buolamwini and T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proceedings of Machine Learning Research,* 81:1-5, 2018, 15 p.

12) See EU Commission, *Guidelines*, p. 92.

13) Hungary adopted amendments in March 2025 to criminalise LGBTQAI+ and to increase biometric surveillance at Pride events. See discussions in P. Haeck and C. Körömi, "Hungary on EU Watchlist

Over Surveillance at Pride," *Politico,* 25.4.2025.https://www.politico.eu/article/hungary-eu-watchlist-facial-recognition-surveillance-lgbtq-pride; Hungarian Civil Liberties Union, Civil Liberties Union for Europe, European Digital Rights, and the European Center for Non-Profit Law, "Hungary's New Biometric Surveillance Laws Violate the AI Act," *Blogpost*, 6.5.2025. https://edri.org/our-work/hungarys-new-biometric-surveillance-laws-violate-the-ai-act/.

14) *AI Act*, Chapter III, Articles 8 et seq.

15) *AI Act*, Chapter III, Articles 16 *et seq.*

16) Recital 7 AI Act.

17) For more about biometric verification under the *AI Act*, see B. Sumer, "The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?" in *EDPL,* pp. 150-161, 2024.

18) *AI Act*, Art. 50.4.

19) Any personal data obtained from these systems shall also be processed in accordance with EU Regulations 2016/679 and 2018/1725, and EU Directive 2016/680, as applicable. See Article 50.3 *AI Act.*

20) *AI Act,* Articles 55- 56.

21) *AI Act,* Article 57. Competent authorities are also prepared to provide such guidance pre-AI Act. See, for example, Datatilsynet, "*Securing Digital Identities. Biometric data and protected templates in eID solutions. Exit report from the "SALT" sandbox project with Mobai,"* https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/reports/salt-mobai-et-al.-exit-report-securing-digital-identities/.

22) *AI Act,* Article 2(8), and below.

23) *AI Act.* Article 2(6). See also *AI Act*, Recital 109.

24) *AI Act,* Article 2(8). Testing in real-world conditions is defined in *AI Act*, Article 3(57).

25) Such scientific research is understood as including both non-commercial (academic), as well as commercial research.

26) *GDPR*, Art. 89.

27) See also *AI Act*, Recital 25. Strictly speaking, the AIA obligations will not apply "prior to being placed on the market or put into service".

28) At the same time, internal guidelines on the use of AI will remain important for the responsible use and implementation of AI technologies in the research environment.