A. Brömme, C. Busch, N. Damer, A. Dantcheva, M. Gomez-Barrero, K. Raja,
C. Rathgeb, A. Sequeira and A. Uhl (Eds.): BIOSIG 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021

Will new definitions of emotion recognition and biometric data hamper the objectives of the proposed AI Act?

Jan Czarnocki[1]

Abstract: The paper explains how the definition of biometric data copied from the GDPR may hamper the regulation of emotion recognition—as defined in the proposed AI Act. A replicated definition of biometric data is suitable for biometric systems, but not emotion recognition technologies. It is because, under the proposed AI Act, an emotion recognition system is understood as such if it processes biometric data—as defined in the GDPR. But the definition from the GDPR does not encompass all biometric data, which are technically biometric data and are processed in the emotion recognition systems. Also, in the proposed AI Act the definition of emotion recognition does not recognize emotion recognition systems not relying on biometric data processing. That is why the obligation in the proposed AI Act for users to inform natural persons about their exposure to the emotion recognition system is unapplicable in the majority of cases. The flawed definition may also put at risk the proposed AI Act-based assessment of whether AI systems should be prohibited. Therefore, a new definition of emotion recognition and biometric data is needed.

Keywords: biometric data, emotion recognition, AI Act, AI, data protection, privacy, biometrics.

1 Introduction

The proposed Artificial Intelligence Act (AI Act) is the first legislative attempt to comprehensively regulate AI systems [Eu21]. Presented recently by the European Commission[2] it is an important part of building a new EU digital constitutionalism [Gr21]—a broad effort to address the challenges of digitalization. The goal of the proposed AI Act is i.a. to safeguard the trustworthiness of AI systems by ensuring their deployment is aligned with the values enshrined in the Charter of the Fundamental Rights of the EU [Eu20]. The proposal is the effect of an EU-wide effort and was preceded by the work of High Group on AI, which culminated in the White Paper on AI [Eu20]. Based on experience with enacting i.e. GDPR [Eu16] it will be some time until the implementation of the new regulation (it took GDPR 6 years from the first draft to come into force). Still, once enacted the AI Act will impact the fate of AI systems development in the EU for the next decades.

[1] Doctoral Researcher, KU Leuven Faculty of Law, Center for IT & IP Law, jan.czarnocki@kuleuven.be. This article has been made possible by received funding from the European Union's Horizon 2020 research and innovation programme in the context of the Privacy Matters Innovative Training Network (prima-itn.eu). I would like to thank prof. Els Kindt for her support and critical review.

[2] It was presented by the European Commission in April 2021. My paper relies on the first draft of the proposal, as presented therein.

The scope of the proposed AI Act encompasses AI applications such as machine learning, logical, statistical, and knowledge-based approaches [Eu21b]. It categorizes AI applications according to their purpose [Eu21c] and according to the risks posed to fundamental rights. The proposed AI Act prohibits or limits AI practices considered too risky, such as remote biometric identification or harmful manipulation of a natural person's behaviour [Eu21d]. The proposed AI Act introduces numerous compliance and due diligence requirements for high-risk AI systems [Eu21e].

One of the new requirements is the transparency obligation for emotion recognition systems using biometric data. Unless it is obvious from the context, users of AI emotion recognition systems are obliged to notify natural persons that they are interacting or are exposed to the workings of such a system [Eu21f]. This obligation can prove ineffective as it may be bypassed if left in its current form. It is due to a faulty definition of emotion recognition, which relies on the definition of biometric data from GDPR for AI applications to be classified as emotion recognition. Definition of biometric data replicated to the proposed AI Act is not suitable for AI systems—especially for emotion recognition, because it will leave most of the systems recognizing emotions out of the scope of the definition of emotion recognition.

2 Why regulate emotion recognition

Emotion recognition is an interdisciplinary research field, encompassing i.e psychology, cognitive science, and computer science. Its goal is to enable computers to understand human emotions and affects, to act accordingly [Pi03]. Emotion recognition is divided into fields of affective computing—mainly related to speech, video, and image processing and real-time analysis, and sentiment analysis—mainly related to longer-term opinions forming analysis, through natural language processing and describing what content is emotional [Pi03]. They are crucial fields to AI development [Mi06][3].

An example emotion recognition system could be embedded in an automated facial recognition system (AFRS), detecting face, extracting needed features, and classifying a natural person according to his or her gender, age, and six basic facial emotions: anger, happiness, fear, surprise, disgust, and sadness [LTL16]. However, emotion recognition can also range to uses of non-obvious types of data, such as stemming from i.e. measuring galvanic skin response (measurement of skin sweat to infer emotional arousal), electrocardiograms (cardiac cycle measurement), electroencephalograms (brain waves activity measurement), electromyograms (electrical measurement of skeletal muscles activity), or measurement of respiration, and skin temperature [UDRS17].

[3] These approaches assume that a key to embedding the machine with human intelligence is the capacity of a machine to understand human emotions and affects. Therefore, this approach teaches machines how to recognize emotions and then adjust actions accordingly. Through analysis of face scans, speech samples, or written excerpts engineers teach AI systems to recognize in what emotional state the natural person is, and what physical traits and behavior are related to what emotion.

Exposure to emotion recognition systems poses numerous risks to privacy and data protection, by revealing what an individual may not want to disclose. Emotions can be added to profiles, putting privacy and data protection at risk. The ability to recognize emotions can give data processors and controllers precise and accurate information about the state of mind of a person, disclosing sensitive knowledge about him or her [Ko21]. It is through emotion recognition systems that numerous predatory practices online are possible, such as profiling [GH08] and nudging [ST09], including using dark patterns to monetize emotions [Cl19]. These practices are the backbone of data power, surveillance capitalism, and attention economy [Zu19]—the dark sides of the digital world.

Emotion recognition systems can be an important part of AI systems, which systems use is prohibited or limited in the new regulation. Judging the impact of an AI system on fundamental rights might be determined by whether the system is capable of recognizing emotion. For example one of the prohibited AI practices in Article 5 is a subliminal, harmful, material distortion of a natural person's behavior [Eu21h]. The capability to recognize emotions and affect is crucial for some AI systems to capacitate such harm. Therefore, a proper legal definition determining what counts as an emotion recognition system is of crucial importance for protecting natural persons. Also, the effectiveness of the obligation to inform the natural person about their exposure to an emotion recognition system depends on how the emotion recognition system is defined.

3 Inheriting the wrong definition of biometric data

According to the proposed AI Act an emotion recognition system is "*AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data"* [Eu21i]. Using conjunction the definition determines that only systems that recognize emotions based on biometric data are emotion recognition systems. However, what is understood from a technical point of view as biometric data, is not always what is understood as biometric data from the legal point of view [Ja15]. The definition of biometric data in the proposed AI Act is duplicated from GDPR [Eu16a][4]. It is a functional definition—affordances of the technology used to process the data define the legal nature of the data [Ki18]. It assumes that personal data becomes biometric data once processed through the system, which allows or confirms unique identification. Otherwise, personal data is not biometric data—it does not enjoy a higher level of protection reserved for the category of sensitive data [Ki18]. The threshold for falling under the definition of biometric data is whether biometric data results from specific, technical processing which allows identifying a natural person. Therefore, unless personal data is processed through technical means that enable to recognize the identity of an individual it is not construed as biometric data. For example, unless scanned through a facial recognition system, or other biometric system for the purpose of "unique

[4] where it is defined as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"*

identification", a photo or video with a natural person's image is not considered biometric data [Eu16b]. As pointed out by Kindt and Jasserand there is a misalignment between technological affordances and legal definition [Eu16b, Ja15]. The current definition of biometric data fails to properly delineate the scope of what must be considered biometric data. It limits the understanding of what is biometric data from a legal perspective [Ki18]. Therefore, this definition leaves numerous data, which technically is biometric data, outside of the scope of higher protection, granted to biometric data by GDPR.

Therefore, since the proposed AI Act replicates the same definition of biometric data, unless an emotion recognition system processes such narrowly understood biometric data and unless it is a biometric system capable to recognize the identity, it is not considered an emotion recognition system. Thus, unless it uses biometric data specifically for purpose of "unique identification" it is not an emotion recognition system. This leaves most of the AI systems capable of recognizing emotion outside of the scope of the definition. Most of them neither process biometric data—as narrowly understood under the definition in the proposed AI Act, or are biometric systems—capable of recognizing the identity or verifying it [KRBDJ18].

The proposed definition of emotion recognition misses its intended object because according to the GDPR and the proposed AI Act's definition [Eu16a] biometric data only becomes biometric data if it is processed through technical means allowing for uniquely identifying a natural person—biometric systems. They are systems for *"automated recognition of individuals based on their biological and behavioural characteristics"* [IS17]. Biometric recognition can form a part of the emotion recognition system but is not a necessary component—it is not essential to identify or verify a natural person's identity, to recognize his or her emotions. The old definition of biometric data is well suited for biometric systems [IS17], but not for other affective computing and sentiment analysis technologies.

For instance, most AFRSs detect emotion, attention, and different states using face modeling, extracting only the features needed, and then compressing them. A particular psychological state or sociodemographic characteristic is recognized through comparison with a dataset of such modeled images using an artificial neural network [LTL16]. Therefore, biometric data as legally defined are not processed, because identification of a natural person is not possible in this case. In one example, the emotions of gamers were measured and analyzed in an experiment, through EEG (electroencephalography – measurement of electrical activity on the scalp, representing the macroscopic activity of the surface layer of the brain) and using machine learning. The system was able to recognize the valence of gamer's emotions like anger, anticipation, joy, trust, fear, surprise, sadness, and disgust [BGT20]. However, the system was not able to tell anything about the gamer's identity, because that was not its purpose. According to the current regulation it would not be branded as an emotion recognition system, because personal data processed through it do not fall under the definition of biometric data. Similarly, mobile applications for emotion recognition can extract facial representations from images or videos. Then face detection module is applied to extract frames of face regions and then

compare them to the model based on training data set containing other faces [HM17]. In this way, emotion can be detected without the need for an AI system to be a biometric system, able to "uniquely identify" a natural person [LTL16].

Emotion recognition system can extract particular features from either video, image (e.g. like muscle movement, wrinkles, or other key facial regions [FM13]), or speech record (e.g. particular qualities of voice), which allows it to recognize and classify emotion, without the need to extract an entire biometric template [VChK15]. According to the current definition only when a biometric template is extracted, the system is processing biometric data. But other methods of emotion recognition can be used, such as through e.g. measurement of galvanic skin response, electrocardiogram, electroencephalogram (brain waves), electromyogram, or respiration, and skin temperature—without processing of legally understood biometric data [UDRS17]. In consequence emotion recognition systems do not have to be able to "uniquely identify" to recognize or infer emotions. Thus, under the GDPR definition, they will not be processing biometric data. However, technically speaking it will be biometric data. Therefore, due to its dependence on narrowly understood biometric data the definition of an emotion recognition system in the proposed AI Act will be ineffective and will consider most emotion recognition systems as outside its scope. This may also hamper the due diligence and compliance process for assessing the impact of an AI system on fundamental rights and whether it can enter the Single Market.

4 The need for new definitions

For the definition in the proposed AI Act to effectively encompass all biometric data, it would require recognition of not only the personal data processed through a biometric system but of data directly relating to biometric characteristics of a person, which is a view proposed by Kindt [Ki13][5]. In her definition condition for data to be biometric data is its relation to certain traits of natural persons, not the fact of being processed through specific technical means—the condition present in deficient definition in the proposed AI Act, repeated after the GDPR.

Perhaps the intention behind what is classified as biometric data in the current definition of emotion recognition is what would have been if Kindt's definition were applied. But the proposed AI Act takes the definition of biometric data from the GDPR. And this understanding of biometric data effectively erases the potential effectiveness of the definition of "emotion recognition system" in the proposed AI Act. Hence, due to deficiencies in the definition from the GDPR, the original sin of the bad definition of biometric data was replicated to the proposed AI Act. As a consequence, if the definition

[5] Under definition proposed by her biometric data are *"all personal data which (a) relate directly or indirectly to unique or distinctive biological or behavioral characteristics of human beings and (b) are used or are fit to be used by automated means (c) for purposes of identification, identity verification or verification of a claim of living natural persons."*.

of the emotion recognition system in the proposed AI Act is deficient—dependent on the definition of biometric data, then the majority of the AI systems recognizing emotions may fall outside of the scope of transparency and notification obligations therein. Thus, natural persons will not have to be notified if they are exposed to most emotion recognition systems. Moreover, if certain AI systems are not recognized as emotion recognition technologies under the current definition, then there is a risk of numerous harmful AI systems squeezing through the AI Regulation regime and entering the Single Market. It is because during assessment whether they pose risk to fundamental rights their capacity or property of being categorized as emotion recognition systems may be taken into consideration. Under the definition of emotion recognition systems from the proposed AI Act, many of them may fall outside of its scope—even though they are capable of recognizing emotion.

Therefore, we either need a new definition of emotion recognition or a new definition of biometric data. The first option is still feasible because work on the AI Act has just started. It will require a small amendment during the legislative process. However, in the long term, there is a need to also amend the definition of biometric data—both in the future AI Act and the GDPR. It will be more complicated because even if the definition of biometric data is changed in the AI Act—for example in a way suggested by Kindt, it will leave a faulty definition of biometric data still present in the GDPR. This would carry the risk of jeopardizing the legal system and sowing confusion. Hence, from a pragmatic point of view objectives of the proposed AI Act concerning emotion recognition can be saved by upgrading the definition of the emotion recognition system. The definition should not encompass biometric data and should not be dependent on it. It should be neutral as to the methods used for recognizing or inferring emotions. It should refer to the capacity to recognize or infer emotion or affects, without specifying how it is done. Thus, the definition should focus on the purpose and effect of the AI system. Each AI system capable of inferring or recognizing emotions should be treated as such. Focusing on the effects of the AI system will render the definition more robust and resilient to technological changes.

That is why, instead of defining an emotion recognition systems as an "*AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data"* it suffices to define them as AI systems to identify or infer emotions, affects or intentions of natural persons.

References

[BGT20] Burak Alakus T.; Gonen M.; Turkoglu I.: Database for an emotion recognition system based on EEG signals and various computer games – GAMEEMO, Biomedical Signal Processing and Control, Volume 60, 2020.

[Cl19] Clifford, D.: The Legal Limits to the Monetisation of Online Emotions, KU Leuven, Faculteit Rechtsgelerdheid, Leuven, 2019.

[Eu16] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).

[Eu16a] Article 4(14) GDPR.

[Eu16b] Recital 51 GDPR, Article 4(14).

[Eu20] European Commission, White Paper On Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.2.2020

[Eu21] European Commission, 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, Brussels, 21.4.2021 COM(2021) 206 final.

[Eu21b] Annex I to the 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, Brussels, 21.4.2021 COM(2021) 206 final.

[Eu21c] Annex III to the 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, Brussels, 21.4.2021 COM(2021) 206 final.

[Eu21d] Article 5, Artificial Intelligence Act.

[Eu21e] Article 52.1, Artificial Intelligence Act.

[Eu21f] Article 52.2, Artificial Intelligence Act.

[Eu21g] Article 5.1(a) Artificial Intelligence Act.

[Eu21h] Recital 7 “The notion of biometric data used in this Regulation is in line with and should be interpreted consistently with the notion of biometric data as defined in Article 4(14) of Regulation (EU) 2016/679 of the European Parliament and of the Council”.

[Eu21i] Article 3(34) Artificial Intelligence Act.

[FM13] Filko D.; Martinović G.: Emotion Recognition System by a Neural Network Based Facial Expression Analysis, Automatika, 54:2, 263-272, 2013.

[GH08] Gutwirth, S.; Hildebrandt, M.: Profiling the European Citizen: Cross-disciplinary Perspectives. 1ed, Springer, New York, 2008.

[Gr21] De Gregorio, G.: The Rise of Digital Constitutionalism in the European Union., International Journal of Constitutional Law 19.1, 41-70, 2021.

[HM17] Hossain M. S.; and Muhammad G.: An Emotion Recognition System for Mobile Applications, in IEEE Access, vol. 5, pp. 2281-2287, 2017.

[IS17] ISO/IEC 2382-37, Information technology, Vocabulary, Part 37:Biometrics, 2017.

[Ja15] Jasserand, C. A.: Avoiding Terminological Confusion between the Notions of 'biometrics' and 'biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective, International Data Privacy Law 6.1, 2015.

[Ki13] Kindt, E.: Privacy and Data Protection Issues of Biometric Applications - A Comparative Legal Analysis, Springer, 2013.

[Ki18] Kindt, E.: Having yes, using no? About the new legal regime for biometric data, Computer Law & Security Review, Volume 34, Issue 3, Pages 523-538, 2018.

[Ko21] Kosinski, M.: Facial recognition technology can expose political orientation from naturalistic facial images, Sci Rep 11, 100, 2021.

[KRBD18] Kartali, A.; Roglic, M.; Barjaktarovic, M.; Duric-Jovicic, M.; and Jankovic, M. M.: Real-time Algorithms for Facial Emotion Recognition: A Comparison of Different Approaches, 14th Symposium on Neural Networks and Applications (NEUREL): 1-4, 2018.

[LTL16] Lewinski, P.; Trzaskowski, J.; and Luzak, J.: Face and Emotion Recognition on Commercial Property under EU Data Protection Law, Psychology & Marketing 33.9: 729-46. 2016.

[Mi06] Minsky, M.: The emotion machine: Commonsense thinking, artificial intelligence, and the future of the human mind, Simon & Schuster, New York, 2006.

[Pi03] Picard, R. W.: Affective Computing: Challenges. International Journal of Human-computer Studies 59.1: 55-64, 2003.

[ST09] Sunstein, C. R.; Thaler, R. H.; Nudge: Improving Decisions on Health, Wealth, and Happiness, Penguin, London, 2009.

[UDRS17] Udovičić, G.; Đerek, J.; Russo, M.; and Sikora M.: Wearable Emotion Recognition System based on GSR and PPG Signals, In Proceedings of the 2nd International Workshop on Multimedia for Personal Health and Health Care (MMHealth '17), Association for Computing Machinery, New York, NY, USA, 53–59, 2017.

[VChK15] Varghese A. A.; Cherian J. P.; and Kizhakkethottam J.J.: Overview on emotion recognition system, 2015 International Conference on Soft-Computing and Networks Security (ICSNS), pp. 1-5, 2015.

[Zu19] Zuboff, S.: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power., First ed., PublicAffairs, New York, 2019.