Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement

From the AI Regulation Proposed by the Commission to the EU Co-Legislators' Positions

Vagelis Papakonstantinou, Evangelos Zarkadoulas

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

In April 2021, the European Commission put forward a proposal for a Regulation to harmonise rules on artificial intelligence (AI) across the EU, including AI in the context of law enforcement. Its horizontal character raised concerns in the police community, prompting a response by some Member States arguing for a separate legal act on the use of AI by law enforcement agencies. Two controversial components that have drawn the attention of the Council of the EU and the European Parliament are remote biometric identification and emotion recognition technologies. While the Council's general approach aligns with the Commission's proposal to balance law enforcement and human rights protection, the European Parliament pursues a narrower approach, advocating for the prohibition of real-time remote biometric recognition and emotion inference applications. It goes without saying that the outcome of the ongoing inter-institutional negotiations (trilogue) between the EU co-legislators and the Commission is being anticipated by law enforcement bodies with considerable interest. After all, this will define how the opportunities provided by AI are leveraged in law enforcement settings as well as how to deal with the misuse of this evolving technology by terrorists and criminals. This article reports on the institutions' positions on remote biometric identification and emotion recognition and highlights the – in the authors' view – flawed approach by the European Parliament toward law enforcement.

AUTHORS

Vagelis Papakonstantinou
Professor on Personal Data Protection Law
Vrije Universiteit Brussels (VUB)

Evangelos Zarkadoulas
Ph.D. Law Student
Vrije Universiteit Brussels (VUB)

CITE THIS ARTICLE

Papakonstantinou, V., & Zarkadoulas, E. (2023). Remote Biometric Identification and Emotion Recognition in the Context of Law Enforcement : From the AI Regulation Proposed by the Commission to the EU Co-Legislators' Positions. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2023-021

Published in eucrim 2023, Vol. 18(2) pp 237 – 240
https://eucrim.eu
ISSN:

CC BY ND

I. Introduction

Recently, artificial intelligence (AI) has been a top-agenda item worldwide. Rapid and ongoing technological advances in AI have triggered legislative initiatives to regulate its use in Europe. In April 2021, the European Commission tabled a proposal for a Regulation laying down harmonised rules on artificial intelligence across the EU.[1] It is based on Art. 114 of the Treaty on the Functioning of the European Union (TFEU), conferring upon the EU competence for the single market, in conjunction with Art. 16 TFEU, providing for legislation on the protection of individuals in the context of the processing of their data. Consequently, this proposal is a horizontal legislative act addressing the function of the internal market whilst also covering the field of law enforcement. A key feature of this proposal is that the Commission has adopted a risk-based approach for classifying AI applications into four categories: prohibited practices, high risk with robust requirements, medium-low risk with transparency obligations, and minimal-no risk without rules.[2]

Law enforcement has been mainly classified under high-risk systems. This decision by the Commission raised concerns in the police community. At the Justice and Home Affairs Council in June 2021, some Member States suggested that a separate legal text on the use of AI by law enforcement authorities be adopted.[3] Their arguments related to the special nature of the police sector and the method followed in setting up the EU personal data protection framework consisting of the General Data Protection Regulation (GDPR) and the Directive 2016/680 (the Law Enforcement Directive). Undoubtedly, the monopoly on legitimate violence distinguishes law enforcement authorities from the remainder of public administration, as the former are responsible for public security and contribute to national security in the field of counter terrorism. What is more, discipline and implementation of criminal law are fundamental elements of the police remit. However, due to the limited support by other Member State delegations in the Council, the Commission's proposal was ultimately backed in its original wording.

The following sections provide an overview of the institutions' positions on remote biometric identification and emotion recognition tools. First and foremost, the article presents the relevant provisions of the Commission's proposal (Section II.). Subsequently, Sections III. and IV. outline the opinions of the Council of the EU and the European Parliament, and how these differ. In conclusion, the article highlights how the Commission and the Council have been able to strike a balance between law enforcement needs and fundamental rights – unlike the European Parliament, which has adopted a problematic angle when it comes to law enforcement.

II. Remote Biometric Identification and Emotion Recognition AI Systems in the Commission Proposal

Two of the Regulation's components that have attracted significant attention during the discussions in the European Parliament and the Council are remote biometric identification and emotion recognition. The Commission has proposed categorising real-time remote biometric identification in public spaces for law enforcement purposes as a prohibited practice unless substantive and procedural prerequisites apply (Art. 5 of the proposal). With regard to these substantive requirements, the Commission has proposed that the use of this technology must pursue one of the following objectives: a) search for potential crime victims, for example, missing minors; b) prevention of threats to the life and physical safety of individuals or a terrorist incident; or c) detection, identification, or prosecution of a perpetrator or a suspect of a criminal offence referred to in Art. 2(2) Council Framework Decision on the European Arrest Warrant, and punishable with at least three years of a custodial sentence or a detention order under the rules of the Member State con-

https://doi.org/10.30709/eucrim-2023-021

cerned. In terms of national procedures, prior authorisation by a judicial or an independent administrative authority is deemed necessary. Nevertheless, the proposal also provides for such authorisation being sought during an operation or ex-post in case of emergency.

Notwithstanding that Art. 5 of the Commission proposal allows real-time at a distance biometric recognition, Annex III defines it as a high-risk AI tool, and the conditions set out for high-risk AI applications must be met. In particular, these requirements include a risk management system, data governance, technical documentation, record-keeping, transparency, human oversight and accuracy, robustness, and cybersecurity (Arts. 8-15 of the proposal).

Annex III also classifies post biometric identification and emotional inference for law enforcement as high-risk. Consequently, this means that law enforcement will need to adhere to the requirements listed above if it intends to harness these tools.

In contrast, the Commission proposal sees the private sector exploiting these technologies more flexibly. It is noteworthy in this context that Art. 5 of the Commission proposal stipulates no requirements for real-time biometric identification in the non-public sector, while Art. 52(2) defines that emotion detection is considered a medium-low risk application with only transparency obligations.[4] This raises the question of why the Commission appears to trust private companies more than law enforcement authorities.

Moreover, when the College of Commissioners approved the legislative proposal on AI, the European Data Protection Supervisor (EDPS) asked for a moratorium on implementing remote biometric identification.[5] In particular, the EDPS – in collaboration with the European Data Protection Board (EDPB) – recommended a ban on the automated recognition of human biometric features in publicly accessible spaces through a joint opinion circulated in June 2021.[6] Despite these recommendations by the EDPS and the EDPB, the Commission has not amended its view, insisting on its initial proposal.

III. The Council's General Approach

Following long internal consultations by the Member State delegations in the Working Party on Telecommunications and Information Society, the Member States endorsed their common position at the Transport, Telecommunications, and Energy Council in December 2022.[7] In view of the remarkable margin of action granted to the private sector when implementing remote biometric identification and emotion recognition in the Commission proposal (see Section II.), the Council has proposed revising the definition of law enforcement in Art. 3(41) and added all other entities that operate on behalf of law enforcement authorities. As for real-time remote biometric identification and emotion recognition, this addition has been incorporated in Art. 5, par. 1(d) and Annex III, par. 6(b) respectively. As a consequence, these entities must respect the requirements stipulated by both Art. 5 on real-time biometric identification and Art. 8–15 on high-risk systems for both technologies.

Considering the definition of law enforcement authority as provided for in Art. 3(40)(b) of the Commission proposal, the objective of this addendum is to include non-state actors not authorised by Member State legislation to perform law enforcement duties. Moreover, the Council has amended the scope of biometric identification by extending it to other offences apart from those listed in Art. 2(2) of the Framework Decision on the European Arrest Warrant, i.e. to include offences punishable by at least five years, as determined by national criminal law.

In relation to emotion recognition, the Council has clarified that affected individuals should not be informed in case of detection, prevention, and investigation of crime, thus defining more exceptions to the transparency obligation as proposed by the Commission in Art. 52 of the proposal. The reason for this amendment is

https://doi.org/10.30709/eucrim-2023-021

that a person involved in a criminal activity may attempt to evade justice or adapt his or her behaviour when informed of being subject to emotion recognition, and thus render this technology ineffective. Likewise, EU and national criminal legislation stipulate criteria under which a suspect or a defendant needs to be informed of actions performed by the police and judicial authorities in order not to jeopardise an ongoing investigation.

IV. The Parliamentary Position

Following the Council's general approach, the report on the AI Act was approved by the EP's Committees on Internal Market and Consumer Protection (IMCO) and on Civil Liberties, Justice and Home Affairs (LIBE) in May 2023,[8] before the EP's plenary adopted the position in June 2023.[9] From the Parliament's perspective, real-time and post remote biometric identification of natural persons, as well as emotional inference, are to be considered prohibited practices. In particular, real-time remote biometric recognition and emotion detection would be banned, even in the context of combating crime.

Yet, retrospective biometric identification is held permissible for law enforcement if the following prerequisites apply: a) *ex-ante* permission by a judicial authority; b) targeted search; and c) link with the investigation of committed serious crimes listed in Art. 83(1)TFEU (terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime).

Nonetheless, the proposed requirement of prior judicial authorisation for post-event biometric recognition applications might have an adverse effect on arresting criminals. Time is a critical factor in criminal investigations in progress, and the obligation to seek judicial permission could, for instance, enable a perpetrator to escape or obstruct the prevention of a terrorist attack or an offence against life.

V. Conclusion

When it comes to the use of remote biometric identification and emotional inference systems in law enforcement, the Council largely agrees with the Commission's AI Act proposal. Its position does not meaningfully deviate from the Commission's proposal aimed at reconciling law enforcement and human rights protection. On one hand, police authorities are to be enabled to better leverage technology to tackle terrorists and criminals who exploit state-of-the-art technology without running into legal restrictions; on the other hand, the principle of proportionality and fundamental rights are to be respected. As a result, both institutions render real-time remote biometric recognition admissible by stipulating substantive and procedural criteria under which law enforcement bodies need to comply.

In contrast, the European Parliament's position reveals a stricter approach, considerably restricting the implementation of AI by the police. From an operational perspective, a major impact of this stance would be the prohibition of AI biometric systems to prevent terrorism and crime. Law enforcement agencies would not be able to use remote biometric identification and emotion recognition to deter terrorist attacks and crimes, ensuring public security, and protecting individuals from victimisation. One additional consequence would be the inability of the police to apply remote biometric identification to detect missing persons and, notably, minors. As regards post remote biometric identification of natural persons, which is a long-standing successful forensic tool, prior judicial authorisation as proposed by the EP will likely harm the swift analysis of recorded footage and – ultimately – the effectiveness of criminal investigations.

Inevitably, the ongoing inter-institutional negotiations (trilogue) between the EP and the Council as EU co-legislators and the Commission are complicated, and a compromise agreement will be hard to achieve. In

https://doi.org/10.30709/eucrim-2023-021

any case, law enforcement authorities expect the outcome of the negotiations with great interest because this will define how the opportunities offered by AI can be leveraged as well as how to tackle the misuse of this emerging technology by criminals.

1. 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", COM(2021) 206 final.↩
2. European Commission, Press Release, "Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence", <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682> All internet links referred to in this article were last accessed on 5 October 2023.↩
3. One of the authors (Evangelos Zarkadoulas) personally attended this Council meeting; for the main results, see Council of the EU, Justice and Home Affairs Council, 7–8 June 2021, <https://www.consilium.europa.eu/en/meetings/jha/2021/06/07-08/>.↩
4. Apart from emotion recognition, this provision governs the biometric categorisation systems, which aim to classify natural persons into specific categories, and not to identify them in the way biometric identification tools do.↩
5. EDPS, Press Release, "Artificial Intelligence Act: a welcomed initiative, but a ban on remote biometric identification in public space is necessary", <"https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en>.↩
6. EDPB-EDPS, "Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)", <<https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf>.↩
7. Council of the EU, Transport, Telecommunications and Energy Council (Telecommunications), 6 December 2022, Main results, <https://www.consilium.europa.eu/en/meetings/tte/2022/12/06/>.↩
8. European Parliament, Press Release, "AI Act: a step closer to first rules on Artificial Intelligence", <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence >.↩
9. European Parliament, Press Release, "MEPs ready to negotiate first-ever rules for safe and transparent AI", <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>.↩

COPYRIGHT/DISCLAIMER
© 2023 The Author(s). Published by the Max Planck Institute for the Study of Crime, Security and Law. This is an open access article published under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0) licence. This permits users to share (copy and redistribute) the material in any medium or format for any purpose, even commercially, provided that appropriate credit is given, a link to the license is provided, and changes are indicated. If users remix, transform, or build upon the material, they may not distribute the modified material. For details, see https://creativecommons.org/licenses/by-nd/4.0/.
Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union