

TILBURG INSTITUTE FOR LAW, TECHNOLOGY, AND SOCIETY TILBURG UNIVERSITY

## Tilburg Institute for Law, Technology, and Society's contribution to the public consultation on the Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

- Tilburg Institute for Law, Technology, and Society (TILT) is one of the leading research groups in Europe at the intersection of law, technology, and society. Our research efforts are aimed at, among others, understanding the interaction of technology and social and normative practices in order to clarify how regulatory challenges of sociotechnical change can be addressed.
- 2. The increasing use of facial recognition technology by law enforcement authorities raises significant challenges due to its potential infringing effects on fundamental rights and freedoms of individuals and its chilling effects on society in general.
- 3. However, under the existing frameworks, both at the Union and Member State level, certain aspects of this technology are still unexplored, not sufficiently addressed, disputed, or fragmented. This creates a fundamental challenge to mitigate the risks that such use poses, especially regarding the right to data protection of individuals.
- 4. Therefore, TILT welcomes these very timely guidelines produced by the European Data Protection Board and believes that they will not serve as guidance not only for law enforcement authorities but also to designers and producers of such technologies, procurers, regulators, and people who are subjected to these technologies in general.
- 5. We also appreciate the opportunity of the public consultation and would like to hereby submit our comments to the draft guidelines.
- 6. To that end, we first introduce some general comments on the draft guidelines deriving from our first observations on the subject matter and how the European Data Protection Board formulated it. Then, we provide further comments specifically addressing the explanations and interpretations made under the draft guidelines.

## A. General Comments

- 7. Although we understand that addressing such issues might fall beyond the scope of the European Data Protection Board's mandate, we believe some important aspects are missing from the scope of the draft guidelines.
  - 7.1. The first aspect could be identified as the mismatch, or non-alignment, between the two main legal frameworks that regulate law enforcement activities in the Member States, namely the Codes of Criminal Procedure and data protection laws. While the latter regulate the processing of personal data and should be understood in general as covering the regulatory efforts directed to implementing the Law Enforcement Directive, the former regulate collecting personal data through various investigation powers. Although collection as such also constitutes a form of processing, we believe that making such a differentiation holds crucial importance since the collection is primarily regulated through the investigation powers, which set clear and precise conditions for when law enforcement authorities can gather certain types of (personal) data. Therefore, we would like to underline the importance of having a holistic approach by also considering



**Understanding Society** 

the conditions enshrined in the Codes of Criminal Procedure on which law enforcement authorities may gather, for example, biometric data and photographs.

- 7.2. The second aspect is attached to the risk of "identification laundering", which refers to cases in which law enforcement authorities unlawfully use facial recognition technology to find out a person's identity by, for example, uploading a photograph of an unidentified suspect to a private database located in the United States, and then reverse engineer the identity from information sources that law enforcement authorities have collected lawfully, for example by showing the photograph of the unidentified suspect to someone in his vicinity who spontaneously recognize the person. In such cases, as long as law enforcement officers do not mention the initial use of the facial recognition technology, the person in question does not have the chance to contest such practice in the subsequent criminal proceedings. Although such use by law enforcement would be unlawful, there is still a chance for such practices to occur especially in serious cases with high societal impact. Hence, we believe the draft guidelines should also consider including such scenarios in its scope.
- 7.3. Another concern is that the draft guidelines pay little or no attention to enforcement and oversight. In specific, the draft guidelines fall short of answering the question of whether the current oversight procedures for law enforcement, which are spread across the judiciary, data protection authorities, and in some instances, special supervisory authorities, are sufficient to deal with the risk of abuse of the facial recognition technologies by law enforcement authorities.
- 7.4. Furthermore, it is with regret that we see that the draft guidelines have a traditional point of view regarding the technology, since it misses the chance to address some of the novel applications such as body-worn cameras that are increasingly being used in practice. Given the particular risks attached to these novel uses that differentiate them from the traditional facial recognition technologies, we believe that they should also be included in the scope of the draft guidelines.
- 7.5. Lastly, although we understand that the draft guidelines are directed to tackle the use of facial recognition technologies by law enforcement, we believe that including the other related types of use into the scope of the draft guidelines, such as the use of facial recognition technologies by individuals to identify police officers in order to, for instance, name and shame them on social media due to discontent with the police activity, or the use of facial recognition as a security or management tool for law enforcement authorities and the judiciary to, for instance, monitor police officers, would also help to provide a holistic review of the topic at hand.

## B. Specific Comments

- 8. Although there are some references to it (§ 16, for instance), the draft guidelines seem to overlook the "categorization" function of the facial recognition technology while defining its functions under Chapter 2.<sup>1</sup> While categorization might not always allow for immediate identification of individuals, this practice might lead to *de facto* identification when combined with auxiliary information from additional data points. In addition to that, considering that novel use cases such as emotion recognition also benefit from this function, we believe it is important to include this function also under the scope of the draft guidelines.
- 9. As correctly highlighted in the draft guidelines under Chapter 2.3., bias and error are serious threats to the reliability of facial recognition technologies. Indeed, various studies have already proven that law enforcement officers tend to ignore such limitations or have "automation bias". These might lead to severe infringements of the key principles in criminal procedure law, such as due process and presumption of innocence. Therefore, the European Data Protection Board should introduce a specific relevance to the presumption of innocence and to

<sup>&</sup>lt;sup>1</sup> See further on this Article 29 Data Protection Working Party (2012), Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, 22 March 2012, p. 2; European Union Agency for Fundamental Rights (2019), Facial recognition technology: fundamental rights considerations in the context of law enforcement, 27 November 2019, p. 7.



Understanding Society

other key principles where relevant, both in relation to the risks generated by the use of facial recognition technologies by law enforcement but also a reference to the Articles 47 and 48 Charter of Fundamental Rights of the European Union under Chapter 3.1.

- 10. Where relevant under Chapter 3.1. of the draft guidelines, it should be stressed that the essence of the fundamental rights under the Charter of Fundamental Rights of the European Union constitutes an inviolable core.
- 11. We believe a different formulation of §74 would bring further clarity and emphasis to the issue. Such reformulation could appear as: "Therefore, biometric data that can be retrieved from a photograph by specific technical means, have not been made manifestly public (e.g., by the manifest publication of the photograph by the data subject), unless the photograph or the related biometric data have been explicitly made public **as** biometric data."
- 12. Furthermore, Chapter 3.2.1.3. could benefit from more real-life examples, especially those related to open-source intelligence.
- 13. The draft guidelines do not provide sufficient explanation under Chapter 3.2.5, especially under the Data Protection Impact Assessment and Data Protection by Design and by Default sections. We consider these obligations as playing a crucial role in protecting individuals subjected to these technologies and complying with data protection principles such as data minimization. Therefore, this chapter should address certain questions to provide sufficient guidelines and clarity for the relevant stakeholders. For instance, what requirements should be part of the public procurements of facial recognition technologies in the law enforcement context so that data protection by design and by default obligations are met by those systems while still fulfilling their purposes? Although the reference to the GDPR guidelines and the hints in the Annex of the draft guidelines were deemed helpful, they are insufficient to provide comprehensive guidance and clarity on the matter. Lastly, it would have helped if the guidelines provided some examples of good practices from the Member States as well as identified "bad" practices.
- 14. Under the first bullet point of §100, the draft guidelines state, "The log should keep a copy of the relevant (added, deleted or updated) image...". We are unsure whether this should be in "the log" itself, as this appears risky. We believe it should instead be in a backup file with more restricted access.
- 15. Lastly, we believe that Scenario 6 is important as it is likely to happen in practice. However, this scenario seems to assume that the private database is in the European Union. What if the database is set up by a private entity in a country where the GDPR and/or Law Enforcement Directive do not apply? It would be helpful if the scenario would add an analysis of the lawfulness of a third country transfer by the police in such a case.

TILT remains at the European Data Protection Board's disposal should it require further information or clarification on the present submissions.

All communications related to this document could be directed to Mr. Taner Kuru via the email address provided herein: <u>t.kuru@tilburguniversity.edu</u>

**Contributors:** 

Prof. Dr. Bert Jaap Koops Prof. Dr. Eleni Kosta Dr. Irene Kamara Taner Kuru, LL.M.

Tilburg, 24.06.2022



**Understanding Society**