Dissertation Exposé

"Facial recognition by private entities and the legitimacy (or lack thereof) for data processing – Incompatibility with the EU data protection framework"

Submitted by

Emily Johnson, LL.B., LL.M.

Aspire academic degree of:

Doctor of Law (Doctor iuris)

Vienna, October 2020

Degree Programme: UA 783 101

Field of Study: Data Protection Law

Doctoral Student: Emily Johnson

Student ID: 11945546

Supervisor: Univ.-Prof. Dr. Nikolaus Forgó

1. Introduction

Globally, the development, testing and use of facial recognition technologies (FRT) is on the rise. Technologically, China has been spearheading the testing and implementation of FRT, but as the use of this technology proliferates in Europe, it is essential to consider the compatibility of FRT with EU primary and secondary law. The notably higher levels of protection accorded to fundamental rights including data protection and privacy in the EU when comparison to other jurisdictions, means that the use of any new technology, as with the processing of any personal data, must be consistent with the law.

At the time of writing, FRT is a relatively new surveillance technique and is beginning to be on the rise internationally. Currently, the primary actors in this field tend to be law enforcement authorities such as police (or equivalent competent authorities), private entities acting on behalf of these organisations and private entities for commercial reasons. Such systems are not without controversy and questions about their legality.[1] There have been notable examples of false recognition[2] adding to the risks presented by facial recognition (FR). The processing of personal data using FRT is directly connected to the right to the protection of personal data set out in Article 8 of the Charter of Fundamental Rights of the European Union (the Charter), as well as Article 7 of the Charter on the right to respect for a private life. Any processing of personal data must be permitted by law. Facial images which are processed using FRT to uniquely identify an individual qualify as biometric data, and therefore a special category of personal data as set out in Article 9(1) of the General Data Protection Regulation (the GDPR).[3] As such, to process this data, one of the provisions set out in Article 9(2) GDPR must be met. Similarly, the Article 5 GDPR principles of processing must also be met. However, the nature of FRT means that there are challenges in confirming both a legal basis for processing and the adherence with the Article 5(1) principles of processing. Given the increased growth and use of FRT in Europe, any legal uncertainties must be resolved to ensure the safeguarding of the data subject's rights.

2. Current Situation

Image based surveillance technologies have existed from as early as 1927[4] and have since proliferated and permeated societies globally. However, more recently, surveillance systems have developed beyond the basic monitoring techniques of a CCTV system to become automated. The rise of these automated FRT systems can be equated to "advances in computer vision processing (where machine learning

[1] I.Liberty, 'Resist Facial Recognition' (I.Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 22 November 2019.

[2] The Associated Press, 'In DC, Face Scans Peg a Lawmaker-And a Long-Dead Singer' (The New York Times, 14 Nov 2019) <https://www.nytimes.com/aponline/2019/11/14/business/ap-us-congress-facial-recognition.html> accessed 22 November 2019.

[3] 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).

[4] Albert Glinsky, *Theremin: Ether Music and Espionage* (University of Illinois Press 2000) 46-47.

techniques can be applied to recognise and learn from patterns in digital image data streams), alongside improvements in digital video camera technology".[5]

FRT utilises biometric identifiers that verify the identity of an individual based upon innate measurable human characteristics such as a fingerprint, an iris or the face. Due to its "universality and uniqueness", the human face "has become the most widely used and accepted biometric method".[6] A principle method of analysing facial characteristics in FRT is through the use of metrics which "most commonly involve measuring the distance between specific points on the face".[7] This method of identification has been used prior to the development in FRT in contexts such as forensics and court proceedings.[8] Using these metrics, FRT software "reads the geometry of a face captured from a photo or video to create a unique code or 'faceprint'" which is then compared with those on a database.[9]

Examples of the use of FRT by private entities is increasingly on the rise such as the use of FRT by retailers,[10] airlines,[11] casinos,[12] and in advertising.[13] In the retail sector, FRT is being used a requirement for ordering food,[14] through the creation recommendations for shoppers,[15] or through personalised

---

[5] Mark Andrejevic and Neil Selwyn, 'Facial Recognition Technology in Schools: Critical Questions and Concerns' [2019] 45(2) Learning Media and Technology 116.

[6] Paramjit Kaur and others, 'Facial-Recognition Algorithms: A Literature Review ' [2020] Medicine, Science and the Law.

[7] Teghan Lucas and Maciej Hennenberg, 'Are human faces unique? A metric approach to finding single individuals without duplicates in large samples' [2015] 257 Forensic Science International.

[8] G. Edmond, 'Specialised Knowledge, the Exclusionary Discretions and Reliability: Reassessing Incriminating Expert Opinion Evidence' [2008] 31(1) University of New South Wales Law Journal 1-55; G. Edmond and others 'Law's Looking Glass: Expert Identification Evidence Derived from Photographic and Video Images' [2009] 20(3) Current Issues in Criminal Justice 337-376; G. Edmond**, '**Impartiality, Efficiency or Reliability? A Critical Response to Expert.

[9] Ian Sample, 'What is Facial Recognition - and How Sinister Is It?' (*The Guardian*, 29 July 2019) <https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it> accessed 27 April 2020.

[10] Steve Symanovich, 'How Does Facial Recognition Work?' (Norton) <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> accessed 22 November 2019.

[11] Kari Paul, 'New Tool Helps Travellers Avoid Airlines That Use Facial Recognition Technology' (The Guardian, 5 June 2019) <https://www.theguardian.com/technology/2019/jun/05/airlines-facial-recognition-privacy> accessed 22 November 2019.

[12] Haley Samsel, 'Major Casino Game Company Will Add Facial Recognition Software to Machines, Adding Security Capabilities' (Security Today, 29 October 2019) <https://securitytoday.com/articles/2019/10/29/major-casino-game-company-will-add-facial-recognition.aspx> accessed 1 May 2020.

[13] Eden Gillespie, 'Are You being Scanned? How Facial Recognition Technology Follows You, Even as You Shop ' (The Guardian, 24 February 2019) <https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop> accessed 1 May 2020.

[14] Truong at al., 'Retail Ordering System with Facial Recognition' (United States Patent Application, 27 February 2020) < https://patentimages.storage.googleapis.com/a7/ae/71/46265c5f78127d/US20200065881A1.pdf > accessed 22 June 2020.

[15] Karuvath et al., 'Retail Store Shelf for Recommending Products Utilising Facial Recognition in a Peer to Peer Network' (United States Patent Application, 3 December 2019) <

targeted advertising in large shopping centres.[16] Whether this type of technology extends to fully-fledged biometric facial recognition is yet to be seen, but with the FRT market being bolstered by investors like Google, Facebook, Target, 7-Eleven and Walmart, along with predictions that global FRT market expected to be worth approximately $6bn USD by 2021,[17] the protection of consumers as data subjects is paramount. The commercial appeal of FRT is not hard to see. Businesses sell FRT by claiming it provides customers with a seemingly valuable service,[18] adding convenience to their lives,[19] improving their safety and security,[20] as a deterrent to crime,[21] improving health monitoring,[22] etc.

However, there are currently few laws sufficiently regulating the use of FRT. In a study looking into the use of invasive surveillance and biometric technologies, China ranked the worst out of 50 of the countries surveyed.[23] Further, 18 out of the 50 countries surveyed were EU countries and it was found that they had no specific laws regulating the use of biometric technologies.[24] The development of surveillance techniques in these two cities represent two culturally and geographically distinct examples of how with unregulated innovation, surveillance leads to increased surveillance. In July 2020 the European Parliament's committee on civil liberties backed a memorandum on banning the use facial recognition for law-enforcement purposes in public spaces. The rapporteur on AI in criminal law and the use of AI by police and judicial authorities warned, "risks linked to AI-technologies are aggravated in law enforcement as they might undermine the presumption of innocence, liberty, security, effective remedy or fair trial rights of individuals".[25]

---

https://patentimages.storage.googleapis.com/b0/ae/13/734f86346baf15/US10497014.pdf > accessed 22 June 2020.

[16] Eden Gillespie, 'Are You Being Scanned? How Facial Recognition Technology Follows You, Even as You Shop' (The Guardian, 24 February 2019) < https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop > accessed 22 June 2020.

[17] Ibid.

[18] Steve Symanovich, 'How Does Facial Recognition Work?' (Norton) <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> accessed 22 November 2019.

[19] Kari Paul, 'New Tool Helps Travellers Avoid Airlines That Use Facial Recognition Technology' (The Guardian, 5 June 2019) <https://www.theguardian.com/technology/2019/jun/05/airlines-facial-recognition-privacy> accessed 22 November 2019.

[20] SUPREMA 'Facial Recognition: Your Face is the key' (SUPREMA) <https://www.supremainc.com/en/solutions/facial-recognition-system.asp> accessed 22 November 2019.

[21] NEC, 'Face Recognition' (NEC) <https://www.nec.com/en/global/solutions/safety/Technology/FaceRecognition/index.html> accessed 22 November 2019.

[22] Madhumita Murgia, 'Who's Using Your Face? The Ugly Truth About Facial Recognition' (The Financial Times, 18 September 2019) <https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e> accessed 22 November 2019.

[23] Paul Bischoff, 'Biometric Data: 50 Countries Ranked by How They're Collecting It and What They're Doing With It' (*Comparitech*, 4 December 2019) <https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/> accessed 15 April 2020.

[24] Ibid.

[25] Elena Sánchez Nicolás, 'Facial-recognition Moratorium Back on EU Agenda' (euobserver, 3 July 2020) < https://euobserver.com/science/148839> accessed 8 July 2020.

As can be seen from the examples above, the use and development of FRT is expanding globally, and yet it is either widely unregulated or insufficiently regulated. As is increasingly the case, innovation supersedes regulation. In examining this technological surge, in combination with the sensitivity of facial recognition data and the uncertain laws regulating the use of FRT, we arrive at various concerns either directly or implicitly related to the right to respect for a private life and the right to the protection of personal data. Namely, the presence of a legal basis in data protection law, adherence to established principles of data protection, issues of data storage, of accuracy and reliability of the technology and the perpetuation of social biases.

The European Data Protection Supervisor has expressed concerns associated with the general legality of FRT[26] and an EU wide temporary ban on FRT has been suggested.[27] Similarly, the European Data Protection Board has noted that "the use *of biometric data and in particular facial recognition entail heightened risks for data subjects' rights*" and thus require due respect to the principles set out in the GDPR.[28] With the increasing growth and use of FRT, comes increased risks to fundamental rights and therefore sufficient regulation is essential.

3. Description of Intended Doctoral Thesis

This thesis will consider how the use of FRT in the context of private entities processing using FRT on members of the public is compatible with the EU data protection regime and will discuss both primary and secondary EU law. This analysis will form its foundations in the examination of the Charter. The Charter requires that any processing has a "legitimate basis laid down by law".[29] The legitimate basis laid down by law not only requires a legal basis for the processing but adherence to the regulatory framework in general. As such, this thesis will use the Article 5(1) principles of the processing of personal data as set out in the GDPR, as a structural guide for examining the compatibility of the use of FRT with EU data protection law, beginning with the lawfulness of processing. This paper hypothesises that this regulatory analysis will likely demonstrate that there is currently no legal basis for the processing of facial recognition data by private entities on members of the public under the GDPR. In addition to assessing the presence of a legal basis in this context, this thesis will also scrutinise the compatibility and contradictions of FRT with all other provisions in the Article 5(1) GDPR principles

[26] Wojciech Wiewiórowski, 'AI and Facial Recognition: Challenges and Opportunities ' (European Data Protection Supervisor, 21 February 2020) <https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en> accessed 1 May 2020.

[27] Javier Espinoza and Madhumita Murgia, 'EU Backs Away From Call For Blanket Ban On Facial Recognition tech' (Financial Times, 11 February 2020) <https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5> accessed 1 May 2020.

[28] European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data Through Video Devices' (European Data Protection Board, 10 July 2019) < https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf> accessed 6 June 2020.

[29] The Charter, Article 8(2).

with the exception of the 'integrity and confidentiality' principle. It is also hypothesised that incompatibility with the other Article 5 principles will be demonstrated. The conclusions of the legal basis and principle related discussion will then lead this thesis to consider the possible options for the EU data protection regime in the case that such processing is incompatible with current legislation. For example, whether FRT should face a blanket ban without the proper protection measures in place, and whether an EU wide Regulation on FR and biometrics could function in the current legislative sphere and what this would mean for the GDPR.

The starting point for this analysis will explain why FRT is distinct from its video surveillance predecessors. Image based surveillance is not new, however the risks associated with FRT are. As such, the general mechanisms of FRT and the technological shift it makes from traditional image-based surveillance techniques will be discussed. Following on from this, the ongoing spread of these technologies and some of the many examples of facial recognition as used by private entities in various contexts will be highlighted. These discussions will set the basis for a broad assessment of the uses of FRT highlight the increasingly unregulated exercise of FRT, where the current lack of targeted or harmonised legislation in the EU will be outlined.

This thesis will acknowledge that the development of a biometric and/facial recognition specific legislation is likely at an EU level. Drawing from this point, this thesis will look at the ways in which such a law would interact with the fundamental rights of the data subject as well as the current protections offered under the GDPR. Ultimately, this thesis will comment on whether the use of FRT technology by private entities should be prohibited in the case that there is no legal basis for it, or what other possible regulatory avenues exist in order to safely and legitimately employ FRT in the EU maintaining fundamental rights protections and adherence to secondary law. Therefore, conclusions will be drawn from the legislative analysis to examine the impacts for the future regulation of biometrics, FRT, and other new technologies. In making this examination, the relationship between the rule of law and the place of the law within the EU and nature of technological development will also be explored.

4. Research Questions

The core question this thesis aims to answer is as follows:

- Is the use of facial recognition technology by private entities on members of the public in the EU incompatible with the GDPR?

In answering this question, the following sub-questions will be discussed:

- Is the processing of facial data using recognition technology by private entities on members of the public in the EU compatible with the Charter?
- Is there a legal basis in the GDPR for the processing of facial data using recognition technology by private entities on members of the public in the EU?

- Is the processing compatible with the principles of processing set out in Article 5(1) of the GDPR?

It is hypothesised that processing will be incompatible with the GDPR, and if this hypothesis is argued to be true, the following conclusive questions will also be asked:

- What does the illegitimate processing of facial data by private entities mean for the GDPR?
- Is there a lowering of standards in EU data protection law?
- Should there be an adaption of the GDPR to make way for these increasingly pervasive technologies?
- Should there be an additional facial recognition/biometrics Directive or Regulation in the EU?
- Without a firm decision, should there be a blanket ban on the use of FRT in this context in favour of the protection of the data subject?
- What does this mean for the regulatory future of FRT and other biometric technologies in the EU?

5. Outline of Doctoral Thesis

Chapter 1

i. Introduction
ii. What is Facial Recognition Technology?
iii. Why does Facial Recognition Technology Require Legal Attention?

Chapter 2

i. Facial Recognition Technology and Fundamental Rights
    a. Privacy
    b. Data Protection
ii. The GDPR
    a. Legal Basis
    b. The Principles

Chapter 3

i. The Future of the GDPR
ii. What is next?
    a. Lowering of Standards
    b. Adaption of the GDPR
    c. Introduction of New Legislation
    d. Prohibition in Favour of Protection

Chapter 4

i. Conclusion

6. Timeline

WiSe 2020: Signing of Doctoral Thesis Agreement, and writing of Chapter 1

WiSe 2020/2021: Writing of Chapter 2

SuSe 2021: Writing of Chapter 3

WiSe 2021: Writing of Chapter 4 and review of entire thesis.

WiSe 2021: Defensio

7. Methodology

This thesis will take a top down approach with regard to the applicable legislation ensuring the preservation of data protection and privacy rights, starting with the Charter of Fundamental Rights of the European Union. The requirements of Articles 7 and 8 of the Charter will each be examined in detail which will set the basis for further discussion on secondary legislation, leading to a discussion of the GDPR. Core questions will be around the principles of processing of personal data as set out in Article 5(1) GDPR. In particular the lawfulness of processing and what the legal basis in data protection is for the processing of FR data. In addition, each of the Article 5(1) GDPR principles mentioned here will be examined to assess the compatibility of the processing of personal data using FRT by private entities on members of the public.

8. Bibliography

Primary Sources

European Convention on Human Rights.

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).

The Charter of Fundamental Rights of the European Union.

Secondary Sources

Andrejevic M. and Selwyn N, 'Facial Recognition Technology in Schools: Critical Questions and Concerns' [2019] 45(2) Learning Media and Technology.

Bischoff P., 'Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?' (*Comparitech*, 15 August 2019) <https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/> accessed 15 April 2020.

Edmond G., 'Impartiality, Efficiency or Reliability? A Critical Response to Expert Evidence Law and Procedure in Australia' [2010] 42(2) Australian Journal of Forensic Science.

Edmond G. and others 'Law's Looking Glass: Expert Identification Evidence Derived from Photographic and Video Images' [2009] 20(3) Current Issues in Criminal Justice.

Edmond G., 'Specialised Knowledge, the Exclusionary Discretions and Reliability: Reassessing Incriminating Expert Opinion Evidence' [2008] 31(1) University of New South Wales Law Journal.

Espinoza J. and Murgia M., 'EU Backs Away From Call For Blanket Ban On Facial Recognition tech' (Financial Times, 11 February 2020) <https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5> accessed 1 May 2020.

European Data Protection Board, 'Guidelines 3/2019 on Processing of Personal Data Through Video Devices' (European Data Protection Board, 10 July 2019) < https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf> accessed 6 June 2020.

Gillespie E., 'Are You being Scanned? How Facial Recognition Technology Follows You, Even as You Shop ' (The Guardian, 24 February 2019) <https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop> accessed 1 May 2020.

Glinsky A, *Theremin: Ether Music and Espionage* (University of Illinois Press 2000).

I.Liberty, 'Resist Facial Recognition' (I.Liberty) <https://www.libertyhumanrights.org.uk/resist-facial-recognition> accessed 22 November 2019.

Karuvath et al., 'Retail Store Shelf for Recommending Products Utilising Facial Recognition in a Peer to Peer Network' (United States Patent Application, 3 December 2019) < https://patentimages.storage.googleapis.com/b0/ae/13/734f86346baf15/US10497014.pdf > accessed 22 June 2020.

Lucas T. and Hennenberg M, 'Are human faces unique? A metric approach to finding single individuals without duplicates in large samples' [2015] 257 Forensic Science International.

Murgia M., 'Who's Using Your Face? The Ugly Truth About Facial Recognition' (The Financial Times, 18 September 2019) <https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e> accessed 22 November 2019.

NEC, 'Face Recognition' (NEC) <https://www.nec.com/en/global/solutions/safety/Technology/FaceRecognition/index.html> accessed 22 November 2019.

Nicolás E.S., ‘Facial-recognition Moratorium Back on EU Agenda’ (euobserver, 3 July 2020) < https://euobserver.com/science/148839> accessed 8 July 2020.

Paul K., 'New Tool Helps Travellers Avoid Airlines That Use Facial Recognition Technology' (The Guardian, 5 June 2019) <https://www.theguardian.com/technology/2019/jun/05/airlines-facial-recognition-privacy> accessed 22 November 2019.

Sample I., 'What is Facial Recognition - and How Sinister Is It?' (*The Guardian*, 29 July 2019) <https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it> accessed 27 April 2020.

Samsel H., 'Major Casino Game Company Will Add Facial Recognition Software to Machines, Adding Security Capabilities' (Security Today, 29 October 2019) <https://securitytoday.com/articles/2019/10/29/major-casino-game-company-will-add-facial-recognition.aspx> accessed 1 May 2020.

SUPREMA 'Facial Recognition: Your Face is the key' (SUPREMA) <https://www.supremainc.com/en/solutions/facial-recognition-system.asp> accessed 22 November 2019.

Symanovich S, 'How Does Facial Recognition Work?' (Norton) <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html> accessed 27 April 2020.

The Associated Press, 'In DC, Face Scans Peg a Lawmaker-And a Long-Dead Singer' (The New York Times, 14 Nov 2019) <https://www.nytimes.com/aponline/2019/11/14/business/ap-us-congress-facial-recognition.html> accessed 22 November 2019.

Wiewiórowski W., 'AI and Facial Recognition: Challenges and Opportunities ' (European Data Protection Supervisor, 21 February 2020) <https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en> accessed 1 May 2020.