TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Teele Nässi

FACIAL RECOGNITION – TECHNOLOGY FOR A SAFER FUTURE OR VIOLATION OF THE RIGHT TO PRIVACY?

Master thesis
Master Program, EU and International Law

Supervisor: Thomas Hoffmann, Dr. iur. LL.M.

Tallinn 2022

I hereby declare that I have compiled the thesis independently and all works, important standpoints and data by other authors have been properly referenced and the same paper has not been previously presented for grading.
The document length is 17812 words from the introduction to the end of conclusion.

Teele Nässi, …… 5 May 2022
Student code: 201352HAJM
Student e-mail address: teele1985@gmail.com

Supervisor: Thomas Hoffmann, Dr. iur. LL.M.
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENT

ABSTRACT 4
LIST OF ABBREVIATIONS 5
INTRODUCTION 6
1. BIOMETRICS 8
1.1. What is facial recognition technology? 9
1.2. History of facial reconstruction and recognition 10
1.3. FRT today 11
1.4. Applicable legal framework 13
2. THE USE OF FRT 17
2.1. FRT in smart cities and public places 18
2.2. FRT usage in computers and social media 19
2.3. FRT in law enforcement 20
2.3.1. Police body cameras 23
2.4. FRT and Covid-19 24
3. ESTONIAN AUTOMATIC BIOMETRIC IDENTIFICATION SYSTEM DATABASE 27
3.1. Overview of ABIS 27
3.1.1. Legal grounds of ABIS 29
3.1.2. Possible infringement on human rights 30
3.2. Other databases collecting facial images 32
3.3. Common database for Europe 33
4. IS FRT VIOLATING PRIVACY? 35
4.1. Current legislation on right to privacy 36
4.2. Right to privacy 37
4.3. Major concerns raised by facial recognition 39
4.4. Privacy vs security 42
5. POSSIBLE SOLUTIONS ON HOW TO USE FRT WITHOUT VIOLATING THE RIGHT TO PRIVACY 45
CONCLUSION 50
LIST OF REFERENCES 53
APPENDICES 62
Appendix 1. Non-exclusive licence 62

ABSTRACT

There is a growing number of technologies which use biometrics, including facial recognition technology, which can identify persons by their facial features. FRT is so powerful that even if we try to cover our face to hide our identity, it can still recognise us. But the legislation that is supposed to be protecting the right to privacy, when it is used, is not catching up in a speed that it needs to.

This current qualitative research that includes historical and semiotic approach and comparative legal research, explores the history, legal framework, and usage of FRT to determine the gaps in the regulations that may be the cause for violations of our right to privacy and right to be anonymous.

Based on the findings of this thesis, it seems, that while using FRT can have potential benefits of making our lives safer and help the law enforcement agencies to prevent crime, catch criminals and find missing people, FRT can pose serious threats to the right for privacy and data security and raises the question of: how can law enforcement use FRT without violating the right to privacy? Also, there is not a clear regulation of how, when and for what purpose this technology can be used without violating our rights for private life and it does not guarantee the protection of our private data.

Keywords: biometrics, facial recognition, privacy, right to privacy, FRT and privacy.

LIST OF ABBREVIATIONS

ABIS	Automatic biometric identification system database
AI	Artificial intelligence
BMS	Biometric matching service
BWC	Body-worn cameras
CCTV	Closed- circuit television
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
FBI	Federal Bureau of Investigation
FRA	EU Agency of Fundamental Rights
FRT	Facial recognition technology
GDPR	General Data Protection Directive
LED	Law Enforcement Directive
MRI	Magnetic resonance imaging
UDHR	Universal Declaration of Human Rights
WHO	World Health Organization
3D	Three-dimensional

INTRODUCTION

New and emerging technologies that use biometrics, like facial (or face) recognition technology (FRT), have an increasing impact on our everyday lives.[1] And in a world where everything is changing it is only natural that the technology changes with it. The growing numbers of internet and mobile device users and the development of different modern technologies shows the need to protect what is important, our rights. People wearing masks are becoming a social habit and a part of our everyday life because of the spreading of Coronavirus Covid-19, but do we always need to know and identify, who are behind those faces and masks? The rapid development of facial recognition technologies has led to complex ethical choices in terms of balancing individual privacy rights versus delivering societal safety.[2] It is evident that this multifaceted technology seems to evolve faster than the rules that govern it.[3]

It is acknowledged that artificial intelligence (AI) is developing in an enormous phase and this rapid development has taken the legal and ethical discussion to a new level. One of the fields that is developing in the same pace is facial recognition technology and since the use of this technology is increasing in different areas, it has also provoked many discussions due to its close link to one of the fundamental human rights – right to privacy.[4] Naker and Greenbaum have explained: "privacy is a precondition for the democracy development and freedom. Without privacy there is no freedom of expression, freedom of religion or freedom of movement." [5]

The author acknowledges that while using the FRT is becoming more common, as it seeks to help law enforcement to prevent and solve crimes, identify criminals, and find missing people, the use

[1] Chochia, A., Nässi, T. (2021). Ethics and emerging technologies–facial recognition. *IDP: revista d'Internet, dret i política*, (34), 1.
[2] Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, Springer, 1.
[3] Caplier, M. (2021). Assessment of the European legal framework of facial recognition technology. *L'Europe Unie,* 17(17), 30.
[4] Chochia, A., Nässi, T. (2021). Su*pra nota* 1, 2.
[5] Naker, S., Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *Boston University Journal of Science and Technology Law*, 23(1), 101.

of the system and collecting data of regular people does not always consider their right to privacy and the right to be anonymous.

This research will be qualitative, comparative legal analysis and literature review that includes historical and semiotic approach and explores the history, legal framework, and usage of facial recognition technology to determine the ways FRT violates our right to privacy and right to be anonymous. The literature research was performed from Google Scholar and Tallinn University of Technology Library portal Primo using different keywords and time limit (2019 and newer) articles. In case of historic background, older sources have also been used.

In the thesis author will answer a research question: How can law enforcement use FRT to prevent and fight crime without violating the right to privacy?

This research explores the analyse existing regulatory frameworks and legal basis for the use of facial recognition technology and its impact to one of the primary human rights, the right to privacy. To solve the research problem, comparative analysis is used. The author evaluates the results based on the literature and findings and discusses the possible solutions and amendments that need to be done in EU legislation. While looking for the answer to the research question, following questions are also discussed:

- Does current EU regulation allow the use of facial recognition technology without violating the right to privacy?
- Do law enforcement agencies breach right to privacy when using FRT?
- Should FRT be banned in all areas?

The first chapter on biometrics gives an overview of facial recognition, its history, and law currently applicable. The second chapter provides an overview of the use of FRT, including smart cities, social media, and ways in which it is used by law enforcement. It also explains how the Covid-19 has influenced the development of this technology. The third chapter provides some insights to the Estonian ABIS database, its principles, and potential breaches. The author also gives examples of other databases that collect and use facial images, which are used worldwide. In the fourth chapter, overview of current legislation on the right to privacy is given, the author examines and discusses the concept of right to privacy and the main concerns that arise when using FRT. In the last chapter the author presents her views and solutions on how to minimize privacy violations when using this modern technology.

1. BIOMETRICS

The term biometrics refers to science or technology to measure and analyse biological data – measurable behavioural and/or physiological characteristics that could be used to verify individual identification. Biometric information, which is unique for everyone, cannot be copied or stolen, but it could be used for verification, for example in different industries, such as healthcare, banking and finance, transport and immigration, gaming, automobile, retail, or even in prison security, secured access, and forensics. Biometric systems recognize individuals using authentication by utilizing different biological features such as the face, hand geometry, iris, retina, and fingerprints.[6] A technique such as face recognition could, at least in principle, be used to recognize people "passively," without their knowledge or cooperation.[7] The use of biometrics has increased tremendously and there is now a technology that is only based on public observation, meaning that in order to identify the suspect there is no longer need to touch, feel or be anywhere close, to identify them.[8]

In some variations, according to J.N. Pato and L.I. Millett and J.A. Unar and his associates, biometric systems are designed with four key modules. The first is an image acquisition module (e.g., reading or scanning device) that records a biometric identifier (e. g., face, fingerprint, or iris). The second component is a feature extraction module that converts the scanned biometric data into a digital code using a secure algorithm. The third module is a matcher module that compares and matches the observed coded data with the data stored in a database and recognizes an individual if their data are available in the database. The fourth component of the biometric system is a database module that stores the coded biometric data for further comparison.[9][10]

[6] AbdELminaam, D., Almansori, A., Taha, M., Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. *PloS One,* 15 (12), 2.
[7] Bowyer, K. (2004). Face recognition technology: Security versus privacy. *IEEE Technology & Society Magazine, 23* (1), 10.
[8] Turley, J. (2020). Anonymity, obscurity, and technology: Reconsidering privacy in the age of biometrics. *Boston University Law Review*, 100 (6), 2203.
[9] Pato, J.N., Millett, L.I. (Eds.) (2010). *Biometric Recognition: Challenges and Opportunities.* Washington: National Academies Press.
[10] Unar, J.A., Seng, W.C., Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recogniti*on, 47 (8).

While there are other biometric identifiers, that may be more accurate, such as fingerprints or gait recognition, as Kelly Gates (2011)[11] has compellingly documented, the face has an integral historical relationship to identity and interpersonal relations.[12]

According to General Data Protection Directive (GDPR)[13] article 4(14) biometric data is considered personal data resulting from specific technical processing. Biometric data allows to confirm natural persons unique identification, such as facial images.[14]

1.1. What is facial recognition technology?

Facial recognition technology is defined in the EU as the "automatic processing of digital images which contain the faces of individuals for identification, authentication/ verification or categorisation of those individuals"[15].

FRT as a part of AI applications for purposes of remote biometric identification means that the template of a person's facial image is compared to many other templates stored in a database to find out if his/her image is stored there and it can be carried out remotely, usually via video cameras (closed-circuit television CCTV), and is commonly called 'live facial recognition technology' or 'remote biometric identification'.[16]

In the process of facial recognition, the information on a mass scale is captured, recorded, and processed, far beyond the capability of any individual or group of individuals. The data collected by FRT systems are reproducible, exportable, and machine readable in ways that human recognition and memory is not.[17]

[11] Gates, K. (2011). *Our Biometric Future* (Critical cultural communication). New York: NYU Press.
[12] Andrejevic, M., Volcic, Z. (2021). "Smart" Cameras and the Operational Enclosure. *Television & New Media*, 22(4), 345.
[13] Regulation 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, OJ 2016 L 119/1.
[14] GDPR Article 4(14) and LED Article 3(13).
[15] Opinion 02/2012 on facial recognition in online and mobile services, Article 29 Data Protection Working Party, 2012, 2.
[16] Caplier, M. (2021). S*upra nota* 3, 30.
[17] Andrejevic, M., Volcic, Z. (2021). S*upra nota* 12, 345.

1.2. History of facial reconstruction and recognition

The first scientific indications of facial reconstructions were made in 1884 by anatomists as an academic exercise. The anatomist Welcker compared, what was thought to be Raphael's skull, with a self-portrait and compared the supposed skull of Kant with his death mask. He found that the respective correlations were too good for chance. Welker used the two-dimensional techniques; providing accurate orthogonal perspective drawings as an outline of the skull and the death mask, and attempting to superimpose the outlines, he made allowance for the outer tissues.[18] After that, there were a number of anthropologists and anatomists, who tried to do the facial reconstructions of early hominoids such as Neanderthal and Pithecanthropus, and others of the Stone Age.[19] As Welinder explains, facial parameters are extremely useful for identification, due to distinction, availability, difficulty to alter, etc.[20]

The first work on automatic facial recognition was done by W.W. Bledsoe around 1964.[21] He´s initial approach was to manually mark various landmarks on the face, which were mathematically rotated by computer to compensate for pose variations. Distance and distance ratios between those landmarks were automatically computed and compared between images to determine goodness-of-fit. Later work also could find those landmarks automatically. He´s research, made alongside H.C. Wolf and C. Bisson, involved about 40 000 comparisons using dataset of 2000 images.[22]

The work done by Bisson was continued in 1970s by Goldstein, Harmon and Lesk, who pruned the initial set of 34 features to 22, for which the data are consistent and reliable.[23]

Computerized facial reconstruction for forensic purposes was first developed in 1980s by Moss and his colleagues at London´s University College in UK and was based on a system used for cranial reconstructive surgery. The system was developed for 3D surface data acquisition of the

[18] Wilkinson, C. (2004). *Forensic facial reconstruction*. Cambridge: University Press.
[19] Verze, L. (2009). History of facial reconstruction. *Acta Biomed*, 80, 8.
[20] Welinder, Y. (2012). A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. *Harvard Journal of Law and Technology*, 26 (1), 167.
[21] Bledsoe, W.W. (1966). Man-machine facial recognition: Report on a Large-Scale Experiment, Technical Report PRI 22, *Panoramic Research Inc.*, CA: Palo Alto.
[22] De Leeuw, K.M.M., Bergstra, J. (2007). *The History of Information Security: A Comprehensive Handbook*. Amsterdam: Elsevier, 264–265.
[23] Goldstein, A., Harmon, L., Lesk, A. (1971). Identification of human faces. *Proceedings of the IEEE*, 59 (5), 759.

human face, it involved limited manual intervention, and was a subject to minimal human error.[24] The author agrees with Kelly A. Gates, who stated, that the search of automated facial recognition technologies and new forms of integration of human and machine, can lead to more sufficient and effective surveillance systems that might reach over time and space. And although this experimental and novel technology can be useful for many things, it is still open to debate, whether it can or should be used to accomplish all the goals, that are set, while considering the trade-off between "security" and "privacy".[25]

Further progress in development of facial recognition software was done by Sirovich and Kirby, who developed a system called Eigenface, that resulted in an extension of the data and imposes even and odd symmetry on the eigenfunctions of the covariance matrix, without increasing the complexity of the calculation.[26]

In 1998 L.A. Nelson and S.D. Michael described a system of computer facial reconstruction named Volume Deformation.[27] This system started with magnetic resonance imaging (MRI), and it used a face that the result would ultimately resemble, and it was therefore only as close to the real face as the sample face was. De Greef and Willems also worked on computer-aided reconstructions in 2005 and specialised on eyes and mouth.[28]

1.3. FRT today

The facial recognition process, as known today, begins with capturing of the face image, also known as the probe image (usually taken from photo camera or video camera, for example), then the face is being detected and extracted from the larger image (background or other faces), the system will then "normalize" the image in the database and pass it through the recognition software

[24] Arridge, S., Moss, J.P., Linney, A.D., James, D.R. (1985). Three dimensional digitization of the face and skull. *J Maxillofac Surg*, 13(3); Moss, J.P., Linney, A.D., Grindrod, S.R., Arridge, S.R., Clifton, J.S. (1987). Three dimensional visualization of the face and skull using computerised tomography and laser scanning techniques. *Eur J Orthod*; 9 (4).
[25] Gates, K. (2011*). Supra nota* 11.
[26] Kirby, M., Sirovich, L. (1990). Application of the Karhunen-Loeve procedure for the characterization of human faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 12 (1).
[27] Nelson, L.A., Michael, S.D. (1998). The application of volume deformation to three-dimensional facial reconstruction: a comparison with previous techniques. *Forensic Sci Int.*, 94 (3), 174.
[28] De Greef, S., Willems, G. (2005). Three dimensional cranio-facial reconstruction in forensic identification: latest progress and new tendencies in the 21st century. *J Forensic Sci*; 50 (1).

where the possible match will be made between the new and database images.[29] As Spiesel explains, FRT is a task-specific computer vision, which relies on the data obtained by its sensors and an algorithm, and is required to be trained to perform matching of the obtained images.[30]

As indicated by Chochia and Nässi in 2021, the FRT is used all around the world by many different law enforcement agencies in order to monitor the public space via biometric data collection.[31] It is seen as a potentially powerful instrument for law enforcement and commercial interests and compared to other biometric security solutions such as palmprints and fingerprints, facial recognition is providing vast benefits, since it captures biometric measurements of a person from a specific distance without interacting with the person.[32]

FRT is used for security and law enforcement and is "trending" across the world as a safe and reliable technology.[33] FRT is widely used in private areas and public places (airports, banks, schools, hotels, casinos etc.) and can help fight crime and corruption, find missing people, or even impose age restrictions on online viewing of pornography[34]. It is also commonly used in the medical and health field – some of the major applications include tracking patients' drug use, detecting genetic diseases such as DiGeorge syndrome, and supporting pain management procedures.[35] During Covid-19 the FRT has also been used to identify persons that are infected and tracing those, who have been in contact with Covid-19 infected persons.[36]

The author accepts the Lai and his associate's prediction that while the FRT and its use is increasing, in the next few years it is also expected to be expanding more to end-user industries, like automotive, smart home and other fields, not only for law enforcement.[37]

---

[29] Introna, L.D., Nissenbaum, H. (2010). Facial Recognition Technology: A Survey of Policy and Implementation Issues, *The LUMS Working Paper Series.* The Department of Organisation, Work and Technology, 11.
[30] Spiesel, C. (2020). Technology's Black Mirror: Seeing, Machines, and Culture. *Int J Semiot Law*.
[31] Chochia, A., Nässi, T. (2021). *Supra nota* 1, 3.
[32] AbdELminaam, D., Almansori, A., Taha, M., Badr, E. (2020). *Supra nota* 6, 2.
[33] *Ibid.*
[34] O'Mallon, F. (2019). *Home Affairs suggests porn viewers be subject to face scans*. Retrieved from https://www.smh.com.au/politics/federal/home-affairs-suggests-pornviewers-be-subject-to-face-scans-20191028-p534yk.html, 14 December 2021.
[35] Lai, X., Patrick Rau, P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior*, 124, 2.
[36] Whitelaw, S., Mamas, M. A., Topol, E., Van Spall, H. G. C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, 2(8).
[37] Lai, X., Patrick Rau, P. (2021). *Supra nota* 35, 2.

When examining people´s trust in these new technologies used by law enforcement, studies show that Chinese citizens trust the central government more than private enterprises to manage and implement surveillance technologies.[38] Another poll conducted in 2019 shows that out of 4109 adult responders in the United Kingdom, 77% are uncomfortable with FRT being deployed by commercial companies and 49% support FRT use for policing purposes given appropriate safeguards. 67% of responders oppose the use of FRT in schools and 61% oppose its use on public transport.[39] In contrast, the 2019 cross-national survey of the USA, UK, China, and Germany indicates that while citizens generally trust their government more in the management and provision of the technology than private companies, more than half of all citizens are also very accepting of public–private partnerships – respondents' acceptance rate of FRT for private use (52%) was higher than that of government-use FRT (42%).[40]

While there is public acceptance and a real need for the use of FRT there are also big concerns about the legal use of this technology. Lai and his associates have expressed that while the original motivation of facial recognition is human well-being, the public is already facing many misuses of the technology that threaten both their safety and privacy."[41] Many researchers have implied the same concerns and these issues will be discussed in this thesis.

1.4. Applicable legal framework

Facial recognition technology deals largely with personal data processing which is regulated in the General Data Protection Regulation, that came into force on 25 May 2018 and its Law Enforcement Directive (LED).[42] The GDPR covers all the Member States of the EU and regulates the main issues about data protection law in the European Union with modern rules, that fit better in the time where technology is evolving in a massive speed. GDPR's main principle is that personal data should not be collected, or processed, more than what is necessary for a certain

[38] Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21 (7).
[39] Ada Lovelace Institute (2019). *Beyond face value: Public attitudes to facial recognition technology*. Retrieved from https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf, 23 January 2022.
[40] Kostka, G., Steinacker, L., Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, 30 (6), 686.
[41] Lai, X., Patrick Rau, P. (2021). *Supra nota* 35, 1.
[42] Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4.5.2016.

purpose. The GDPR principles also include making clear to individuals when and how facial recognition data are being collected, stored, and used; developing data management practices that consider how individuals are enrolled and what the risks, harms, and benefits of such (in)voluntary enrolment and maintaining the accuracy and integrity of any stored data may be.[43]

The Law Enforcement Directive is more specific regime than the GDPR and it is applicable when public authorities process personal data for the purpose of the prevention, investigation, detection, or prosecution of criminal offences.[44] It also includes safeguards and regulation on the prevention of threats to the public security.

It has been expressed that the GDPR "has been seen as setting the bar at the highest level for the management of personal data"[45] and processing of biometric data. As formulated in the GDPR articles 1 and 2, the regulation protects fundamental rights and freedoms of natural person and their right to the protection of their personal data.

Following the main legal principles of data protection (GDPR art 5 and LED art 4), the processing of facial images must be: lawful, fair and transparent; follow a specific, explicit and legitimate purpose; comply with the requirements of data minimisation, data accuracy, storage limitation, data security and accountability.[46]

GDPR (art. 9) protects and requires consent for the collection of personal data, particularly sensitive data, including biometrics. GDPR explains: "processing of […] biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited".[47] This general prohibition is subject to ten exceptions, exhaustively listed in Article 9(2). The first, processing such a sensitive category of personal data can only be lawful when the "data subject has given explicit consent" to it "for one or more specific purpose".[48] "Consent" is defined and clarified several times throughout the text, but its main characteristics are that it must be "freely given,

[43] National Telecommunications and Information Administration. (2016*). Privacy Best Practices Recommendations for Commercial Facial Recognition Use*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recogntion.pdf, 17 February 2022.
[44] LED Recitals 11 and 12 and GDPR Recital 19.
[45] Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). *Supra nota* 2, 4.
[46] European Parliamentary Research Service (2021*). Regulating facial recognition in the EU. In-depth analysis.* Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698021, 13 April 2022.
[47] GDPR Article 9(1).
[48] GDPR Article 9(2) a).

specific, informed and unambiguous."[49] Recital 43 lays down a relevant exception: it states that consent will be presumed not to have been freely given "in a specific case where there is a clear imbalance between the data subject and the controller". Also, one must bear in mind, that the data subject can withdraw the consent at any time,[50] meaning that at the time of processing any data, controller must make sure, that the consent still exists. According to Caplier: "Even if the provision lacks precision, one can understand that the consent given by an ordinary citizen to a public authority therefore not provides a valid legal basis for the processing of the citizen's data, given the manifest balance of power between the actors involved." [51]

Another important legal ground is when "processing is necessary for reasons of substantial public interest"[52], meaning that the national and EU legislators have the discretion to decide the specific cases, where the use of FRT guarantees a proportionate and necessary interference with any human rights."[53]

It´s elaborated, that the data can only be processed when necessary to protect "vital interest of the data subject or of another person"[54], appropriate safeguards are considered, such as "the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data."[55] Another exception is where the "processing relates to personal data which are manifestly made public by the data subject"[56], for example when information is posted in social media.

Although the GDPR protects individual´s personal and sensitive data, including biometrics, it remains unclear if facial images always fall under the scope of GDPR, depending, for example, on the legal justification for processing because substantial public interest such as national security or public safety may afford path for circumventing consent.[57] Jennifer Lynch, a researcher on biometrics and facial recognition, has indicated that this highly developed biometric technology

[49] GDPR Recital 32 and Article 4(11).
[50] GDPR Article 7(3)
[51] Caplier, M. (2021). *Supra nota* 3, 32.
[52] GDPR Article 9(2) g).
[53] Bu, Q. (2021). The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. *Internntional Cybersecurity Law Review,* 2, 116.
[54] GDPR Article 9(2) c) and LED Article 10 b)
[55] LED Recital 37.
[56] GDPR Article 9(2) e) and LED Article 10 c).
[57] Buckley, B., Hunter, M. (2011). Say Cheese! Privacy and facial recognition. *Computer Law and Security Review*, 27 (6), 639.

such as facial recognition might create additional concerns, since the data that is collected, may be collected without a person's knowledge.[58]

The author agrees that although the GDPR has tried to regulate the use of biometric data, including the facial recognition, it still has no clear indications on how to use the technology without violations and always considering people's privacy.[59] Many researchers have claimed that there are many privacy risks that the use of biometrics can raise, Omar Tene indicated that these risks can also include function creep, identity theft, and government surveillance.[60]

Buckley and Hunter have claimed that since use of facial recognition technology involves using an individual's facial image and therefore includes processing of personal data of a person, this usage of technology can only take place if a legal justification exists.[61] This legal justification is elaborated by Chochia and Nässi, stating that any processing of personal data falls within the conditions set in article 7 of GDPR, meaning that individuals must be informed of the processing of their data according to GDPR-s articles 10 and 11.[62]

The author acknowledges that although some legal framework to processing biometric data and FRT is given, as indicated by many scholars before, the regulation is still far from being completely clear and needs improvement. The author agrees with Caplier, that anyone wishing to use FRT or any other technology using biometrics, must make sure that the legal ground to do so exists and the sensitive data is processed lawfully, therefore special guidelines are needed, especially for facial recognition.[63]

Fortunately, some progress has already been made, when at the end of January 2021, the Council of Europe published guidelines on facial recognition, that is addressed to legislators and decision-makers, developers, manufacturers, service providers and " for entities using FRT".[64] Although not a binding document for EU, the guideline still sets some grounds for FRT applications.

---

[58] Lynch, J. (2012). What Facial Recognition Technology Means for Privacy and Civil Liberties. *Senate Committee on the Judiciary*, 14.
[59] Chochia, A., Nässi, T. (2021*). Supra nota* 1, 4.
[60] Tene, O. (2011). Privacy: The new generations. *International Data Privacy Law*, 1 (1), 21.
[61] Buckley, B., Hunter, M. (2011). *Supra nota* 57, 639.
[62] Chochia, A., Nässi, T. (2021). *Supra nota* 1, 4.
[63] Caplier, M. (2021). *Supra nota* 3, 33.
[64] Council of Europe. (2021). *Guidelines on facial recognition. Consultative committee of the Convention for the protection of individuals with regard to automatic processing of personal data*. Retrieved from https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3, 12 March 2022.

2. THE USE OF FRT

Already in 1999 it was acknowledged that facial recognition and video surveillance technology can be successful in catching criminals and preventing criminal activity.[65]

The facial recognition system is fast gaining attention and importance among thousands of corporate and government organizations because it is believed that it has high level of security and reliability.[66] But where can we find it? When looking at one of the main goals of FRT, which is the security and protection of people and their property, there are many more areas that use FRT for their own purpose. As already mentioned, it´s being used in mobile phones and web platforms for authentication, in various public places, but also in private industries like smart homes and automotive. Everyone already knows there are possibilities to use our face in some situations, for example it is possible to unlock and enter our phones, pay, or even prevent tiredness while driving a car, but the use of facial recognition goes a step further: it also allows police to track and identify criminals, find missing children, use it for commercial purposes or go through passport control to enter another country, etc.

As stated by Andrejevic and Volcic: "Given the interest in the technology by authorities both public and private, there is a strong likelihood that facial recognition technology will transform the spaces through which we move into a visual sensing system that will reconfigure the experience of what it means to be "out in public" by making comprehensive tracking the rule rather than the exception—for everyone."[67]

This chapter gives an overview of the uses of FRT both in private and public sectors.

[65] Milligan, C. S. (1999). Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal*, 9 (1), 323.
[66] AbdELminaam, D., Almansori, A., Taha, M., Badr, E. (2020). *Supra nota* 6, 2.
[67] Andrejevic, M., Volcic, Z. (2021). *Supra nota* 12, 355

2.1. FRT in smart cities and public places

According to European Commission, "a smart city is a place where traditional networks and services are made more efficient with the use of digital solutions for the benefit of its inhabitants and business."[68] It goes beyond the use of digital technologies, and it means a more interactive and responsive city administration, public spaces that are safer for everyone and making sure that the needs of an aging population is met.[69] Manon Caplier has indicated that smart-city concept is a dream world for many private companies, as it promises a simpler, safer, and smoother environment.[70]

In smart city, every innovative technology is welcomed as long as it helps to keep the city safer and user friendlier. One of the emerging technologies, which is becoming more common there, is facial recognition technology since it´s a possible solution to identify and/or recognise people and track their movement throughout the city. And it is not only the smart cities, which are moving towards using new ways to identify people. Biometric systems are also used in public places by private companies, such as banks, telecommunication companies but it is also used in retail and e-commerce, to monitor, help and guide shoppers.

News about FRT being used in public places are coming around the world. This new trend is also been used in education, for example, to help combat school bullying or track attendance;[71] workplaces are also adopting FRT, allowing employees to clock in and out, but the downside is that they also use the FRT to track workers activity and productivity.[72] But it's not only work or school, there has also been indications, that FRT is used in shopping malls, to read expressions

[68] European Commission. *Smart cities.* European Commission´s official website. Retrieved from https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en, 11 March 2022.
[69] *Ibid*
[70] Caplier, M. (2021). *Supra nota* 3, 30.
[71] Levy, A. (2010). *School installs £9000 facial recognition cameras to stop students turning up late… and teachers could be next target.* Retrieved from https://www.dailymail.co.uk/news/article-1317520/School-installs-9kfacial-recognition-cameras-stop-students-turning-late.html; Chronicle, D. (2018). *Artificial Intelligence Can Help Schools Safeguard Children.* Retrieved from https://www.asianage.com/technology/in-other-news/310518/artificial-intelligence-can-help-schools-safeguard-children.html; Durkin, E. (2019). *New York school district's facial recognition system sparks privacy fears*. Retrieved from https://www.theguardian.com/technology/2019/may/31/facialrecognition-school-new-york-privacy-fears, 23 March 2022.
[72] Creed, S., Dixon, A. (2020). *Facial recognition technology in empolyment: What you need to know.* Retrieved from https://www.twobirds.com/en/insights/2020/global/facial-recognition-technology-in-employment, 11 March 2022.

and track de-identified individuals from camera to camera across shopping malls with the intention of inferring the gender, age, and 'mood' of individual shoppers.[73]

2.2. FRT usage in computers and social media

Already in 2008, Lenovo launched a new series of laptops that instead of requiring a password, could recognise the face of their authorised user.[74] It was seen as a marketing benefit for Lenovo and many users consented and engaged with the new feature.[75] Since then the facial recognition solutions for computers and smartphones both for personal and professional users, are nothing new, since it is used to grant access to all these devices and to many digital services, like Facebook or Snapchat.

One of the biggest and most controversial issue with the use of FRT was the Facebook´s technology, which helped user to "tag"[76] friends in photos they uploaded to the platform. Along with just "tagging" their friends, Facebook helped their users to identify the persons in the picture, using facial recognition technology, that enabled the company to identify a person's face with nearly 98% accuracy.[77] This advanced and accurate technology was seen as the most robust and well-developed of all the other private sector products.[78] Very soon after the company started using the FRT, problems occurred, biggest being that there were no specific biometric privacy laws issued, giving Facebook privileges to prevail over their users, who didn't really understand all the terms that were set in the Terms of Service and Data Policy.

By collecting data, Facebook was soon found in a lawsuit. In Facebook v. Patel, it was alleged that Facebook misled tens of millions of users about their ability to control facial recognition within their accounts.[79] Although it was supposed to be a privacy-protective case, which might help see,

---

[73] Anscombe, L. (2017). *Westfield is using facial detection software to watch how you shop*. Retrieved from https://www.news.com.au/finance/business/retail/westfield-is-using-facial-detection-software-to-watch-howyou-shop/news- story/7d0653eb21fe1b07be51d508bfe46262, 14 March 2022.
[74] Gates, K. (2011). *Supra nota* 11.
[75] Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). *Supra nota* 2, 3.
[76] According to Facebook, "when you tag someone, you create a link to their profile ... you can tag a photo to show who's in the photo." What is tagging and how does it work? Facebook. Retrieved from https://www.facebook.com/help/267689476916031/?helpref=hc_fnav, 12 March 2022.
[77] Higginbotham, S. (2016). *Inside Facebook's Biggest Artificial Intelligence Project Ever*. Retrieved from https://fortune.com/longform/facebook-machine-learning/, 26 March 2022.
[78] Lynch, J. (2012). *Supra nota* 58, 9.
[79] Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019).

how court views FRT[80], the Supreme Court unfortunately declined the case. Facebook still made some changes in their "Photo Tag Suggest" feature in 2019 and by today they have decided to stop using the FRT feature altogether.[81]

2.3. FRT in law enforcement

For the author, the most important part of this research is to understand if the usage of facial recognition technology in law enforcement is currently allowed and legal or are Government agencies abusing their rights and invading people´s privacy.

Law enforcement agencies are always looking for more advanced ways to keep our environment safe and for that they are looking to adapt new and improved technologies. These new technologies include using surveillance cameras, automated license plate readers, body cameras, drones, and now even facial recognition technologies.[82] Q. Bu has even expressed that "FRT improves efficiency of law enforcement and enhances a state's national security."[83] When using any of these crime deterrent applications, they can possibly help many organizations identify a person, who might have any kind of criminal record or other legal issues.[84] But by using these possibilities, it is very clear that personal data is also used, and that can clear impacts on individuals rights.[85]

Although the modern technologies are used around the world, they are developed at different speeds in different countries, depending on their specific capabilities and financial resources, which means that the use of technologies, such as FRT, is not uniform across the EU.

The deployment of facial recognition by law enforcement agencies is subject to similar conditions under the LED (Articles 4(1)(a) and 10 LED).[86] Within law enforcement contexts, police departments invoke criminal procedure codes or surveillance codes and police laws as legal

[80] Bu, Q. (2021). *Supra nota* 53, 119.
[81] Pesenti, J. (2021). *An update on our use of face recognition*. Retrieved from https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/, 23 March 2022.
[82] Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). *Supra nota* 2, 1.
[83] Bu, Q. (2021). *Supra nota* 51, 115.
[84] AbdELminaam, D., Almansori, A., Taha, M., Badr, E. (2020). *Supra nota* 6, 2.
[85] Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). *Supra nota* 2, 2.
[86] European Union Agency for Fundamental Rights (FRA). (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* Retrieved from https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law, 12 March 2022.

bases.[87] In a United Kingdom case, the Appeals Court overturned a decision of the first instance, inter alia because the legal framework did not qualify as a legal basis, because it was imprecise and afforded individual police officers too much discretion concerning who could be placed on a watch-list and where FRT could be deployed.[88]

The FRT is most commonly used by police in places where many people are gathered together, for example in big concert halls, or in public gatherings or demonstrations, or any other places that might possibly have ill-intentioned persons, "persons of interest"[89] or even potential terrorists among spectators.[90] All this is usually done in good intentions, we would expect, to help people feel safer and help to the enforcement agencies identify the potential criminal easier and more quickly.

Every innovative technology is hopefully providing benefits, like helping simplify the everyday work that any police officer or official has to do, for example, in the current case, automatic recognition and identification is not as time-consuming as the manual work would be.

Another benefit for law enforcement is that FRT helps them by creating valuable and reliable evidence from video footage and keep track of criminals or potential lawbreakers, which enables law enforcement to react more effectively.[91] Despite all the serious concerns, facial recognition technology has been useful for law enforcement in many criminal investigations.[92]

The author already indicated that people believe and trust, that when law enforcement officials use FRT, they do it with good intentions. This trust is one of the main components that motivates acceptance of police use of FRT, and as proposed by Bradford et al. "trust provides reassurance that this new power will be used in the correct way and not be abused."[93] They continue that when people believe that police uses their power appropriately, they also believe that they have a right to use this power, because the ends to which this power was directed are appropriate.[94] The author

[87] UK Information Commissioner's Office, Opinion on The use of live facial recognition technology by law enforcement in public places, 2019, p. 9.
[88] Judgment in Case No. C1/2019/2670, Court of Appeal, 11 August 2020, paras. 90-96.
[89] Purshouse, J., Campbell, L. (2021). Automated facial recognition and policing: A Bridge too far? *Legal Studies*, 3.
[90] Caplier, M. (2021). *Supra nota* 3, 34.
[91] Hamann, K., Smith, R. (2019). Facial recognition technology: where will it take us? *Crim Justice*, 34 (1), 9–19.
[92] Haddad, G. M. (2021). Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom. *Vanderbilt Journal of Entertainment and Technology Law*, 23 (4), 897.
[93] Bradford, B., Yesberg, J.A., Jackson, J., Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *British Journal of Criminology,* 60 (6), 1505.
[94] *Ibid*, 1506.

elaborates, that by believing, that police is competent, acting with their right intentions, being moral and good, it is expected, that they also act the same way, when using any new technology, like facial recognition.

The research by Bradford et al. also indicates that people worried about crime tended to be more accepting of police use of FRT, but the primary factor motivating acceptance or rejection of police use of FRT, is the concern about privacy—the sense that this technology may be used to intrude into people's lives. They found specific public concerns including fears about eroding privacy, undemocratic implementation, and a lack of trust.[95]

The author understands that while most people are accepting that the police use of new and emerging technologies are helpful and useful, there are also many, that feel the opposite.

Groups such as Amnesty International, an organisation who´s priority is to help people claim their rights, is calling for a ban on the use, development, production, sale and export of facial recognition technology for mass surveillance purposes by the police and other state agencies.[96] Another civil liberties group, Liberty, has also campaigned to ban the police use of FRT altogether, particularly in public spaces.[97] Other bodies articulate that while FRT is beneficial, there must be 'meaningful restrictions'.[98]

Research conducted by Bragias et al. indicates that people expressed concerns about the potential abuse of police authority and power when using FRT. Though previous work has typically labelled this concern as 'mistrust', it is more nuanced to examine it through the lens of the fear of abuse.[99] Bromberg et al. assert that while many citizens do approve of this technology, many also report feeling a social obligation to approve of police use of FRT.[100]

---

[95] *Ibid*, 1515.
[96] Amnesty International (2020). *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance.* Retrieved from https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/, 17 March 2022.
[97] Liberty. (2022). *Resist facial recognition.* Retrieved from https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/, 18 March.2022.
[98] Electronic Frontier Foundation. (2017). *Street-level surveillance: Face recognition*. Retrieved from https://www.eff.org/pages/face-recognition, 03 February 2022.
[99] Bragias, A., Hine, K., Fleet, R. (2021). 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice & Research,* 22 (6), 1650.
[100] Bromberg, D. E., Charbonneau, E., Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly*, 37 (1), 1–8.

2.3.1. Police body cameras

Police body-worn cameras (BWC) are widely used a across the world. These are basically wearable little cameras, which are attached to police uniform to record audio, video and/or photographic systems that are used by police officers, to record any events that law enforcement officers are involved in. BWC were originally designed to record patrol activities, their interactions with suspects, and communication with members of the general public in order to increase transparency of police work and decrease the possible misconduct.[101]

Although BWC can also be used without the facial recognition technology, it is more advanced, when FRT software is integrated into BWCs, then the faces can be scanned, analysed, and categorized in real-time, but possibly without the consent or even knowledge of the person who is being recorded.[102] The author elaborates that the use of FRT in BWCs without any knowledge of the subject causes serious privacy concerns since persons biometric and therefore private data is compromised.

These privacy concerns have been indicated by many scholars, like Ringrose, who has explained that when the FRT is incorporated into body worn cameras, it presents a myriad of potential constitutional issues and negative effects.[103] Hood continues: "[...] not all facial recognition systems are designed to be hidden, but in the case of live or post-facto use with BWCs, embedding this technology within existing surveillance systems presents specific concerns related to privacy, consent, and bodily autonomy."[104]

Axon (formerly Taser International), a major police body camera manufacturer, has established their own AI Ethics Board and published the first report, concluded that the deployment of facial recognition technology in police body cameras should be stopped until such technology performs better accuracy and "equally well across races, ethnicities, genders, and other identity groups"[105].

[101] Hood, J. (2020). Making the body electric: The politics of body-worn cameras and facial recognition in the United States. *Surveillance & Society,* 18 (2), 161.
[102] *Ibid*, 163.
[103] Ringrose, K. (2019). Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. Virginia Law Review Online, 105, 62.
[104] Hood, J. (2020). *Supra nota* 96, 165.
[105] Axon Enterprise. (2019). *First Report of the Axon AI & Policing Technology Ethics Board.* Retrieved from https://www.policingproject.org/s/Axon_Ethics_Board_First_Report.pd, 15 March 2022.

Crow et al.[106] found that perceptions of police performance (an aspect of trust) and privacy concerns predicted views of the 'benefits' of police body-worn cameras (as measured by questions such as "Body-worn cameras will improve police officer behaviour during interactions with residents"[107].

Bromberg et al.'s used a survey to examine public perceptions of the use of FRT by police, specifically examining FRT within body-worn cameras. Their research acknowledged how nuanced public support is, reliant on the type and manner of surveillance such as whether it is used in real-time or after the fact, as well as the demographic surveyed within the sample.[108]

The author acknowledges that while the use of BWC might make police officers work more efficient and accordance with law, it can also be, that the use of BWC can give them more room for interpretation, since they only rely on the evidence that are caught on camera and maybe not seeing what's behind the "scenes".

2.4. FRT and Covid-19

On 31.12.2019 World Health Organisation (WHO) learned about a new disease, that is caused by coronavirus called SARS-CoV-2, commonly known as Covid-19, that started out from Wuhan, People´s Republic of China.[109] Since the most common symptom of Covid-19 is dry cough, the WHO advised people to wear face masks to control and limit the spread of the virus. This advice was quickly accepted by most countries of the world, making the mask wearing mandatory preventive measure for all adults and older children.

Although facial recognition is meant to be used to identify people using their facial features, the face masks, that people were forced to wear since the outbreak of Covid-19, covered half of a face,

[106] Crow, M. S., Snyder, J. A., Critchlow, V. J., Smykla, J. O. (2017). Community Perceptions of Police Body-Worn Cameras: The Impact of Views on Fairness, Fear, Performance, and Privacy. *Criminal Justice and Behavior*, 44, 589–610.
[107] Bradford, B., Yesberg, J.A., Jackson, J., Dawson, P. (2020). *Supra nota* 93, 1516.
[108] Bromberg, D. E., Charbonneau, E., Smith, A. (2018). Body-worn cameras and policing: A list experiment of citizen overt and true support. *Public Administration Review*, 78 (6); Bromberg, D. E., Charbonneau, E., Smith, A. (2020). *Supra nota* 100.
[109] World Health Organization. *Coronavirus disease (Covid-19)*. WHO official website. Retrieved from https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19, 13 April 2022.

therefore interfering the use of FRT.[110] But since FRT was seen as one of the tools to help fight the virus,[111] new algorithms that recognises a person even if they wear a mask, were created, to overcome this obstacle.[112] Many new digital systems, like the contact management software (e.g., the WHO-provided Go.Data), were developed and adopted in order to control the spread of the virus or to track persons that might have been in contact with the it (e.g., mobile contact tracing applications) and these new systems have attracted the attention of the public administration, private enterprises, and research institutions all over the world.[113] Many of these novel systems have incorporated biometric technologies and also facial recognition, in order to check people's temperature or to identify and recognize people even if they are wearing protective masks.[114] It has been indicated that the FRT systems work with same performance for differentiating people with and without a face mask.[115]

Research done by L.F.M Ramos indicates that during Covid-19 pandemic there were many countries (China, France, Israel, Poland, Singapore, South Korea, and Russia) that used different FRT systems but the information that was available about the analysed systems, showed that in most of these countries the necessary safeguards that were supposed to protect people´s privacy was not always considered.[116] The research also indicates that measures, that had to guarantee that the personal data collected was used only to control the spread of Covid-19 and not for additional law enforcement and national security purposes, were not clear and provided no assurance that appropriate risks assessments were adopted.[117]

Since it was not clear which measures were used to protect the data that was collected during Covid-19, there were growing concerns that when coronavirus passes, this data could be misused. The author agrees that the lack of adequate regulations does not provide the certainty that

[110] Ziccardi, S., Crescenzo, F., Calabrese, M. (2022). "What Is Hidden behind the Mask?" Facial Emotion Recognition at the Time of COVID-19 Pandemic in Cognitively Normal Multiple Sclerosis Patients. *Diagnostics (Basel), 12*(47), 1.
[111] Chochia, A., Nässi, T. (2021). *Supra nota* 1, 5.
[112] Talahua, J.S., Buele, J., Calvopiña, P., Varela-Aldás, J. (2021). Facial Recognition System for People with and without Face Mask in Times of the COVID-19 Pandemic. *Sustainability*, 13, 6900.
[113] Ramos, L.F. (2020). Evaluating privacy during the COVID-19 public health emergency: the case of facial recogntion technologies. *In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. Association for Computing Machinery, New York*, 176.
[114] Ring, T. (2020). Face ID Firms Battle Covid-19 as Users Shun Fingerprinting. *Biometric Technology Today*, 4.
[115] Talahua, J.S., Buele, J., Calvopiña, P., Varela-Aldás, J. (2021). *Supra nota* 112, 16.
[116] Ramos, L.F. (2020*). Supra nota* 113, 176.
[117] *Ibid*, 178.

governments will restrict their measures, particularly if there is no specific legislation establishing the rules on the processing, storing, or discarding the collected data.[118]

Fortunately in order to mitigate the risks, the European Commission issued guidelines for apps supporting the fight against Covid-19 pandemic in relation to data protection.[119] Also the European Data Protection Board (EDPB) published some guidelines on the use of location data, contact tracing tools, and the processing of personal data.[120] Ramos implies and the author agrees that these two documents provide valuable insights for facial recognition systems and a well needed recommendations for this long emergency period.[121]

The Human Rights Watch, together with numerous other organizations, has issued a joint statement, indicating some conditions that technology-assisted measures to fight the Covid-19 pandemic should present, so that these respect human rights.[122]

The author agrees that although FRT is widely used in different fields and can be considered as a good tool to fight and control pandemics and provides better solutions to help healthcare system, many researchers have pointed out existing gaps of such technology and, consequently, to unsatisfactory results.[123]

[118] *Ibid*, 178.
[119] E-Health Network. (2020). *Mobile Applications to Support Contact Tracing in the Eu's Fight against COVID-19.* Retrieved from https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf, 17 April 2022.
[120] European Data Protection Board. (2020). *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak*; European Data Protection Board. (2020*) Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.* Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, 17 April 2022.
[121] Ramos, L.F. (2020). *Supra nota* 113, 178.
[122] Human Rights Watch. (2020). *Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights*. Retrieved from https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight, 16 March 2022.
[123] Chochia, A., Nässi, T. (2021). *Supra nota* 1, 5-6.

3. ESTONIAN AUTOMATIC BIOMETRIC IDENTIFICATION SYSTEM DATABASE

Saxena and Varshney have said: "Security and privacy are important for every single individual. Having a local database of identified people helps with both security and privacy."[124]

Estonian Government is currently establishing an automatic biometric identification system database – ABIS, which should help the better protection of biometric personal data processing, crimefighting and better law implementation including the collection of evidence in offence proceedings. Biometric data collecting is nothing new in Estonia, but the data that is collected today during various state procedures, is stored today in ten separate databases, all for their own specific purpose (for example the identity documents database, national fingerprint registry, visa registry, etc.) The ABIS database would be an enhancement and would collect all this data into one system.

The current chapter will provide some overview of the development of a new database and the legal issues that have aroused by that, the author will also compare this database to others that have been used for a long time and will look into the idea of a new EU database.

3.1. Overview of ABIS

The decision to create the ABIS database was made in 2017. The development project is led by the Police and Border Guard Board, and the IT and Development Centre of the Ministry of the Interior is responsible for the development and management of the system. The state's partners in the acquisition and development of ABIS are IDEMIA and Cybernetica AS. The Police and Border Guard Board, the Estonian Forensic Science Institute and the Ministry of Foreign Affairs will be the controllers and main users of the database. The ABIS database will be implemented step by

[124] Saxena, N., Varshney, D. (2021). Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks. *International Journal of Cognitive Computing in Engineering*, 2, 155.

step – in 2021, the ABIS modality was implemented for conducting forensic examinations in offence proceedings, and in the first quarter of 2022, ABIS will be introduced for providing support in administrative proceedings.[125]

The ABIS database is based on the principle of minimum processing of biometric data – as little processing as possible and as much as necessary to achieve the purpose of the procedure. And in order to ensure security more effectively, including the prevention of double identities, the prevention of crime, the collection of evidence in criminal proceedings and other possible additional uses, it is also necessary to continuously update the solutions for identification and verification of identity, including electronic identification and verification of identity.[126]

The database is meant to provide a higher level of assurance that people really are who they claim to be.[127] The ABIS database will store biometric data like facial images, fingerprints and palmprints but won´t include people´s biographic data like name, date of birth, personal ID code, citizenship, etc. This should ensure the better protection of data, since the person´s biographic data is in a separate database and the biometric data can be connected to specific person´s identity only if investigator has access to both databases.

The lawmakers have indicated that the data in the ABIS database will be processed in accordance with all the data protection principles, ensuring the lawful and transparent use of the data which can only be accessed by officials who have a legal basis or are authorised to do so.[128] Although ABIS is also available to private sector, they can only use the data if identification of a person is needed, meaning that they interface with ABIS via another database and can only do one-to-one comparison of the biometric data (e.g. the Money Laundering and Terrorist Financing Prevention Act § 31 (5)[129]), to determine if the person is, who he says he is.

As already mentioned, one of the ways that the database can be used, is by comparing biometric data using one-to-one method, meaning that biometric data are taken from the person and compared with his/her previous ABIS records. The data are not compared with those of other

[125] Estonian Ministry of the Interior. *Automated biometric identification system database – ABIS*. Official website. Retrieved from https://www.siseministeerium.ee/en/activities/tohus-rahvastikuhaldus/abis, 1 March 2022.
[126] Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, 11. Retrieved from https://eelnoud.valitsus.ee/main/mount/docList/739ee44b-9df3-47b3-94c8-5f7ae3e1b559#44WhXv4z, 28 March 2022.
[127] Estonian Ministry of the Interior. *Supra nota* 125.
[128] *Ibid.*
[129] Money Laundering and Terrorist Financing Prevention Act, RT I, 02.06.2021, 10.

persons. Another method is the one-to-many comparison, which identifies the person, i.e. identifies, who the person is. This is done by taking biometric data from the person and comparing them with other data available in ABIS. In response, the ABIS provides a specific set of similar candidate prints or facial images, on which basis an expert makes a decision on the data match. One-to-many comparisons allow, for example, to identify a deceased person, whose identity is unknown. The one-to-one comparison is always made first since it is less intrusive. Only if this fails, a one-to-many comparison can be used.[130]

The biometric data that is stored in ABIS, is not allowed by current law to be used for automatic comparison by public cameras in real time. The author agrees that this would be a very intense interference with fundamental rights and would require a clear mandate. According to Section 34 of the Law Enforcement Act[131], the police or, in the cases provided for by law, another law enforcement agency, may use surveillance equipment in public places for ascertaining and countering a threat or for eliminating a disturbance. However, identity may be established only with the person's knowledge. Identification by means of public cameras is therefore not permitted.[132]

According to the Ministry of Interior, a person has no right to demand his data to be removed from ABIS, but they do have a right to check, who, and for what purpose has looked, used, or erased their data. This information can be requested from the holder of the database, Police and Border Guard Board.[133]

3.1.1. Legal grounds of ABIS

According to the legislators ABIS complies with applicable international and European Union law, including the Charter of Fundamental Rights, the GDPR, the Law Enforcement Authorities Directive and other relevant EU legislation, and the restrictions arising therefrom. The legal basis for the collection of biometric data is set out in GDPR Article 9(2) point (g), which allows processing, where it is necessary, for reasons of substantial public interest under Union or Member State law, where it is proportionate to the aim to be achieved and respects the essence of the right to the protection of personal

[130] Estonian Ministry of the Interior. *Supra nota* 125.
[131] Law Enforcement Act, RT I, 03.03.2021, 5.
[132] Estonian Ministry of the Interior. *Supra nota* 125.
[133] *Ibid.*

data, and where appropriate and specific measures are taken to safeguard the fundamental rights and interests of the data subject.[134]

In the explanatory memorandum of the so-called ABIS law[135] it is elaborated: "The protection of personal data is part of everyone's constitutional right to family and private life. State authorities, local authorities and their officials may not interfere in the family or private life of any person except in cases and in accordance with the procedure laid down by law, in order to protect health, morals, public order or the rights and freedoms of others, to prevent crime or to apprehend a criminal (§ 26 of the Constitution[136]). The purpose, scope and manner of the processing of data in ABIS are precisely and clearly set out in the draft." [137]

Nevertheless, when the process of changing the legislations, to develop the new database, was still ongoing, several Ministries and lawyers raised concerns about the invasion of privacy and indicated that the implementation of the draft bill might conflict with obligations under the European Convention on Human Rights (ECHR) and the case law of the European Court of Human Rights (ECtHR).

3.1.2. Possible infringement on human rights

The Ministry of Foreign Affairs, for example, referenced in their letter of agreement that under the GDPR, personal data of a kind which are by their nature particularly sensitive and include biometric data, deserve special protection because the context in which they are processed may present a substantial risk to fundamental rights and freedoms. They also indicate that ECtHR also considers the processing of biometric personal data to be an intensive interference with a person's right to privacy, which is protected by Article 8 (right to respect for private and family life) of the ECHR. The granting of the power to adopt legislation on data retention and deletion to the executive is questionable, as the processing of biometric personal data is an intensive interference with a person's rights. Ministry also elaborates that some of the most important questions have been left open, like the term "biometric data" which is still not clearly defined in the level of the law or has been defined differently in the laws. They

[134] *Ibid.*
[135] Act Amending the Law on Identity Documents and Amending Other Related Acts, RT I, 08.07.2021, 1.
[136] The Constitution of the Republic of Estonia, RT I, 15.05.2015, 2.
[137] Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. *Supra nota* 126, 55.

are convinced that the main regulations of the ABIS, like the composition of the data or the retention period, must be determined in the law and not only in the ABIS statute[138].[139]

Ministry elaborates, that same ideas are also confirmed by the Data Protection Inspectorate's Guide on Databases[140], as it explains that the need to lay down at the level of the law the content and scope of the processing of personal data depends on the intensity of the interference with fundamental rights, both in the case of a database and for other public information.[141]

The author agrees that the composition of the data is and should stay in the level of law to better protect data processing, but unfortunately when looking at the statute, this proposal has not been considered and the term "biometric data" has also not been defined in detail neither in the ABIS law or in the statute. Data Protection Inspectorate has also expressed, that the deprivation of a person's fundamental rights and the imposition of obligations must result from the laws, since the processing of personal data is a violation of fundamental rights and freedoms, as it affects both family and private life privacy and the freedom of informational self-expression (§ 26 and 19 of the Constitution).[142]

Constitutional law expert and University of Tartu lecturer Paloma Krõõt Tupay has said that there is always a violation of a person's fundamental rights in the case of such databases and their permissibility. She pointed out that even though the police can still legally and under certain conditions use a photograph and fingerprints given in a passport application in criminal proceedings, people may not be aware of the possible violation of their rights. She acknowledges that it is not always understandable, on what legal grounds and for what purposes people's data can be cross-used in today´s e-government.[143]

Lawyer Paul Keres has also found that such cross-use of data can be problematic. He elaborates that while people give away their data in one procedure, for example to get a passport, it can be used in a criminal procedure later, but in those proceedings the principle is that the person has no legal obligation

[138] Statutes of the Automated Biometric Identification System database, RT I, 31.12.2021, 18.
[139] Välisministeerium. (2020). *Isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise seaduse eelnõu kooskõlastus.* Retrieved from https://eelnoud.valitsus.ee/main#6PBGFIzy, 12 March 2022.
[140] Andmekaitse Inspektsioon. (2013). *Andmekogude juhend*. Retrieved from www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf , 12 March 2022.
[141] Välisministeerium. (2020). *Supra nota* 139.
[142] Andmekaitse Inspektsioon. (2013). *Supra nota* 140.
[143] Sarv, H. (2021). *Õiguseksperdid näevad probleemi ABIS-e info ristkasutuses*. Retrieved from https://www.err.ee/1608247482/oiguseksperdid-naevad-probleemi-abis-e-info-ristkasutuses, 15 March 2022.

to share any data with the state. "If the state has previously obtained this data from somewhere and now has a direct connection to this data and can collect this data, then it can be said that this privilege against self-incrimination has been circumvented by a small fraud," Keres said.[144]

3.2. Other databases collecting facial images

There are many databases used worldwide, where different kind of biometric data is collected. While governments collect the data to protect and provide services to their citizens, private companies have also started their own databases, some to track their costumers, others to keep an eye on their employees.

When talking about the facial recognition databases, one of the biggest is a company called Clearview AI, that claim they are "The World´s Largest Facial Network"[145]. They have created a research tool, that is used by law enforcement agencies to identify perpetrators and victims of crimes. They provide their service worldwide and their facial recognition database has 20+ billions of facial images, which they have allegedly collected from open web searches (including news media, mugshot websites, public social media, and other open sources). The database can be used by analysts, who can compare the uploaded crime scene images with publicly available images in the database. In the recent news, it is stated that the Clearview AI´s facial recognition has now been used in Ukraine during the war.[146]

The European Data Protection Board has raised concerns about the Clearview AI, regarding certain developments in facial recognition technologies and has said: "The EDPB has doubts as to whether any Union or Member State law provides a legal basis for using a service such as offered by Clearview AI. […] The EDPB is therefore of the opinion that the use of Clearview AI services by law enforcement authorities in the EU would, as it stands, likely not be consistent with the EU data protection regime."[147]

---

[144] *Ibid.*
[145] Clearview AI. Official website. Retrieved from: https://www.clearview.ai/, 13 March 2022.
[146] Dave, P., Dastin, J. (2022). *Exclusive: Ukraine has started using Clearview AI's facial recognition during war.* Retrieved from https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/, 24 March 2022.
[147] EDPB. (2020). *Response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI*. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, 24 March 2022.

Another big database is FaceFind, developed by Russian origin company NTechLab, who claims that "it is the first in speed and accuracy when it comes to detecting and identifying people in the video stream […] it´s capable of performing a split-second search across a multibillion database".[148] This database has also claimed to pose serious threat to the privacy.[149]

The USA´s Federal Bureau of Investigation's (FBI) facial recognition database has allegedly over 640 million photos of mostly US citizens, including driver´s licence photos from 21 US states. But what is startling, is that FBI claims, that they can use FRT on individuals without a warrant or a probable cause.[150]

Compared to the Estonian ABIS database, these global databases contain biometric data, which in many cases are collected from open media, making the data not as trustworthy as it should be. The Estonian ABIS database is designed to collect and store information that has been collected through legal procedures, and this provides assurance that the collected data is authentic and dependable, the individual is aware that the data is collected, used and stored and person can always request feedback on the use of the data.

3.3. Common database for Europe

In May 2019, in the provisions of Regulation 2019/817 establishing a framework for interoperability between EU information systems in the field of borders and visa[151], the European Commission has announced that a shared biometric matching service (shared BMS) among with some others, should be established.[152] It will replace the different central systems that are used today and should regroup and store these biometric templates in one single location, allowing cross-system comparisons.[153]

[148] NtechLab official website. Retrieved from https://ntechlab.com/about/, 24 March 2022.
[149] Sanders, L. IV. (2016). *When citizens spy: Russia´s FindFace sparks privacy controversy*. Retrieved from https://www.dw.com/en/when-citizens-spy-russias-findface-sparks-privacy-controversy/a-19232491, 23 March 2022.
[150] Guliani, N.S. (2019). *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database.* Retrieved from https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through, 21 March 2022.
[151] Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa. OJ L 135, 22.5.2019.
[152] *Ibid*, recital 9.
[153] *Ibid*, recital 18.

The European Data Protection Supervisor (EDPS) has stated in its opinion to the establishing a framework for interoperability between EU large-scale information systems, that they understand the need for the best possible tools to quickly identify the perpetrators of terrorist acts and other serious crimes, but they emphasise, that "facilitating the access by law enforcement authorities to non-law enforcement systems, even to a limited extent, is far from insignificant from a fundamental rights perspective. Routine access would indeed represent a serious violation of the principle of purpose limitation." With this the EDPS "stresses the importance of first further clarifying the extent of the problem of identity fraud among third-country nationals so as to ensure that the measure proposed is appropriate and proportionate."[154]

When comparing existing worldwide databases to the Estonian ABIS database, which is still under development, it seems, that the privacy in the Estonian database will be better protected because the possible safeguards have already been considered and established and live-FRT is prohibited, making the whole database more "human-friendly".

[154] European Data Protection Supervisor. (2018). *Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.* 2018/C 233/12. Retrieved from https://edps.europa.eu/sites/edp/files/publication/18-04-16_opinion_interoperability_executive_summary_en.pdf, 29 March 2022.

4. IS FRT VIOLATING PRIVACY?

Both the public usage of FRT and the police use of it raise privacy concerns. Although biometrics and in particular facial recognition technology has potential to bring enormous benefits, such as crime prevention and finding missing people, the benefits must be sufficiently great so as to justify any interference with other rights.[155] With all its potential benefits, FRT can also pose serious challenges to the right for privacy and data security. It creates problems of unwanted identification, discrimination, and the hacking of large datasets of not only faces, but also all the data that has been associated with those faces.[156] But what are more important: the personal rights of people or the rights of a law enforcement, when using novel technology, such as FRT?

The EU Agency for Fundamental Rights (FRA) has conducted a study on the human rights issues related to the live FRT, focusing on its use for law enforcement and border-management purposes, an emphasis that "a clear and sufficiently detailed legal framework must regulate the deployment and use of facial recognition technologies", but it does not provide any specific legal regulations.[157] European Commission's White Paper on AI addresses the issue of remote biometric identification and indicates, that it carries specific risks for fundamental rights, but again, no additional guidelines are given.[158]

Although there are many fundamental rights that might be interfered with by the use of facial recognition technology, in the current thesis the author focuses on the right to privacy. Sharon Naker and Dov Greenbaum have said: "Privacy is a precondition for the democracy development and freedom. Without privacy there is no freedom of speech, freedom of religion or freedom of movement."[159]

[155] Bu, Q. (2021). *Supra nota* 53, 135.
[156] Naker, S., Greenbaum, D. (2017). *Supra nota* 5, 122.
[157] European Union Agency for Fundamental Rights (FRA). (2019). *Supra nota 86*.
[158] European Commission. (2020). *White Paper on Artificial Intelligence - A European approach to excellence and trust.* COM(2020) 65 final. Retrieved from https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, 12 March 2022.
[159] Naker, S., Greenbaum, D. (2017). *Supra nota* 5, 101.

In this chapter, the author discusses the potential privacy violations caused by the use of facial recognition technology.

4.1. Current legislation on right to privacy

Protection of privacy and citizens right to personal and family life is guaranteed not only in the constitutional acts of most countries of the world, but also in most human right instruments, including, for example, the Universal Declaration of Human Rights (UDHR)[160] (Article 12 states that "no one shall be subjected to arbitrary interference with his privacy"), the International Covenant on Civil and Political Rights[161] (Art. 17: (a) "No one shall be subjected to arbitrary or unlawful interference with his privacy [...](b) Everyone has the right to the protection of the law against such interference or attacks"), the European Convention for the Protection of Human Rights and Fundamental Freedoms[162] and the Charter of Fundamental Rights of the European Union.[163] This shows that privacy is universally accepted at the international level.

It is acknowledged that the Human Rights legislation is considered more holistic, as it offers frameworks for consideration of law enforcement versus individual rights in the rollout considerations for FRT. These legislations enshrine principles of equality and inclusion but also privacy and rights to fair legal processes.[164]

While there are many legislations that state that right to privacy is essential, there still is no standardised human rights framework or specific requirements that can be easily applied to FRT.[165] This already indicates that legislators should regulate how this fast-growing industry should be deployed in public without the intrusion of privacy.

Steinacker et al. discovered in their 2020 research, that although some of US Governments have banned the use of FRT by city and state agencies, there is currently no federal legislative consensus

[160] Universal Declaration of Human Rights (adopted by the UN General Assembly on 10.12.1948).
[161] International Covenant on Civil and Political Rights (Adopted on December 16, 1966 by Resolution 2200 (XXI) at the 1496th plenary meeting of the UN General Assembly).
[162] Convention for the Protection of Human Rights and Fundamental Freedoms (Concluded in Rome 04.11.1950), article 8.
[163] Charter of Fundamental Rights of the European Union, 2012/C 326/02, article 7 and 8.
[164] Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). *Supra nota* 2, 6.
[165] *Ibid*, 1.

despite the extensive activism for regulation. Neither has the European Commission nor any of the EU Member states explicitly ruled on FRT.[166]

4.2. Right to privacy

In 1890, Warren and Brandeis defined the right to privacy as the right to "be let alone" and stressed that this was essential because invading a man's privacy "subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury".[167] The right to privacy can be understood as the right of everyone to self-determination, to live according to his or her wishes and desires with a minimum of external interference, to control information about himself or herself and to be protected from private interference.[168] Bellin elaborates that "Modern "privacy" objections often mask worries about abuse of power, not the inability to prevent disclosure of information about ourselves"[169] and continues: "Although the term "privacy" is invariably invoked when the government considers new technologies, the common thread in most modern critiques is abuse of power."[170] Clarke, for example, suggests that people should avoid using privacy as a right, and rather think of it as an "interest that individuals have in sustaining personal space, free from interference by other people and organizations".[171]

Naker and Greenbaum have emphasised: "The tension between the technology and the right to privacy highlight the dialectic between national security and law enforcement, economic efficiency or public health promoted through the application of facial recognition systems, on the one side, and concerns relating to the potential for disproportionately violating fundamental principles on our society such as the right to personal autonomy, anonymity, to be forgotten, to control one's own personal identifying information, and the person right to protect its own human body, on the other."[172]

Researchers have raised the issues over privacy violations before. For example, Christopher S. Milligan has stated that although there are constitutional issues that are debated, there are also

[166] Steinacker, L., Meckel, M, Kostka, G., Borth, D. (2020). Facial Recognition: A cross-national Suvery on Public Acceptance, Privacy, and Discrimination, *Law and ML Workshop*, 1.
[167] Warren, S.D., Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4 (5), 205.
[168] Maruste, R. (2004). *Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse.* Tallinn: Juura, 429.
[169] Bellin, J. (2021). Pure privacy. *Northwestern University Law Review,* 116 (2), 507.
[170] *Ibid*.
[171] Clarke, R. (1999). Internet privacy concerns confirm the case for intervention, *Commun. ACM,* 42 (2), 60–67.
[172] Naker, S., Greenbaum, D. (2017). *Supra nota* 5, 100.

social and even ethical issues that need to be considered and discussed when using video surveillance and facial recognition. The author agrees that the questions of whether people agree to live their lives under the watchful lens of a camera is much more extent, people also have to consider if they are willing to sacrifice their personal autonomy and risk having their data being abused in order to have the sense of safety and order, that video surveillance is meant to provide.[173] Milligan also emphasises that by using video surveillance with facial recognition software, it eliminates some amount of personal privacy and anonymity, that is expected.[174] The author agrees that while individuals expect privacy in the comfort of their homes, there is also reasonable expectation of privacy in public areas as well.[175]

Q. Bu has stated that FRT violates the "essential core of privacy" and is a threat to fundamental rights.[176] Jennifer Lynch also explains that biometrics programs that collect, store, share and combine sensitive and unique data, just like FRT does, poses critical threats both to privacy as well as civil liberties.[177] Brenda Leong, director of strategy at Future of privacy Forum, elaborates that when considering where, how and for what purpose the facial recognition systems is used, even exceed the boundaries of traditional privacy considerations.[178]

Hirose specifically explored the public's right to privacy in public spaces. He acknowledges that facial recognition surveillance, like these forms of more intrusive surveillance, crosses the boundaries of socially acceptable behaviour in public.[179]

The author agrees that the lack of precise regulation that explains and controls the specifics on the collecting, using, and storing such a sensitive data, as the biometrics and facial images, is desperately needed. The GDPR has offered some perspective into the subject but it´s still not efficient enough to provide all the safeguards that are expected. Addition to the privacy aspect there are also several other concerns that need to be considered – like the actual accuracy of the system and the fear of the system being misused.

[173] Milligan, C. S. (1999). *Supra nota* 65, 299.
[174] *Ibid*, 326.
[175] *Ibid*, 319.
[176] Bu, Q. (2021). *Supra nota* 53, 138.
[177] Lynch, J. (2012). *Supra nota* 58, 2.
[178] Leong, B. (2019). Facial recognition and the future of privacy: I always feel like … somebody's watching me, *Bulletin of the Atomic Scientists*, 75 (3), 113.
[179] Hirose, M. (2017). Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology. *Connecticut Law Review*, 49 (5).

4.3. Major concerns raised by facial recognition

As already mentioned, there are many concerns, that people have, when they realise that facial recognition technology has been or will be used.

Perhaps one the biggest privacy concern with facial recognition is that "Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the Government buildings you enter, and the photos your friends post online."[180]

The author feels that this concern is a bit extreme, since any facial image, which is received when using the FRT, does not automatically reveal the identity of a person. But the fear might still exist, because regular people are unaware, how the technology works. Also, the specific purpose of the use of this technology is not something, that is known to everyone. Another concern, that "someone is always watching", must also be explained. When using cameras in a public place for surveillance purposes, it should be elaborated, that the typical CCTV cameras do not always use facial recognition software along with it. If this was acknowledged to the public, maybe the fear of "being on camera" wouldn't seem so scary and people would know, that facial image received from public camera, does not contain a nametag. The principle on transparency and awareness-raising is also expressed in the GDPR – it elaborates, that the information about when and how facial recognition data are being collected, stored, and used must be made clear to the individuals. Bowyer has also expressed that, if people are notified that FRT is used, they can make a choice of whether or not to subject themselves to surveillance.[181] He continues: "If all airports install face recognition systems, then there may be little practical "choice" left for some travellers. However, given the level of screening already in place for passengers boarding an airplane, posing for a picture for a face recognition system would seem to be a rather minimal added inconvenience."[182]

Another concern that people seem to have is not that individuals can be identified, but the concern that the face itself has "been deprived of what we might have thought of as its distinctive claim".[183] Andrejevic and Volcic explain that people don't want to lose the way their face looks, when they

[180] Committee on the Judiciary. (2012). *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S.* 112th Cong 1-2. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf, 23 March 2022.
[181] Bowyer, K.W. (2004). *Supra nota* 7, 15.
[182] *Ibid.*
[183] Andrejevic, M., Volcic, Z. (2021). *Supra nota* 12, 356.

are seen by another human, who can respond with uniqueness and humanity, to a machine, that only sees a still image.[184]

The author finds this understandable, since we all want to be unique, one in a million, not just an image along hundreds, which may look similar and indistinguishable from others.

While there are many different types of biometric techniques that are used, FRT is still considered as more concerning, given the high degree of intrusion into privacy.[185] The author agrees, facial image is something no one wants just laying around and everyone to see, even if it is just for law enforcement purposes. If you give your fingerprints or iris, they cannot be connected to you by just looking at you, but when using facial image, person can possibly be recognised without any extra tests. When using FRT the privacy is invaded more deeply, because a face image might not only give away persons hair or eye colour, but it can also indicate the specifics of a person's background, like their race or nationality, or in some cases even their sexual orientation. As a series of experiments conducted at Carnegie Mellon University objectively concluded "If an individual's face on the street can be identified using a face recognizer and identified images from social network sites such as Facebook or Linkedin, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her."[186]

Zeng et al. have also summarized several controversies that may further lead to the risk of FRT misuse, additional to privacy and security, they mention bias.[187] K.M. Cannon also mentioned in her master´s thesis that: "The use of facial recognition technology, regardless of its intended purpose, has faced public scrutiny over the fact that it is inaccurate and racially biased."[188] Prof. Kosinski has focused in his research on how FRT can determine several characteristics of individuals and argues that even though FRT is often seen as a useful tool to improve human-technology interactions, it could also identify more sensitive data, such as political or sexual

[184] *Ibid.*
[185] Condliffe, J. (2017). *Facial recognition is getting incredibly powerful-and ever more controversial. MIT Technology Rev.* Retrieved from https://www.technologyreview.com/2017/09/08/149250/facial-recognition-is-getting-incredibly-powerful-and-ever-more-controversial/, 11 March 2022.
[186] Committee on the Judiciary. (2012). *Testimony of Professor Alessandro Acquisti from Carnegie Mellon University, What Facial Recognition Technology Means for Privacy and Civil Liberties*. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/12-7-18AcquistiTestimony.pdf, 23 March 2022.
[187] Zeng, Y., Lu, E., Sun, Y., Tian, R. (2019). Responsible facial recognition and beyond. *ArXiv:*1909, 12935.
[188] Cannon, K.M. (2019). *America´s panopticon: privacy implications of facial recognition by law enforcement.* (Master´s thesis). TalTech School of Information Technology, Tallinn, 39.

orientation or personality.[189] The author agrees that since facial recognition enables to see more than just facial features, like skin colour or ethnicity, it might automatically lead to prejudices about racial or behaviour patterns.

Another equally important concern and real threat to privacy is when using the FRT, the technology does not actually work. Although Bowyer explains that while FRT "cannot be simultaneously both a technology that does not work and one that presents a serious threat to privacy"[190], the author argues, that the two can coexist, because if the technology fails to work at the expected time, both law enforcement and ordinary people will be affected. For example, if FRT is used by law enforcement to identify criminals in crowded places, but the technology fails to detect them due to some technical flaw or malfunction, this failure to detect could be fatal to people, who believe they are in a safe place, because the use of the technology protects them and ensures their safety.

FRT can have a remarkably high rates of positive/false negatives and bias may lead to different types of discrimination against specific categories of populations.[191] There have been several indications about the threats that FRT poses to minorities or people of colour. Gender and race biases and discrimination issues against minorities are extensively discussed by Timnit Gebru.[192] In China, for example, the Government has announced that they are using a programme called "Sharp Eyes Project", meaning they are using public and private CCTV cameras all over China, to monitor the entire country, and not only CCTV cameras but also special TV boxes that are installed in people´s homes, so that local residents can watch live security footage even with smartphones.[193] But all these millions of cameras that are equipped with facial recognition software, that can be found everywhere, raise concerns among minorities, like the Uighurs population, who are being targeted and when detected, then alerted to the police.[194] Although an extreme example, it shows that FRT might not only have purpose of detecting criminals, but also interfering into lives of people with different religious beliefs and background. Fortunately, in Europe such a mass

[189] Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Sci Rep*, 11**(**100).
[190] Bowyer, K. (2004). *Supra nota* 7, 16.
[191] European Parliamentary Research Service (2021). *Supra nota* 46.
[192] Gebru, T. (2020). Race and gender. *The Oxford handbook of ethics of AI*, 251-269.
[193] Gershgorn, D. (2021). *China´s „Sharp Eyes" Program Aims to Surveil 100% of Public Space*. Retrieved from https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015, 26 March 2022.
[194] Bhuiyan, J. (2021). *Major camera company can sort people by race, alert police when it spots Uighurs*. Retrieved from https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur#:~:text=Facial%20recognition%20software%20developed%20by,the%20Turkic%20ethnic%20group%20Uighurs, 26 March 2022.

surveillance of people is not allowed – the ECtHR has ruled that UK laws that enabled mass surveillance had violated human rights, and more specifically the right to privacy protected by Article 8 of the ECHR.[195]

Additional to concerns that directly involve the use of facial recognition, there are also concerns, that arise, when the recognition process is already done. One of those situations is the possible data breaches, which might occur, when all the data is collected and stored. No matter how protected the data is, data breaches can still happen. Zeng et al. explain that "data breaches can also put victims at a considerable disadvantage, especially when considering the biometric information is almost permanent, and the consequences of the leak are severe and lasting."[196]

Additional to the fear of a data breach, there is also a developing field of face-swap and deepfake technologies, which are challenging for FRT systems, meaning that people are concerned that someone might be using their face image and will fool the FRT system.[197]

While FRT is becoming widespread, it gives the possibility to identify and track whoever goes to public, resulting in creating various new databases, which can be sold or shared, making it fragile and exposed to security breaches.[198] And even if there are no security concerns, the presence of FRT seriously damages regular people and their ability to maintain their anonymity in the public. And just like people have a right to be forgotten, the author agrees that people should also have the right to remain anonymous.[199]

4.4. Privacy vs security

As already indicated in the topic of the thesis and throughout this research, the conflict between the potential benefits of FRT and the possible violation of privacy exists. The author feels that even though the benefit on secure environment that the use of FRT provides for people in public places, cannot overweight the intrusion of privacy it causes, when the faces of every person in the public

[195] Big Brother Watch & Others v. The United Kingdom, applications nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021) §387 and §251.
[196] Zeng, Y., Lu, E., Sun, Y., Tian, R. (2019*). Supra nota* 187, 2.
[197] Pavel, K., Marcel, S. (2018). Deepfakes: A New Threat to Face Recognition? Assessment and Detection. *ArXiv Preprint, ArXiv:*1812,08685.
[198] Naker, S., Greenbaum, D. (2017). S*upra nota* 5, 109.
[199] *Ibid.*

area are scanned with automated or live FRT. The author understands, that although the use of FRT might make people feel secure, there is still possibility that the system does not work as expected and mistakes can happen, which means that the security is not providing enough benefit over privacy.

The author agrees that it is hardly justified to convert the question into a debate on whether economic well-being matters more or less than human rights,[200] and as expressed by Bu, whether any benefit of FRT overweighs the intrusion into people's privacy, or more specifically, whether it is worth sacrificing privacy and civil liberties.[201]

When talking about automated facial recognition, scholars have stated that it can be used either for beneficial or malicious purposes.[202] While it can enhance law enforcement capabilities and protect public safety, its detrimental effects should not be ignored, because it is an intrusive technology, that has potential to destroy people's privacy rights and by that also force individuals to change their behaviour.[203] The author agrees that when people acknowledge, that there is a camera observing, especially one, that uses automatic or live FRT, it might influence people to act differently (better or more friendly), since they might fear, that if they are watched and identified, not only their face but also their body language can give a wrong impression.

The author is in the opinion that while law enforcement officials use FRT for the specific purpose of providing security, and catch those, that might harm us, they must use FRT only, if the safeguards, that are important, are considered and appropriately applied. One of the necessary measures is described both in Article 32 of the GDPR and in Article 29 of the LED– it requires that Member States make sure to prevent personal data from being disclosed to unauthorised parties. This means, that while trying to protect people´s security, the collected data must be protected too.

The author discusses that the distinction between good and questionable intentions is very thin, which indicates that it must be clearly specified, who are the target groups, who are authorised to

[200] McCrudden, C. (2008). Human dignity and judicial interpretation of human rights. *Eur J Int Law* 19 (4).
[201] Bu, Q. (2021). *Supra nota* 53, 129.
[202] *Ibid,* 114.
[203] *Ibid,* 115

use this technology. To avoid situations where FRT is used by unauthorised persons, such regulations must be made. If the technology is in wrong hands, it can cause more harm than good.

When it comes to the acceptance of FRT, Bradford et al. research indicates that people who are concerned about crime, are more likely embracing new developments such as FRT, and are more accepting of it, believing that no matter the extent, the use of FRT will help make crimefighting more effective and simpler.[204] The author agrees, this is to be expected, because fear is a good motivator to accept new technologies in order to create something that can alleviate this fear.

The author believes, that until there are no proper guidelines, which consider the privacy aspect in FRT, the debate about the proper balance between privacy and public safety will continue to play out in the courts.[205]

Another illustration on the conflict between security and privacy is shown in the survey, done by German and Switzerland researchers. The survey indicated, that almost half of all German (48%) and US responders (44%) believes that FRT increases privacy violations, and majority of Germans (66%) and roughly half of UK and US responders believe that FRT increases surveillance.[206] More than half of every country's responders agreed, that FRT increases security. The author agrees with Chochia and Nässi, that the last one was expected, since most people feel secure, and do not consider the fact, that it might also invade their privacy, if they see a camera in public areas or for example in shops. People usually presume, that when a camera is watching their every move, it is there to protect them, like in cases when anything happens to them or their property, someone behind the camera, will notice in time and if needed, someone can help.[207] Steinacker et al. analysis showed that the "interpretation of privacy threat is a strong and significant negative predictor of acceptance" and elaborate, that the more a participant feels that their privacy is threatened by the technology, the less likely they are agree to the use FRT in a public place.[208]

[204] Bradford, B., Yesberg, J.A., Jackson, J., Dawson, P. (2020). S*upra nota* 93, 1505.
[205] Hamann, K., Smith, R. (2019). *Supra nota* 91.
[206] Steinacker, L., Meckel, M., Kostka, G., Borth, D. (2020). *Supra nota* 166, 5.
[207] Chochia, A., Nässi, T. (2021). *Supra nota* 1, 4.
[208] Steinacker, L., Meckel, M., Kostka, G., Borth, D. (2020). *Supra nota* 166, 5.

5. POSSIBLE SOLUTIONS ON HOW TO USE FRT WITHOUT VIOLATING THE RIGHT TO PRIVACY

Throughout this thesis, the author has been searching for an answer to the question whether the current EU regulations allow the use of facial recognition technology without violating the right to privacy. The short answer is "no", the current regulation does not provide specific guidelines on how to use the technology without the invasion of privacy and in most cases, when FRT is used, the breach is inevitable. When considering the rules provided in the GDPR for example, it is stated that the collection of data, including biometric data, that is essential also in FRT, is allowed, if the safeguards that are mentioned, are used. But the author believes that these safeguards are not specific enough and provide ways to disregard them, since they do not clearly state, to what extent these safeguards should be respected. Q. Bu has expressed: "Regarding the applicability of Article 8 of the ECHR on the right to respect for private life, a government may interfere with these rights if sufficiently justified by legality and necessity. It requires that personal data be processed only for specified purposes, which must be explicitly defined by law."[209]

The author suggests that the use of FRT must be hand in hand with the regulations, meaning that before using any innovative technology, which concerns people and their rights, there must be clear rules of when, where and to what purpose it is used for. This is also true for FRT. The same idea is clearly stated by the court when elaborating that the algorithms of the law must keep pace with new and emerging technologies.[210] Although it is mentioned, that FRT is designed to be used for good, it can cause serious breach of rights, when used by unauthorized persons or groups. The FRT system itself should be more stable and reliable, to be used more widely. There is no justification on the use of this technology, until there is no error rate, which is acceptable for the EU, is set.

The author feels that specific conditions that allow the use of this kind of emerging technology should be given in European Union level and not be left to decided country by country, since the privacy is meant to be accepted consistently and beyond countries borders. For example, in LED

[209] Bu, Q. (2021). *Supra nota* 53, 117.
[210] R (Bridges) v. Chief Constable of South Wales Police and Others [2019] EWHC 2341 (Admin).

article 5 it is suggested that in criminal cases Member States must provide the appropriate time limits for erasure of personal data and a periodic review of stored data, but the author believes that these time-limits must be set in European Union level, if not for all data, at least for the much more sensitive biometric data.

It is also essential to specify in EU level, what kind of facial recognition surveillance is acceptable and what is not. The author is in the opinion that the most controversial part of FRT is, that it can be used live or automatically, meaning that people´s motions can be detected real-time, and people can be identified anywhere, making the privacy issues even more critical. The author believes that live real-time monitoring violates privacy rights severely and should not be allowed in public areas. Live or automated FRT allows mass surveillance and matching live footage of individuals with images from the database. Such mass surveillance has a significant impact to privacy to the extent that it can affect any part of a person´s life. Automated FRT does not only show the facial image, but it might also expose political preference, social behaviour and much more. The author believes, that live or automated facial recognition can only be used in a controlled environment and for a very specific purpose, for example on borders and in airport security gates etc., where it is crucial to detect any misbehaviour or suspicious activity and keep an eye on the people that might cause trouble. In these situations, the tracking of people´s movements and activities can also help predict possible violations.

The same idea is stated in the European Commission´s proposal (draft AI Regulation) of 21.04.2021[211]. According to the Article 5 1.(d) the use of real-time remote biometric dentification systems (like the FRT) are prohibited in publicly accessible spaces for the purpose of law enforcement, unless such use is strictly necessary for at least one of the following objectives: the targeted search for specific potential victims of crime, including missing children; the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; or the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence and punishable by a custodial sentence or a detention order for a maximum period of at least three years.

[211] European Commission. (2021). 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 act. COM(2021) 206 final.

Some of the lawmakers have expressed that the use of facial recognition should be banned in specific contexts. For instance, the European Parliament has recommended banning automated biometric identification such as facial recognition for educational and cultural purposes (unless exceptionally allowed by law).[212] Following the same line of reasoning, a group of more than 100 Members of the European Parliament called on the European Commission to enshrine an explicit ban on biometric mass surveillance in public spaces in EU law.[213]

From a legal point of view the author thinks that big worldwide FRT databases that use pictures that are collected from social media (like the Clearview AI), are not acceptable. These pictures can reveal more than just one person, meaning that the identification of a specific person might not be accurate. As GDPR principles suggest, to process any sensitive data, a consent must be given, and even if a person posting the picture online, is happily sharing a picture to the world, it does not mean, that he/she wishes to be identified in public because of that picture. Also, if someone posts a picture in social media, the database presumably also collects these pictures and adds these pictures into their database as well, which means that any other person, that is captured on someone else's picture, might be added to the database, although they might not be even known that this kind of image of them exist, let alone is used to identify them.

The information that is stored in the database is also not always reliable, since there is no control over the social media and posts, which are collected – basically anyone, wishing to use a fake account, can post any picture and claim it is about them, making the connections between pictures and identification information questionable. The author also thinks that if a person discovers that their pictures have been added to the database, they should have a right to demand these images to be removed from databases, since the collection does not have any legal justification and a consent to use these pictures for identification purposes does not exist. Photos received from public platforms (just like images received from live-FRT) can reveal more than just information about the name and identity of an individual: social media photos can also provide information about person´s gender or emotional state, financial or health status, their religious or political beliefs and preferences – all this information is invading individuals' privacy.

[212] European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector, 2020/2017(INI).
[213] EDPB. (2021). *Supra nota* 147.

The author agrees that there is a real need to adopt binding laws on the matter.[214] The regulations should clearly indicate that the FRT database cannot include specific data about the person. Just like the right to be innocent until proven guilty, people should have to right to stay anonymous until proven guilty.

When talking about the cross-use of data, the author is on the opinion that if sensitive data is collected for a specific purpose, like making a document (when fingerprints, facial images are collected), it should be use for just this purpose and in other procedures the same data should not be used without a person's specific consent. The same ideas were pointed out in the making of Estonian database ABIS. The author suggests that when consenting to have their biometric data used, people should be able to decide, whether they allow their data to be used for other purposes or not. The author believes that a person should have a right to decide what consent they give – if the consent is given only to use this data for the same purpose as in the collection, the data should not be added in the common database and should be held separately. Person should also have a right to decide how long their consent is valid and take it back whenever they decide.

The author is of the opinion that the use of FRT is justified for specific purposes like for criminal investigations or finding missing people, but not to track regular people's daily routines or their life. FRT should work only to process facial images by comparing them, not to identify them.

As stated by both GDPR and LED[215] the personal data may only be processed for a precisely defined, explicit and legitimate purpose. The intended purpose must be formulated with sufficient precision that the person concerned may be able to envisage the purpose for which their data will be processed.[216]

Based on the foregoing, the author considers that additional to the safeguards that are supposedly protecting our rights, the person who´s data is used (data subject) must have a right to an effective remedy in case their rights are unduly violated for example if the data was collected without a consent. Such a right is well enshrined in the EU Charter of Fundamental Rights.[217]

[214] Caplier, M. (2021). *Supra nota* 3, 38.
[215] GDPR Article 5(1)(b) and LED Article 4(1)(b).
[216] Advocate-General J. Kokott Opinion in Case C-275/06, Promusicae, CJEU, 18 July 2007, para. 53.
[217] EU Charter of Fundamental Rights, Article 47.

Additional of having right to object the use of the data, a person should also have a right to know for what purpose their biometric data has been used, and if their data has been compared to someone else's data.

CONCLUSION

Every new emerging technology and the digitalisation process in general has an increasing impact on our daily lives. Facial recognition technology is being used worldwide in a variety of fields, for both public and private purposes. It is a tool to help us in our everyday lives, it can unlock phones and doors, but it is also a powerful instrument that can help prevent terrorism, find missing children, or track people. While facial recognition has its benefits, in the wrong hands and without supervision it can pose a serious threat to our fundamental right to privacy.

This thesis intends to contribute to the discussion on whether facial recognition technology has enough benefits to overrule its possible invasions to privacy, to determine whether and to what extent the use of this technology violates the right to privacy and how the law enforcement can use the FRT without violating the right to privacy?

After an extensive literature review the author can conclude that if facial recognition technology is used, there is a violation of right to privacy. Various sources and examples have indicated that when law enforcement uses FRT, there often really is a violation of human rights, since not all safeguards provided by the EU law, are considered, or these safeguards are not efficient enough. Author acknowledges that there is a lack of clear regulation of how, when and for what purpose FRT can be used, and until there is, the use of this technology should be on hold.

While the pioneers in the world to use FRT in every different field are USA and China, the EU has been a pioneer on trying to address these complicated issues related to widespread and rapidly growing usage of modern technologies, including FTR, by providing extensive documentation on this topic, like the European Parliamentary Research on regulating facial recognition in the EU[218] or the draft AI Regulation[219] and many other that are mentioned above. The draft AI Regulation provides harmonised rules, that are applicable to the design, development and use of certain high-risk AI systems, such as FRT, and restrictions on certain uses of remote biometric identification

[218] European Parliamentary Research Service (2021). *Supra nota* 46.
[219] European Commission (2021). *Supra nota* 211.

systems. The explanatory memorandum of the proposal elaborates, that it proposes a legal framework for trustworthy AI to ensure that AI systems (including FRT) that are placed and used on the Union market are safe ad respect the existing law on fundamental rights and Union values. By proposing solutions to a number of controversial problems, that arise from the use of AI systems and also categorizing the AI risks, this draft AI Regulation has made significant improvements to help legislators create acceptable rules for regulating AI systems.

The author summarises the above-mentioned recommendations and suggestions by proposing the following:

1. Legislators should clearly set out the rules on when, where and for what FRT can be used.
2. Safeguards need to be more specific, with clear indications of when and to what extent they are to be respected.
3. Regulation should include a distinction between how data is collected and how it is subsequently used.
4. An acceptable error rate for FRT should be set on EU level.
5. Real-time FRT should be prohibited in public areas, with exceptions set at EU level.
6. Definitions are needed for the use of FRT in real-time and for FRT in retrospect comparison.
7. Cross-use of data should be prohibited. (If sensitive data is collected for a specific purpose, it can be used for the same purpose). Exceptions should be developed at EU level.
8. Different categories of consent should be introduced – individual must have a right to decide whether to allow biometric data to be used for purposes other than those for which they were collected. If the consent is given only for the data to be used for the same purpose for which it was collected, the data should not be included in the common database and should be held separately.
9. The period of validity of consent should be established.
10. Databases using images from open sources or social media should be prohibited.
11. Regulations should clearly indicate that the FRT database must not contain personal data of a specific data subject.
12. Effective remedies should be put in place in cases where a person´s rights have been unduly infringed.

In conclusion, the author indicates that the world is not yet ready to make full use of facial recognition technology. The biometric information used for facial recognition is so delicate, that

there is a clear need for a specific and understandable regulation to help both the people who use it and those against whom it is used. Whenever facial recognition is used, the privacy of individuals must be safeguarded, especially when it is used by law enforcement authorities.

LIST OF REFERENCES

Scientific books

1. De Leeuw, K.M.M., Bergstra, J. (2007). *The History of Information Security: A Comprehensive Handbook*. Amsterdam: Elsevier.
2. Dubber, M.D., Pasquale, F., Das, S. (2020). *The Oxford Handbook of Ethics of AI.* Oxford: Oxford Handbooks.
3. Gates, K. (2011). *Our Biometric Future* (Critical cultural communication). New York: NYU Press.
4. Pato, J.N., Millett, L.I. (Eds.) (2010). *Biometric Recognition: Challenges and Opportunities*. Washington: National Academies Press.
5. Maruste, R. (2004). *Konstitutsionalism ning põhioiguste ja -vabaduste kaitse*. Tallinn: Juura.
6. Wilkinson C. (2004). *Forensic facial reconstruction*. Cambridge: University Press.

Scientific articles

7. AbdELminaam, D., Almansori, A., Taha, M., Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. *PloS One*, 15(12), 1-27.
8. Andrejevic, M., Volcic, Z. (2021). "Smart" Cameras and the Operational Enclosure. *Television & New Media,* 22(4), 343-359.
9. Arridge, S., Moss, J.P., Linney, A.D., James, D.R. (1985). Three dimensional digitisation of the face and skull. *J Maxillofac Surg*, 13(3), 136-143.
10. Bellin, J. (2021). Pure privacy. *Northwestern University Law Review,* 116(2), 463-514.
11. Bowyer, K. (2004). Face recognition technology: Security versus privacy. *IEEE Technology & Society Magazine*, 23(1), 9-19.
12. Bradford, B., Yesberg, J.A., Jackson, J., Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *British Journal of Criminology*, 60(6), 1502-1522.
13. Bragias, A., Hine, K., Fleet, R. (2021). 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice & Research,* 22(6), 1637-1654.
14. Bromberg, D. E., Charbonneau, E., Smith, A. (2018). Body-worn cameras and policing: A list experiment of citizen overt and true support. *Public Administration Review,* 78(6), 883–891.
15. Bromberg, D. E., Charbonneau, E., Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly*, 37(1), 1–8.

16. Bu, Q. (2021). The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, 2, 113–145.

17. Buckley, B., Hunter, M. (2011). Say Cheese! Privacy and facial recognition. *Computer Law and Security Review*, 27 (6), 637-640.

18. Caplier, M. (2021). Assessment of the European legal framework of facial recognition technology. *L'Europe Unie*, 17(17), 29-40.

19. Chochia, A., Nässi, T. (2021). Ethics and emerging technologies–facial recognition. *IDP: revista d'Internet, dret i política*, (34), 1-12.

20. Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Commun. ACM*, 42(2), 60–67.

21. Crow, M. S., Snyder, J. A., Critchlow, V. J., Smykla, J. O. (2017). Community Perceptions of Police Body-Worn Cameras: The Impact of Views on Fairness, Fear, Performance, and Privacy. *Criminal Justice and Behavior,* 44, 589–610.

22. De Greef, S., Willems, G. (2005). Three dimensional cranio-facial reconstruction in forensic identification: latest progress and new tendencies in the 21st century. *J Forensic Sci*; 50(1), 12-17.

23. Gebru, T. (2020). Race and gender. In *The Oxford handbook of ethics of AI.* 251-269.

24. Goldstein, A., Harmon, L., Lesk, A. (1971). Identification of human faces. *Proceedings of the IEEE*, 59(5), 748-760.

25. Haddad, G. M. (2021) Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom. *Vanderbilt Journal of Entertainment and Technology Law*, 23(4), 891-918.

26. Hamann, K., Smith, R. (2019). Facial recognition technology: where will it take us? *Crim Justice*, 34(1), 9–19.

27. Hirose, M. (2017). Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology. *Connecticut Law Review*, 49(5), 1591–1620.

28. Hood, J. (2020). Making the body electric: The politics of body-worn cameras and facial recognition in the United States. *Surveillance & Society*, 18(2), 157-169.

29. Introna, L.D., Nissenbaum, H. (2010). Facial Recognition Technology: A Survey of Policy and Implementation Issues, *The LUMS Working Paper Series. The Department of Organisation, Work and Technology*, 1-60.

30. Kirby, M., Sirovich, L. (1990). Application of the Karhunen-Loeve procedure for the characterization of human faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 12(1), 103-108.

31. Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific Reports*, 11(100), 1-8.

32. Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society*, 21(7), 1565–1593.

33. Kostka, G., Steinacker, L., Meckel, M. (2021). Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*, 30(6), 671-690.

34. Lai, X., Patrick Rau, P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior*, 124, 1-13.

35. Leong, B. (2019) Facial recognition and the future of privacy: I always feel like … somebody's watching me. *Bulletin of the Atomic Scientists*, 75(3), 109-115.

36. McCrudden, C. (2008). Human dignity and judicial interpretation of human rights. *Eur J Int Law*, 19(4), 655-724.

37. Milligan, C. S. (1999). Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal*, 9(1), 295-334.

38. Moss, J.P., Linney, A.D., Grindrod, S.R., Arridge, S.R., Clifton, J.S. (1987). Three-dimensional visualisation of the face and skull using computerised tomography and laser scanning techniques. *Eur J Orthod*, 9(4), 247-253.

39. Naker, S., Greenbaum, D. (2017). Now you see me: Now you still do: Facial recognition technology and the growing lack of privacy. *Boston University Journal of Science and Technology Law*, 23(1), 88-122.

40. Nelson L.A., Michael S.D. (1998) The application of volume deformation to 3D facial reconstruction: a comparison with previous techniques. *Forensic Science*, 94, 167-181.

41. Purshouse, J., Campbell, L. (2021). Automated facial recognition and policing: A Bridge too far*? Legal Studies*, 1-19.

42. Ring, T. (2020). Face ID Firms Battle Covid-19 as Users Shun Fingerprinting. *Biometric Technology Today*, 4, 1–2.

43. Ringrose, K. (2019). Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns. *Virginia Law Review Online*, 105, 57-66.

44. Rodrigues Silva Almeida, D., Shmarko, K., Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 1-11.

45. Saxena, N., Varshney, D. (2021). Smart Home Security Solutions using Facial Authentication and Speaker Recognition through Artificial Neural Networks. *International Journal of Cognitive Computing in Engineering*, 2, 154-164.

46. Spiesel, C. (2020). Technology's Black Mirror: Seeing, Machines, and Culture. *International Journal for the Semiotics of Law*, 35, 351-367.

47. Steinacker, L., Meckel, M, Kostka, G., Borth, D. (2020). Facial Recognition: A cross-national Suvery on Public Acceptance, Privacy, and Discrimination, *Law and ML Workshop*, 1-8.

48. Talahua, J.S., Buele, J., Calvopiña, P., Varela-Aldás, J. (2021). Facial Recognition System for People with and without Face Mask in Times of the COVID-19 Pandemic. *Sustainability*, 13(6900), 1-19.

49. Tene, O. (2011). Privacy: The new generations. *International Data Privacy Law*, 1(1), 15-27.

50. Turley, J. (2020). Anonymity, obscurity, and technology: Reconsidering privacy in the age of biometrics. *Boston University Law Review*, 100(6), 2179-2261.

51. Unar, J.A., Seng, W.C., Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*, 47(8), 2673–2688.

52. Verze, L. (2009). History of facial recognition, *Acta Biomed*, 80, 5-12.

53. Warren, S.D., Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5). 193–220.

54. Welinder, Y. (2012). A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. *Harvard Journal of Law and Technology*, 26(1), 166-237.

55. Whitelaw, S., Mamas, M. A., Topol, E., Van Spall, H. G. C. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, 2(8), e435–e440.

56. Zeng, Y., Lu, E., Sun, Y., Tian, R. (2019). Responsible facial recognition and beyond. *ArXiv*:1909.12935, 1-14.

57. Ziccardi, S., Crescenzo, F., Calabrese, M. (2022). "What Is Hidden behind the Mask?" Facial Emotion Recognition at the Time of COVID-19 Pandemic in Cognitively Normal Multiple Sclerosis Patients. *Diagnostics (Basel)*, 12(47), 1-14.

Estonian legislation

58. Act Amending the Law on Identity Documents and Amending Other Related Acts, RT I, 08.07.2021, 1.

59. Law Enforcement Act, RT I, 03.03.2021, 5.

60. Money Laundering and Terrorist Financing Prevention Act, RT I, 02.06.2021, 10.

61. Statutes of the Automated Biometric Identification System database, RT I, 31.12.2021, 18.

62. The Constitution of the Republic of Estonia, RT I, 15.05.2015, 2.

European Union and international legislation

63. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, 391–407.

64. Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950.

65. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016.

66. International Covenant on Civil and Political Rights (Adopted on December 16, 1966 by Resolution 2200 (XXI) at the 1496th plenary meeting of the UN General Assembly).

67. 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), OJ L 119, 4.5.2016, 1–88.

68. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa. OJ L 135, 22.5.2019.

69. Opinion 02/2012 on facial recognition in online and mobile services, Article 29 Data Protection Working Party, 2012 (00727/12/EN WP 192).

70. Universal Declaration of Human Rights. United Nations, 10.12.1948.

Court Decisions

71. Advocate-General J. Kokott Opinion in Case C-275/06, Promusicae, CJEU. 18 July 2007. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006CC0275, 14 March 2022.

72. European Court of Human Rights (2021). Big Brother Watch & Others v. The United Kingdom, applications nos. 58170/13, 62322/14 and 24960/15. Retrieved from https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}, 16 March 2022.

73. Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (9th Cir. 2019), 18-15982. Retrieved from https://epic.org/wp-content/uploads/amicus/bipa/patel-v-facebook/Patel-v-FB-9th-Cir-Opinion.pdf, 17 April 2022.

74. Royal Court of Justice (2019). R (Bridges) *vs.* CC South Wales & ors. EWCA Civ 1058, Case No: C1/2019/2670. Retrieved from https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf, 13 April 2022.

Other sources

75. Ada Lovelace Institute. (2019). *Beyond face value: Public attitudes to facial recognition technology*. Retrieved from https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf, 23 January 2022.

76. Amnesty International. (2020). *Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance*. Retrieved from https://www.amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance/, 17 May 2021.

77. Andmekaitse Inspektsioon. (2013). *Andmekogude juhend*. Retrieved from www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf, 12 March 2022.

78. Anscombe, L. (2017). *Westfield is using facial detection software to watch how you shop*. Retrieved from https://www.news.com.au/finance/business/retail/westfield-is-using-facial-detection-software-to-watch-howyou-shop/news-story/7d0653eb21fe1b07be51d508bfe46262, 14 March 2022.

79. Axon Enterprise. (2019). *First Report of the Axon AI & Policing Technology Ethics Board*. Retrieved from https://www.policingproject.org/s/Axon_Ethics_Board_First_Report.pd, 15 March 2022.

80. Bhuiyan, J. (2021). *Major camera company can sort people by race, alert police when it spots Uighurs*. Retrieved from https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur#:~:text=Facial%20recognition%20software%20developed%20by,the%20Turkic%20ethnic%20group%20Uighurs, 26 March 2022.

81. Bledsoe, W.W. (1966). Man-machine facial recognition: Report on a Large-Scale Experiment, Technical Report PRI 22, *Panoramic Research Inc.*, CA: Palo Alto.

82. Cannon, K.M. (2019). *America´s panopticon: privacy implications of facial recognition by law enforcement.* (Master´s thesis). TalTech School of Information Technology, Tallinn.

83. Clearview AI (n.d.). *Clearview AI official website*. Retrieved from https://clearview.ai, 13 March 2022.

84. Committee on the Judiciary. (2012). *Testimony of Professor Alessandro Acquisti from Carnegie Mellon University, What Facial Recognition Technology Means for Privacy and Civil Liberties*. Retrieved from https://www.judiciary.senate.gov/imo/media/doc/12-7-18AcquistiTestimony.pdf, 23 March 2022.

85. Committee on the Judiciary. (2012). *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the S. Subcomm. on Privacy Tech. and the Law of the S.* 112th Cong 1-2. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf, 23 March 2022.

86. Condliffe, J. (2017). *Facial recognition is getting incredibly powerful-and ever more controversial. MIT Technology Rev*. Retrieved from https://www.technologyreview.com/2017/09/08/149250/facial-recognition-is-getting-incredibly-powerful-and-ever-more-controversial/, 11 March 2022.

87. Council of Europe (2021). *Guidelines on facial recognition. Consultative committee of the Convention for the protection of individuals with regard to automatic processing of personal data*. Retrieved from https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3, 12 March 2022.

88. Chronicle, D. (2018). A*rtificial Intelligence Can Help Schools Safeguard Children.* Retrieved from https://www.asianage.com/technology/in-other-news/310518/artificial-intelligence-can-help-schools-safeguard-children.html, 23 March 2022.

89. Creed, S., Dixon, A. (2020*). Facial recognition technology in employment: What you need to know*. Retrieved from https://www.twobirds.com/en/insights/2020/global/facial-recognition-technology-in-employment, 11 March 2022.

90. Dave, P., Dastin, J. (2022). *Exclusive: Ukraine has started using Clearview AI's facial recognition during war*. Retrieved from: https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/, 24 March 2022.

91. Durkin, E. (2019). *New York school district's facial recognition system sparks privacy fears*. Retrieved from https://www.theguardian.com/technology/2019/may/31/facialrecognition-school-new-york-privacy-fears, 23 March 2022.

92. EDPB (2020). *Response to MEPs Sophie in 't Veld, Moritz Körner, Michal Šimečka, Fabiene Keller, Jan-Christoph Oetjen, Anna Donáth, Maite Pagazaurtundúa, Olivier Chastel, concerning the facial recognition app developed by Clearview AI*. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out_2020-0052_facialrecognition.pdf, 24 March 2022.

93. E-Health Network (2020). *Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19*. Retrieved from https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-19_apps_en.pdf 12 November 2021.

94. Electronic Frontier Foundation. (2017). *Street-level surveillance: Face recognition*. Retrieved from https://www.eff.org/pages/face-recognition, 03 February 2022.

95. Estonian Ministry of the Interior. *Automated biometric identification system database – ABIS.* Official website. Retrieved from https://www.siseministeerium.ee/en/activities/tohus-rahvastikuhaldus/abis, 1 March 2022.

96. European Commission (2020). *White Paper on Artificial Intelligence - A European approach to excellence and trust.* COM(2020) 65 final. Retrieved from: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, 12 March 2022.

97. European Commission. *Smart cities.* European Commission´s official website. Retrieved from: https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en, 11 March 2022.

98. European Data Protection Board. (EDPB) (2020). *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak.* Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, 14 June 2021.

99. European Data Protection Board. (2020*). Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.* Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf, 13 June 2021.

100. European Data Protection Supervisor. (2018). *Summary of the Opinion of the European Data Protection Supervisor on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*. 2018/C 233/12. Retrieved from https://edps.europa.eu/sites/edp/files/publication/18-04-16_opinion_interoperability_executive_summary_en.pdf, 29 March 2022.

101. European Parliamentary Research Service. (2021). *Regulating facial recognition in the EU. In-Depth Analysis*. Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698021, 13 April 2022.

102. European Union Agency for Fundamental Rights (FRA). (2019). *Facial recognition technology: fundamental rights considerations in the context of law enforcement.* Retrieved from https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law, 12 March 2022.

103. Facebook. *Tagging.* Facebook official website. Retrieved from https://www.facebook.com/help/267689476916031/?helpref=hc_fnav], 12 March 2022.

104. Gershgorn, D. (2021). *China´s „Sharp Eyes" Program Aims to Surveil 100% of Public Space*. Retrieved from https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015, 26 March 2022.

105. Guliani, N.S. (2019). *The FBI Has Access to Over 640 Million Photos of Us Through Its Facial Recognition Database.* Retrieved from https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through, 21 March 2022.

106. Higginbotham, S. (2016). *Inside Facebook's Biggest Artificial Intelligence Project Ever*. Retrieved from https://fortune.com/longform/facebook-machine-learning/, 26 March 2022.

107. Human Rights Watch. (2020). *Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights*. Retrieved from https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight, 16 March 2022.

108. Isikut tõendavate dokumentide seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. Retrieved from https://eelnoud.valitsus.ee/main/mount/docList/739ee44b-9df3-47b3-94c8-5f7ae3e1b559#44WhXv4z, 28 March 2022.

109. Levy, A. (2010*). School installs £9000 facial recognition cameras to stop students turning up late… and teachers could be next target.* Retrieved from https://www.dailymail.co.uk/news/article-1317520/School-installs-9kfacial-recognition-cameras-stop-students-turning-late.html, 23 March 2022.

110. Lynch, J. (2012). *What Facial Recognition Technology Means for Privacy and Civil Liberties,* Senate Committee on the Judiciary. Retrieved from https://www.govinfo.gov/content/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf, 15 March 2022.

111. Liberty (2022). *Resist facial recognition*. Retrieved from https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/, 18 March 2022.

112. National Telecommunications and Information Administration (2016). *Privacy Best Practices Recommendations for Commercial Facial Recognition Use*. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commer-cial_use_of_facial_recogntion.pdf, 17 February 2022.

113. NtechLab official website. Retrieved from: https://ntechlab.com/about/, 24 March 2022.

114. O'Mallon, F. (2019). *Home Affairs suggests porn viewers be subject to face scans*. Retrieved from https://www.smh.com.au/politics/federal/home-affairs-suggests-pornviewers-be-subject-to-face-scans-20191028-p534yk.html, 14 December 2021.

115. Pesenti, J. (2021). *An update on our use of face recognition*. Retrieved from https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/, 23 March 2022.

116. Ramos, L.F.M. (2020). Evaluating privacy during the COVID-19 public health emergency: the case of facial recognition technologies. *In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. Association for Computing Machinery, New York*, 176-179. Retrieved from https://collections.unu.edu/eserv/UNU:7838/p176-Ramos.pdf, 11 March 2022.

117. Sanders, L. IV. (2016). *When citizens spy: Russia´s FindFace sparks privacy controversy*. Retrieved from https://www.dw.com/en/when-citizens-spy-russias-findface-sparks-privacy-controversy/a-19232491, 23 March 2022.

118. Sarv, H. (2021). *Õiguseksperdid näevad probleemi ABIS-e info ristkasutuses*. Retrieved from https://www.err.ee/1608247482/oiguseksperdid-naevad-probleemi-abis-e-info-ristkasutuses, 15 March 2022.

119. UK Information Commissioner's Office (2019). *Opinion on the use of live facial recognition technology by law enforcement in public places*. Retrieved from https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf, 22 April 2022.

120. Välisministeerium (2020). *Isikut tõendavate dokumentide seaduse ja teiste seaduste muutmise seaduse eelnõu kooskõlastus*. Retrieved from https://eelnoud.valitsus.ee/main#6PBGFIzy, 12 March 2022.

121. World Health Organization. *Coronavirus disease (Covid-19)*. WHO official website. Retrieved from https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19, 13 April 2022.

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis

I, Teele Nässi

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Facial recognition – technology for a safer future or violation of the right to privacy?" supervised by Thomas Hoffmann,

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

_____05 May 2022.