UNIVERSITY COLLAGE STOCKHOLM DEGREE PROJECT

Master's program in Human Rights and Democracy Spring, 2024

Facial Recognition Technology

Potential Benefit and Harm in Relation to Privacy

Author: Karin Evars

Supervisor: Susanne Wigorts Yngvesson

University College Stockholm

Acknowledgements

Special thanks to my supervisor, Susanne, for your expertise, patience, and insightful feedback. Your encouragement and constructive critique have been valuable in shaping my research.

Special mentions and my gratitude extended to everyone who has supported me during the period of writing the paper. Their support has been a constant source of strength and motivation.

Abstract

A thorough analysis of Facial Recognition Technology (FRT) with attention to potential implications for human rights violations. Focusing on the extensive debates in the European Parliament, evaluating FRT's pro et contra in the context of current legal European Union (EU) framework. The effect of FRT on the right to privacy is investigated, as well as its wider ramifications for other human rights that EU citizens are legally entitled to. Utilizing the approach of the Swedish *argumentationsanalys* (argumentative analysis) as the means to highlight the pro et contra of FRT, the method allows an organized evaluation of the technology's overall consequences on the citizens of the EU.

The paper highlights the need of taking contextual norms into account as well as the necessity of consent and transparency in data collection, particularly in regard to the processing of biometric data. Even with FRT's potential to improve security and law enforcement, there are still a lot of ethical questions about its effectiveness, privacy invasion, algorithmic prejudice, and possible data exploitation.

Effort is made to address the need for strict controls and regulations to guarantee the moral and legal use of FRT. This is reflected in the primary materials coverage of European parliamentary members during the recent debates. It emphasizes the necessity of striking a balance between innovation and the upholding of fundamental rights, arguing in favour of steps to preserve individuals privacy, freedom, and democratic principles. The need of fostering legal clarity, trust with citizens, and accountability in the creation and use of FRT is underscored in the paper's conclusion in order to reduce possible hazards and preserve human rights standards in the digital era going forward.

Keywords

Facial Recognition Technology, Contextual Integrity, Privacy, European Union, Right to Privacy, Mass Surveillance, Biometric Data Protection

Table of Contents

1 Introduction

Facial Recognition Technology (FRT) has emerged at the forefront of technical innovation, a powerful tool for identifying individuals through analysis of facial features. Its importance in supporting security and surveillance measures is highlighted by its quick spread throughout a variety of public and private sectors. On August 7th, 2020 Black Lives Matter activist Derrick "Dwreck" Ingram was the target of an attempted arrest by the New York Police Department (NYPD). Facial recognition software was purportedly used to identify and track during their five-hour siege of his flat. NYPD showed up with dozens of police, a helicopter, SWAT officers, and police dogs on June 14th. He was accused of assaulting a police officer after yelling into a megaphone close to the officer. Dwreck did not resort to physical violence. While covering the attempted arrest, a reporter for the publication "The Gothamist" noticed a printout of a facial recognition report in the hands of a police officer, said report had Dwreck's name and details on it. After the attempted arrest, Dwreck's neighbourhood and the NYPD's social media accounts displayed wanted posters including his own photos from Instagram.[1] The same year New Yorkers who attended protests during the Black Lives Matter (BLM) movement were more likely to be exposed to FRT. The Domain Awareness System, a surveillance tool created by Microsoft, used by the NYPD, provides law enforcement with access to over 20,000 feeds from both public and private cameras. Such feeds may be used to follow the face of each person in New York City when paired with additional cameras and facial recognition software. Mass surveillance technologies run the potential of deterring legal protest because individuals may be afraid to exercise their right to freedom of assembly for fear of being recognized, followed, harassed, or even punished. Their use at BLM demonstrations against the backdrop of the heightened struggle for racial justice serves as a sobering reminder of the ways in which this technology still impacts minority communities more than any other.[2] This paper aims to examines the pro et contra arguments for the usage of FRT in Europe and the scope of its potential effect on privacy.

---

[1] Amnesty International. Ban the Scan. Amnesty International 2024. https://www.amnesty.se/agerahub/ban-scan/. (Access 17-04-2024).

[2] Amnesty International. Decode: A New AI Tool to Detect Facial Recognition in Your Photos. Amnesty International 2024. https://banthescan.amnesty.org/decode/ (Access 17-04-2024).

1.1 Research Problem

Facial Recognition Technology (FRT) is an advance technical innovation that uses biometric data and machine learning for identification, verification, or classification to automatically identify people based only on their facial traits. The widespread use of biometric technology, such as facial recognition, in many aspects of everyday life highlights the significant influence these technologies have on society at large. FRT has been vastly integrated in both the public and private sectors for anything from improving security measures to streamlining surveillance operations. The ongoing development of FRT offers both possibilities and problems, each of which needs to be carefully considered in this paper. Supporters of FRT highlight how it may improve public safety by supporting security protocols and assisting law enforcement in identifying and tracking suspects. This viewpoint, however, stands in stark contrast to FRT's opponents worries about the possible erosion of citizens' rights to privacy. Concerns due to the invasiveness of monitoring and its effects on civil rights are elevated by the indiscriminate use of FRT in public areas and commercial settings. Critical analysis of FRT's advantages and disadvantages are essential as FRT continues to develop and permeate through daily society. Striking a balance between the need for security and the protection of individual privacy rights is crucial in the present discussion over FRT as well as this paper. For this reason, careful research into the intricate implications of FRT on individual rights is crucial to make educated judgments and create the ethical and legal standards that govern its application in the European Union and the world at large.

1.2 Aim

The primary objective of this paper aims to conduct a thorough out analysis of Facial Recognition Technology (FRT), paying close attention to any potential implications for human rights. This paper is based on a thorough evaluation of relevant discussions held in the European Parliament and weighs both the benefits and drawbacks of FRT juxtaposing them to current European Union (EU) legal implications. The impact of FRT on the right to privacy is also examined in this paper, along with its wider implications for the entire range of human rights entitled to EU residents by law. Through a complete investigation, the papers research endeavours to furnish an all-encompassing comprehension of the complex correlation between FRT and human rights, therefore promoting knowledgeable debate and educated decision-making in this crucial domain.

1.3 Research Questions

1. What is the context of human rights mentioned when discussing pro et contra of Facial Recognition Technology (FRT) in the context of European Union (EU) law?

2. In regards to Facial Recognition Technology (FRT) what are the expectations of any effects on privacy of the individual?

2 Background

This chapter aims to provide an overview of FRT, covering various aspects including its functionality, mechanics, and implications, and to offer insights to facilitate a better understanding of its operation. Privacy perspectives and the existing legislative framework concerning FRT within the European Union (EU) will also be covered.

2.1 Facial Recognition Technology

Facial recognition is a technology that uses software systems with the ability to analyse similarities between facial features in photos and videos, in both recordings and in real-time. Facial recognition can be utilized to verify a person's identity through artificial intelligence (AI) processes or previous data of one's face. Facial recognition might be considered a means of assessing a specific individual's claim and can cover a variety of queries. These range from a simple question of one's identity verification "is this person really who they claim to be?", database queries "does this person's face profile match any records previously stored?" or even simple recognition checks "has this person ever been recorded by the system?". Although such activities can be completed by automated processes (i.e. AI), facial recognition systems usually include human examiners who oversee reviewing and approving the conclusions made by the program, which in turn ironically serves both as a safety contingency and as a safety issue.[3]

The automated facial recognition (AFR) use pattern recognition algorithms to identify individuals in pictures or videos. Applications for AFR are widely established, ranging from

[3] Crumpler William & A. Lewis James. How Does Facial Recognition Work? A Primer. *Center for strategic and International Studies (CSIS)*. 2021:2.

sophisticated authentication systems to social networking. However, AFR from recorded camera images in an unrestricted real-world setting remains highly challenging and poses changes due to significant variations in acquisition conditions and facial expressions. [4] The great majority of modern facial recognition systems are built using AI deep learning techniques, which are a subset of machine learning approaches that use artificial neural networks for data analysis. In facial recognition software development, developers use deep learning techniques to create software that can turn facial renderings or photos into numerical representations, for the resemblance to be determined through facsimile comparisons. It is crucial to recognize that although facial recognition functions as a type of biometric identification, not all biometric processing approaches need the application of AI deep learning algorithms.[5]

A common use for FRT is verification, in which the technology is used, is to confirm if a person matches an identity record. Today this technique is widespread. Examples of verification include using facial recognition to unlock smartphones, or to verify one's identification at airport security, or to access banking applications. When a user tries to log in, the system takes a picture of ones face, then compares it to a picture saved for that specific person. If the facial data matches, access is granted. Data used for comparison are usually taken at the time of registration from reliable sources, such as national identification registers or passports.[6] The process of identification entails utilizing facial recognition software to determine if the profile of an unknown person is included in a bigger collection of recognized data. Law enforcement use FRT to create a line-up of possible suspects based on both facsimiles, photos, or videos. They also use identification for purposes other than criminal investigations, such as finding individuals who have gone missing, identifying deceased persons, or removing existing duplicate entries from databases. Identification is also used in the private sector for many uses such as imposing blacklists in casinos (surveying clients for indicators of cheating and signs of gambling addiction), monitoring tables, and whitelists, and automating access control for workers or residents.[7] FRT can be utilized in situations where identification does not involve

---

[4] Olszewska, Joanna Isabelle. Automated Face Recognition: Challenges and Solutions. University of Gloucestershire. 2016. https://www.intechopen.com/chapters/52911

[5] Ibid., 2.

[6] Crumpler William & A. Lewis James. How Does Facial Recognition Work? A Primer. *Center for strategic and International Studies (CSIS).* 2021:3.

[7] Ibid.,3.

obtaining or linking personal data about a specific person. For example, some retail businesses may use customer tracking systems to identify recurring customers and track in-store behaviour such as trends and marketing purposes, but there is a legal expectation that it wouldn't link the information to identifiable personal information (names, addresses, or past purchases). As a result, the FRT used in such retail settings simply recognizes the return of said visitor, identified as visitor #010101 on a certain day, and would not be able to determine the visitor's full identity. Similar systems can also be applied in the inverse, to determine whether an individual has not been seen previously.[8]

2.1.1 Understanding the Mechanics of FRT

Facial recognition is a multi-step process that begins with data collection and ends with data consolidation. Although the specifics of various models and types of facial recognition systems may differ, the overall procedure is unchanging.[9] The objective of facial identification algorithms is to locate each face's spatial coordinates inside said picture. To determine if a certain portion of the image meets the criterion for being a facial area, this technique involves a thorough scan of the image. The output of the face coordinate system can have many shapes, but not limited to, square or rectangular dimensions. The coordinate localization of facial characteristics inside the face detection coordinate framework is referred to as facial position. Modern deep learning framework developments are essential for integrating advanced location technologies into facial recognition systems.[10] Data acquisition, or the gathering of facial imaging data, is the first step in the facial recognition process. Depending on the kind of system, cameras that can collect 2D, 3D, or thermal images are commonly used. The photos may come from a variety of sources, including dedicated facial recognition equipment, smartphone cameras, and video surveillance. After the initial recording of facial data, identification follows as the technique searches and locates human faces within the data. Utilizing advanced algorithms, the complete image is scanned to isolate the characteristics from the surrounding area based on attributes like facial structure, colour, and form. The method proceeds to extract

[8] Ibid., 3.

[9] Li Qinjun, Cui Tianwei, Zhao Yan, Wu Yuying, Facial Recognition Technology: A Comprehensive Overview. *Academic Journal of Computing & Information Science*. Vol. 6, Issue 7, 2023:15.

[10] Lixiang, Li & Xiaohui, Mui & Siying, Li & Haipeng, Peng. 2016. A Review of Face Recognition Technology. *Information Security Center*. Vol. 4, 2016:1.

relevant information from an image once it has been identified. The procedure entails recognizing, quantifying, and turning unique facial traits into numerical data. The length of the jawline, the width of the nose, the depth of the eye sockets, the form of the cheekbones, and the separation between the eyes are many of the facial traits that are frequently assessed. Certain methods, as eigenface-based systems, capture holistic aspects by seeing the face as a whole. Some, such as local feature analysis systems, focus on certain local characteristics such as the lips, nose, and eyes. Matching is the last phase in the facial recognition process. Matching entails contrasting the traits that were extracted with the facial data that was previously recorded in the database. The system searches the database for matches by comparing the characteristics of every face image accessible. Finally, in the verification process, the system verifies a person's identification by comparing their traits with the data that has been previously saved and stored in relation to them.[11]

Some systems use a similarity score to determine if two objects match. Once the similarity score surpasses a specific threshold, the algorithm determines that a match has been identified to a certain degree of certainty. In recent years, the techniques of feature extraction and matching have made extensive use of machine learning, and more especially AI deep learning. The accuracy and speed of facial recognition may increase through the use of deep learning algorithms to identify patterns in the facial data. A variety of advanced methods and tools are used in facial recognition. All facial recognition systems are built on the fundamental processes of data collection, face detection, feature extraction, and matching. However, there are significant differences in how each of these phases is implemented, resulting in varying degrees of accuracy and performance.[12]

2.1.2 Perspective on Privacy

In the European Union human dignity is enshrined in law and acknowledged as an inherent fundamental human right. The idea of dignity lays a strong emphasis on privacy, the right to a private existence, autonomy, control over personal information and solitude. Privacy is a fundamental right recognized in almost every nation’s legal framework within the Union and

[11] Li Qinjun, Cui Tianwei, Zhao Yan & Wu Yuying, Facial Recognition Technology: A Comprehensive Overview. *Academic Journal of Computing & Information Science*. Vol. 6, Issue 7, 2023:20-21.

[12] Ibid., 20-21.

is protected by constitutional clauses. Respecting one's right to privacy is both a societal and individual right. While privacy is widely acknowledged as a basic human right, data protection has not yet attained the same prominence. Such interests might include concerns about national security, as well as freedom of the press, speech, and freedom of information. Consideration of macro-scale public interests, especially those related to national security, must be carefully balanced to protect privacy while also safeguarding data.[13]

There are several ways to interpret and describe privacy through ethical and legal frameworks. Although numerous scholars have proposed that privacy is the capacity to manage information about oneself, [14] Clarke observes that "privacy is often thought of as a moral right or a legal right." Regardless of the definition of privacy used, it is obvious that there are many kinds of privacy-related difficulties. Clarke expressly specifies parameters on information privacy as "the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves".[15] The legal concept of privacy is complex, having multiple aspects and references to a set of values within the wide scope of human rights. This is not a new debate in the public and private sphere as data privacy has been an 'in vogue' debate in its modern sense since the 1960s in Europe. Current data protection laws only partially address the aspect of privacy and fall short of meeting the basic human need for privacy.[16]

[13] European Data Protection Supervisor. *Data Protection*. 2024. https://edps.europa.eu/data-protection/data-protection_en

[14] Bélanger, France & Crossler, Robert E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *Management Information Systems Research Center, University of Minnesota. MIS Quarterly,* Vol. 35, No. 4 2011:1017–1041.

[15] Clarke, Roger. Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*. 42:2, 1999:60.

[16] Clarke, Roger. A Framework for Analysing Technology's Negative and Positive Impacts on Freedom and Privacy. *Datenschutz und Datensicherheit*. Volume 40, 2016: 79-80.

2.2 Current Legal Framework in the European Union

The European Convention on Human Rights (Article 8)[17], the European Union Charter of Fundamental Rights (Article 7) [18] and the Universal Declaration of Human Rights (Article 12)[19] all specifically reference the right to privacy, or private life. However, as stated in the European Union (EU), privacy and data protection are not absolute rights, and can therefore be limited under certain conditions according to the EU Charter of Fundamental Rights. A proverbial 'balancing act' is frequently necessary, which pit the right to data protection and privacy against other EU principles, human rights, and the interests of the public and private sectors.

The Law Enforcement Directive states that regardless of a person's country or place of residence, the basic rights and freedoms they enjoy including the right to the protection of their personal data, shall be upheld by the principles and regulations governing the processing of their personal data.[20] Under the EU data protection acquis, processing of facial data is governed by EU legislation. The most pertinent instrument in the sphere of police and judicial cooperation in criminal situations is the Law Enforcement Directive which creates an extensive framework for protecting personal data in a specific relation to law enforcement. According to the Law Enforcement Directive, facial photos that are utilized for biometric matching in order to uniquely identify or authenticate a person are expressly referred to as biometric data.[21]

The General Data Protection Regulation (GDPR) distinguishes between the legal status of biometric "facial images" and basic "photographs" in recital Article 5(1)(a). Photographs are only considered biometric data when they are processed using particular technological methods that enable a person to be uniquely identified or authenticated. Facial photographs are classified as special categories of personal data, or sensitive data, due of their delicate nature. Article 17 "Right to Erasure" or in layman's terms "Right to be Forgotten," of the GDPR, enshrines the

---

[17] European Court of Human Rights. Council of Europe. European Convention on Human Rights. https://www.echr.coe.int/documents/d/echr/Convention_ENG

[18] Official Journal of the European Union C 326/391. Charter of Fundamental Rights of the European Union (2012/C 326/02).

[19] Universal Declaration of Human Rights. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

[20] Directive (EU) 2016/680 of the European Parliament and of the Council. Official Journal of the European Union, L 119/89, 27 April 2016. https://eur-lex.europa.eu/eli/dir/2016/680/.

[21] Ibid,.

ability to ask controllers to delete their personal data.[22] The aim of such laws are to advance the areas of justice, security, and freedom. Strong frameworks that ensure high standards of data protection are necessary to provide security against public threats both inside and outside the European Union, and to facilitate the sharing of personal data amongst competent agencies for the purposes of crime prevention, investigation, and prosecution. The creation of a strong and unified data protection framework inside EU, bolstered by efficient enforcement measures, is imperative.[23]

3 Previous Research

In this chapter nine examples of previous research shall be presented. These studies look at FRT from different perspectives, highlighting issues related to civil rights, equity, regulatory frameworks, and privacy. Studies were selected on their relevance to the previously highlighted categories. The studies are published from 2019-2023 underscoring relevance as the technology discussed is expanding and changing at a progressive rate. The studies will be explained one by one for further clarity.

The paper, "Facial recognition technology in schools: critical questions and concerns" by Andrejevic and Selwyn, takes a critical perspective of possible effects and ramifications of the uses of FRT in classrooms. Concerns about campus security, computerized registration, and student mood monitoring have led to a growing trend of integrating FRT in compulsory education. In the US, UK, and Australia there has been little debate or opposition to such technologies. Supporters point to advantages, including increased accountability, security, and efficiency, but preoccupations over the social effects of these technologies are growing. Concerns exist over misidentification, and the potential for FRT to go beyond its intended purpose.[24] The authors emphasise it is a crucial topic for discussion determining whether such technologies have any place at all in an educational setting. Facial privacy rights could be

[22] General Data Protection Regulation. Art. 17 GDPR. Right to erasure ('right to be forgotten') https://gdpr-info.eu/art-17-gdpr/.

[23] Directive (EU) 2016/680.

[24] Andrejevic, Mark & Selwyn, Neil. Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, 45:2, 2020:116–118.

seriously threatened by the introduction of such technology in schools. The authors argue that educational institutions shouldn't serve as stepping stone for the normalization of a technology that poses serious hazards to society. A technology that could jeopardize people's right to privacy and autonomy, with risks such as automated sorting and prejudice against students, must be disregarded.[25]

Dauvergne's study "Facial recognition technology for policing and surveillance in the Global South: a call for bans" collected data from interviews with legal experts, policy analysts, activists, and researchers with expertise in FRT. It found that FRT has become widely used in surveillance and law enforcement throughout several continents, including Asia, Africa, and Latin America. The supporters of FRT point to its ability to stop terrorist attacks, investigate crimes, and find missing people. In accordance to this paper, using FRT for surveillance and policing puts civil society at serious risk, especially when it comes to identifying and following citizens without a criminal history. Dauvergne stipulates that the uncontrolled use of FRT has the potential to worsen biased policing and suppress activity. Risks to one's personal security also exist. Anyone participating in a public demonstration faces the possibility that FRT can scan through social media posts and video recordings, detaining them days or weeks later if a "match" is found.[26] The paper contends even in nations with strong data and privacy laws, with a high degree of political freedom and civil liberties, FRT still poses serious a threat to civil society. The potential for abuse in such settings would persist as long as proponents of FRT push legal boundaries, conceal its use, create new applications, and allow FRT to infiltrate state agencies into unregulated areas forming new methods of social control. This holds true even if misidentifications and algorithmic bias were to be eliminated and the technology was only used for serious crimes, missing persons, and border crossings. The Global South is seeing an increase in calls to outlaw FRT. [27]

The study "Policy designs for adaptive governance of disruptive technologies: the case of facial recognition technology (FRT) in China" examines the possibility and requirement of new methods to policy development surrounding disruptive technologies. Regulatory reforms alone

---

[25] Ibid., 125-126.

[26] Dauvergne, Peter. Facial recognition technology for policing and surveillance in the Global South: a call for bans. *Third World QuarTerly*, Vol. 43, No. 9, 2022:2325–2328.

[27] Ibid., 2332-2333.

are an insufficient safeguard of privacy to guarantee data security. For regulatory difficulties to be properly addressed, key policy measures including the policy mix, stakeholder engagement, and the regulatory sandbox approach are necessary. Policy tools outside are an alternative option, especially considering the unknowns surrounding the creation and application of disruptive technologies. To create and carry out policy solutions for the problems presented by disruptive technologies, it is critical that the government expand its knowledge base and experience by collaborating with the business community and academic institutions.[28]

Bu Qingxiu´s study offers a thorough examination of the privacy, ethical, and legal issues related to the use of automated facial recognition (AFR) technology. The paper highlights the dual nature of AFR, which can be used for both good and bad, sparking a contentious discussion about how it can affect fundamental rights, including privacy. Attention is drawn to the spread of AFR across several industries, law enforcement and the commercial sectors, expressing worries about the absence of clear legislative frameworks controlling its use and resulting the privacy risks.[29] It accentuates the absence of consistent norms for data access, exchange, and protection in the context of AFR. AFR-specific legislation are essential in handling the particular hazards posed by the technology, and also highlights the lack of comprehensive global governance structures supervising AFR implementation, creating consequences for privacy protection. Qingxiu concludes by recommending a multifaceted approach to AFR technology governance through accountability systems, legal protections, procedural safeguards, and stakeholder involvement. Policymakers as well as stakeholders should navigate the complex challenges posed by this technology while upholding fundamental freedoms and privacy rights by integrating considerations of fundamental rights into the architecture of AFR, creating frameworks for global governance, and encouraging public discussion on the ethical implications of AFR.[30]

Stevens and Keyes, on the other hand, outlines a historical-contextual background to comprehend FRT datasets and the conditions surrounding their production, application, and

---

[28] Zhizhao, Lia & Yuqing, Guoa & Masaru, Yarimea & Xun, Wu. Policy designs for adaptive governance of disruptive technologies: the case of facial recognition technology (FRT) in China. *Policy Design and Practice*. 2023, Vol. 6, NO. 1, 2023:27–38.

[29] Qingxiu, Bu. The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. *International Cybersecurity Law Review*, 2021:113–118.

[30] Ibid., 138-139.

distribution. Law enforcement, and security are using FRT more frequently. Those opposed to FRT have often focused on the discriminatory consequences of surveillance, or how the design and implementation of FRT systems disproportionately subject minorities to special observation and occasionally violent intervention. People who are underrepresented in the datasets used to create the technologies are said to suffer from FRT's biased inaccuracies. FRT includes a range of technologies that facilitate facial matching and are used in a variety of applications, including marketing, security, and attendance monitoring. These databases, which contain millions of images together with related metadata, are often exchanged by the private sector, government agencies, and academic institutions. They blur the lines between different sectors by embodying knowledge and power relations. Comprehending databases as locations of knowledge and authority exposes the wider political ramifications of FRT, depicting it as a cultural instrument that sustains certain state power structures via visual monitoring.[31]

The paper "Mass Data Gathering and Surveillance: The fight against facial recognition technology in the globalized world" examines the effects of FRT on essential rights and values, emphasizing its capacity to compromise privacy and sustain bias and discrimination. FRT is expected to progress quickly, making it possible to compare biometric photos kept in IT systems. While AI has the potential to revolutionize society and address major global issues, it also raises some very real concerns, considering the increasing use of surveillance technology by the government and commercial sector, which can infringe on fundamental rights. FRT is being regulated by the EU as part of its effort to create a moral and legal foundation for reliable AI. The author expresses that even with strict regulations already in place, such as the EU General Data Protection Regulation (GDPR), further guidelines and a well-defined legal framework are required to guarantee the reliable application of FRT.[32]

The study" Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology" looks at public opinion on FRT in China, Germany, the UK, and the US show differing degrees of acceptability about Facial Recognition Technology (FRT) that is being used by governments worldwide for improved law enforcement and public services, despite

[31] Stevens, Nikki & Keyes, Os. Seeing Infrastructure: Race, Facial Recognition and the Politics of Data. 833-835. *Routledge Taylor & Francis group*. Vol. 35, 2021:833-835.

[32] Nesterova, Irena. Mass Data Gathering and Surveillance: The fight against facial recognition technology in the globalized world. *Globalization and its Socio-Economic Consequences*. 2019:1-2.

privacy concerns and discriminatory practices. Although AI and smartphone technologies are effective in resolving social problems, their potential for widespread surveillance and privacy violations is concerning. It is important to comprehend how the public feels about this socio-technical change. The study demonstrates that FRT acceptability is influenced by centralized technology administration, overall tech-friendly attitudes, and trust in government organizations. The public's approval or rejection of policies is primarily influenced by privacy concerns, which underscores the urgency with which politicians must close regulatory loopholes and inform the public on the implications of privacy policies.[33]

Lindsey Jacques analyses the five permanent members of the United Nations Security Council and the usage of FRT. Under the UN Charter, these five countries are responsible with upholding international security as permanent members of the Security Council. Although FRT may seem unsettling, it has a lot of potential applications in terms of national security, criminal identification, and countering terrorist threats. Racial and gender prejudice has left FRT mostly unregulated and with extremely inconsistent accuracy. The technology's security safeguards, and privacy infractions provide an ethical conundrum due to the advantages and disadvantages of FRT. The issue that national authorities in these nations must address is whether the benefits of FRT in minimizing national security exceed the privacy and equity risks that the technology presents to groups who are frequently deemed to be the most vulnerable.[34]

The paper" Defrosting the Chill: How Facial Recognition Technology Threatens Free Speech" underscores how law enforcement authorities may be more likely to misuse FRT. Protected expression is allegedly under danger due to law enforcement frequent uses of FRT. The recommendation is to severely control FRT and lessen any infringement on people's First Amendment rights in America by executive or legislative action. The growing use of FRT by law enforcement has sparked discussions about its advantages and disadvantages across the country. Significant differences were found, for example that FRT algorithms often misidentified black women but did well when analysing the features of white males. The

[33] Kostka, Genia & Steinacker, Léa & Meckel, Miriam. Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*. Vol. 40, 2022:1-2.

[34] Jacques, Lindsey. Facial Recognition Technology and Privacy: Race and Gender - How to Ensure the Right to Privacy Is Protected, *San Diego International Law Journal*, vol. 23, no. 1, 2021:112-114.

tyrannical potential of such invasive technology is a serious worry. FRT's broad usage might stifle free expression and association rights and jeopardize privacy expectations.[35]

4 Methodology

This section explains in more detail the material, limitations, ethical considerations, and the reasoning of the method chosen. The selected method in this paper is argumentative analysis, chosen to highlight both the pro et contra of FRT and its effect on privacy.

4.1 Material

To weigh the pro et contra arguments of FRT in Europe, primary material is extracted from debates about the Artificial Intelligence (AI) Act in the European Parliament. The material, videos from the debates published by the European Parliament, has been meticulously self-transcribed. Sections of the primary material have then been translated to English since the language spoken in the videos vary among the EU official languages. The primary topics of discussion, throughout the debates are the benefits of AI and biometrical technology whereas FRT is highlighted in the contra arguments outlining risks it entails. The debates took place between the 10th of April 2021 and 13th of Mars 2024. The videos vary in length but are up to 43 minutes long. The debate material gives an overall view of the core arguments of FRT. The arguments in the AI Act debates are relevant, up to date and show the current arguments pro et contra FRT in Europe and therefore this is chosen as the primary material.

The choice was made to combine the primary material with the secondary material "Person identification, human rights and ethical principles. Rethinking biometrics in the era of artificial intelligence" to give more specific details about FRT and to give an even more in-depth argumentative analysis. The study is written by Professor Gloria González Fuster and Michalina Nadolna Peeters[36] of the Law, Science, Technology and Society (LSTS) Research Group at Vrije Universiteit Brussel (VUB), at the request of the Panel for the Future of Science

[35] Roy, Kirsten E. Defrosting the Chill: How Facial Recognition Technology Threatens Free Speech. *Roger Williams University Law Review*, vol. 27, no. 1, 2022:185-187.

[36] Madiega, Tambiama & Mildebrath, Hendri. Regulating Facial Recognition in the EU. European Parliamentary Research Service. Brussels, European Union. 2021. 1-37.

and Technology (STOA) and is intended for use as background information for European Parliament staff members and members in their parliamentary duties for the AI Act debates. The secondary material is credible, established and includes relevant sources that contribute to the primary material. Its inclusion fortifies the argumentative analysis method giving a more in-depth answer to the questions posed. Both the primary-, and secondary material are credible, relevant, and provided sufficient material to conduct the argumentative analysis, addressing the purpose of the paper.

4.2 Limitations

The primary material in this paper are videos from the debates about the AI Act published by the European Parliament. For a more thorough understanding of the AI act and its ramifications, it is critical to acknowledge the limitations of the political discourse of the primary material. In these debates an abundant of arguments related to FRT and privacy are presented. The AI Act was debated by politicians, and not researchers and scientists. These discussions are insightful, but they might not have the depth and knowledge that a scientific examination could. On the other hand, the secondary material consists of a study that was conducted by the European Parliament for the benefit of the staff and members of the European Parliament. Background information is additionally provided here to give insight on parliamentary work.

It is essential to acknowledge that FRT is a developing technology and there is limited history of research into the subject. The need to rely on recent sources, current advancements, and conversations within the field of FRT is acknowledged in order for the study to stay relevant. Another limitation is the difficulties in performing an ethical study of technology. Technology is not inherently ethical or unethical, making it difficult to analyse its ethics. The ethical ramifications vary depending on the user and how they utilize it.

4.3 Ethical Consideration

Research has a significant position in our society and is expected to be held to a high standard. Researchers are held to specific requirements and make every effort to produce exemplary studies/research. One needs to stay true to said standards of research which include not to act in one’s own interests, or the interests of other stakeholders and the research must be free from

outside influence and manipulation. A strong foundation of trust is essential for good research.[37] Research misconduct, or scientific misconduct, diminishes public trust in scientific publications, the research community, and society at large.[38] The All-European Academies have stated fundamental principles for good research practice that research fundings within EU are using as their ethical framework. In this qualitative research the principles of reliability and honesty are pursued by working methodically. Structuring the research process in a way so that the reader can follow the whole process from design, data collection to analysis and use of resources. Argumentative analysis shall be used within this paper's framework and the different steps in the process will be clearly informed in an open and complete way. The principle of respect is shown in the researcher´s relationship to the research task, assignment, authors of different articles and even for society. The research is aiming to analyse FRT through a human rights lens, weighing the pro et contra by a comprehensive evaluation of relevant EU law and ethical recommendations to understand how human rights considerations are integrated into discussion about the advantages and disadvantages of FRT. This paper scrutinizes and weighs the effects of FRT on the individual's right to privacy while investigating the greater scope of any and all effects of FRT on general human rights of citizens in the EU. Respect is a crucial ethical principle in this research and the researcher should be aware of the importance to follow a respectful ethical framework throughout the whole research process. Only by doing so can the researcher achieve a level of accountability for said research from idea to publication and hopefully for wider consequences that can strengthen the knowledge about the use of FRT.[39]

4.4 Method

The method of this paper is the Swedish style '*Argumentationsanalys*' which is a combination of both Argumentative and Analytical Thesis structures. Argumentative analysis is the chosen framework in this study to highlight the advantages and disadvantages of facial recognition technology (FRT). The method focuses on the structural framework of the authors 'argument/s' and is utilized across the broad spectrum of social sciences. It is imperative with an argumentative analysis to examine and clarify the conceptual framework essential to the debate

[37] Vetenskapsrådet. *Good Research Practice*. 2017:10.

[38] Ibid., 63.

[39] Vetenskapsrådet. Ethics in research and good research practice. 2019.

at hand. The primary rhetoric of the argumentative analysis is to present and debate facts and data. It is crucial to weight the data analysis as a priority, with more significance than any existing ’emotional arguments’ which instead would serve as a 3rd dimensional dilution rather than a better macroscopic overview. [40]

The central concepts of rhetoric are logos, pathos and ethos. With Logos, the structure makes use of the readers' capacity for reason, relevant texts that primarily utilize Logos present as factual, shying away from judgmental stances and phrases. Ethos refers to the persona, or ‘essence’ that one aspires to project forward in order to pique attention and earn confidence in the argument presented forward. One considers to be firmly present in the text if Ethos is well-pronounced. If strong emotions are to arise in a target audience, as a tool to convince or strengthen one’s argument, then is what is known as Pathos. Argumentative analysis prioritizes Logos over Ethos, and avoids, if possible, the use of Pathos. [41]

Firstly, an argumentative analysis can be descriptive, one should reconstruct and organize the relationships between individual texts or debates. The second purpose the method serves is evaluative, argumentation may be assessed from various perspectives and determinates how strong an argument argues in favour of or against a particular standpoint. A descriptive analysis is essential before making such an assessment, examining logical fallacies can be useful in determining the veracity of an argument. Additionally, argumentative analysis can be employed as a means of preliminary examination of a given text in order to efficiently extrapolate the core reasoning and argument. [42] The stronger the authors argument the more based in relevant and contextual evidence, and author must be weary of straying into a one-dimensional argument or over complication. One can hail to Occam’s Razor rather than oversaturating a particular standpoint when presenting an argument. In evaluating an argument's strength in relation to its thesis, an assessment of relevance and validity is imperative. Firstly, the combination of validity and relevance must be the basis for evaluating any argument, one should weigh the overall strength of a thesis’ support against the overall strength of resources in opposition. The validity of an argument is the crux of any given criterion used. When said requirements are satisfied, an

---

[40] Boréus, Kristina & Bergström, Göran. Textens mening och makt, metodbok i samhällsvetenskaplig text- och diskursanalys. Studentlitteratur AB, 2018:24.

[41] Ibid., page 94.

[42] Ibid., 95-96.

argument reaches a higher threshold of evidentiary relevance. On the other hand, a deviation from the previous framework results in a corresponding loss in evidentiary relevance, and thus power. Arguments that are not accepted as relevant degrade the overall stance and undermine any ability to substantiate evidence claims. In many cases, the argument's overall threshold is compromised by both validity and relevance flaws, which exacerbate the effect on the persuasiveness of the evidence.[43]

The method argumentative analysis is used as a tool to understand the different perspectives about FRT in the perspective of the European Union and its relation to privacy. This paper will use the pro et contra technique of the argumentative analysis to present arguments of both for and against FRT. This approach makes it easier to conduct an organized analysis and assessment of the arguments.[44] As a researcher, this enables to methodically understand and assess the advocacy and critical viewpoints related to FRT. While counterarguments require evaluating and studying opposing ideas, pro-arguments comprise examining and finding claims and reasons in favour of FRT. This method makes it easier to understand the arguments about FRT more deeply and allows for a more thorough assessment of its benefits and drawbacks connected to privacy. It clarifies the current discussion and range of factors surrounding the FRT execution, allowing for the analysis of many points of view. The pros and cons technique offers an organized and methodical framework for examining the numerous arguments related to the subject.[45]

5 Theory

Contextual Integrity (CI) offers a systematic framework for examining privacy in connection to information flow, which facilitates in understanding the impact to people's privacy by FRT. Beyond privacy, CI takes into account general human rights issues; assessing how FRT affects equality, freedom of speech, and individual autonomy. It also offers a systematic method for

[43] Björnsson, Gunnar & Kihlbom, Ulrik & Ullholm, Anders. Argumentationsanalys, färdigheter för kritiskt tänkande. Natur & Kultur Akademisk, 2009:48, 194–195.

[44] Boréus, Kristina & Bergström, Göran. Textens mening och makt, metodbok i samhällsvetenskaplig text- och diskursanalys. Studentlitteratur AB, 2018:106.

[45] Ibid., 127-129.

assessing legal compliance, in line with the study's objective of reviewing EU rules pertaining to FRT. Furthermore, by emphasizing both advantages and disadvantages of FRT, CI aids to provide a fair evaluation of its benefits and drawbacks from a human rights standpoint. It should be considered that CI offers a useful instrument for examining how FRT may affect human rights and privacy inside the EU.

There is not a binary approach to the theory, one is free to accept and use some concepts while rejecting others. The theory is divided into four ideas. Firstly, privacy is defined by how information flows, due to the existence of various privacy models, such as secrecy, data reduction, and leaking, CI emphasizes the significance of its perspective. Such models frequently display inflexible and absolute character, classifying data as either private or public, secret, or not. CI understands that privacy is a dynamic concept and therefore it cannot be categorized information as ‘secret’ or ‘not secret’ or as ‘private’ or ‘public’. One can readily disclose information that might otherwise be deemed private and off-limits in appropriate situations. On the other hand, data that is readily visible to the public, such a visit to a store or a purchase we make there may still be regarded as private if it is extracted from its original context, such as when it is combined to produce a comprehensive profile of our travel patterns or purchasing preferences. CI tackles said issue by considering the information flow in addition to the particular data type. According to CI, ‘improper’ information flow results in privacy infringement. [46]

The second idea is that information flow is suitable when occurring in accordance with the standards of a certain informational environment and claims the idea of contextual information. Sharing information in a manner that deviates from said deeply ingrained norms is improper and constitutes a privacy breach. When information defined as Contextual Integrity flows produced by a practice or activity adhere to the ‘acceptable’ contextual informational norms, privacy is protected. When such norms are broken, privacy is therefore ‘damaged’. Concerns about privacy don't ‘magically disappear’ as therein the user selected "I accept." CI posits that norms serve as the primary deterrent for privacy. Norms are commonly accepted expectations

[46] Malkin, Nathan. Contextual Integrity, Explained: A More Usable Privacy Definition. Usable Security and Privacy for Security and Privacy Workers. *University of Maryland and University of California, Berkeley.* 2023:59.

and norms for what will happen to supply information.[47] Norms can be defined to be rigid or approximate, or from a range of sources, be demanded or just emergent, be codified in legislation, change over time and between cultures, be widely or only locally recognized, and so on.[48] This flexibility implies there could not be a single, accurate rule applicable to a particular circumstance. The interaction of many situations, cultures, and values can result in the presence of several norms, some of which may even conflict with one another. As a result, opinions regarding the accepted standard may differ. In certain situations, CI might not provide a solution.[49]

The third idea is that such contextual norms can be described or identified by data type, data subject, sender, recipient, and transmission principle among others. To understand the privacy norms at play in a given situation all such parameters must be considered and identified. For instance, one cannot choose how information should be shared if one does not know what the information is or who it is about. For instance, users of smart speakers give voice assistants with their speech and interaction data in the hopes it will be used to respond to inquiries, offer services, and maybe enhance the devices. However, many would feel it inappropriate if this data were used for advertising.[50] Nissenbaum emphasizes that "respective roles, activities, purposes, information types do not exist in a context; rather, these factors constitute a context.".[51]

The fourth idea is that flows, and newer norms should be evaluated through their context. According to CI, consideration must be given to the objectives, values, and roles within a context, as well as the interests of the parties involved and the political and moral principles at stake. Prioritizing the interests of all parties involved is followed by a more thorough examination of ethical considerations, which includes ideas like justice, equality, freedom of expression, personal autonomy, and privacy. These judgments are arbitrary and prone to disagreement. Arguments over whether certain policies are consistent with a particular ideal

---

[47] Ibid., 60.

[48] Nissenbaum, Helen. *Contextual integrity up and down the data food chain*. Theoretical Inquiries Law, vol. 20, no. 1, 2019:224,227.

[49] Malkin, Contextual Integrity, 60.

[50] Ibid., 61.

[51] Nissenbaum, Contextual integrity, 227.

occur beyond the context of privacy. Although CI cannot provide a conclusive answer in every situation, the framework offers a structured method of considering whether a certain action compromises or protects privacy.[52]

6 Results and Analysis

The following results and analysis will be based on the debates in the European Parliament about the AI Act which include perspectives on FRT. Diagram 1.0 shows a simplified compendium of the key arguments for pro et contra of the usage of FRT. There is no stark divide between the different arguments for the pro et contra of FRT, the arguments affect and flow into each other.

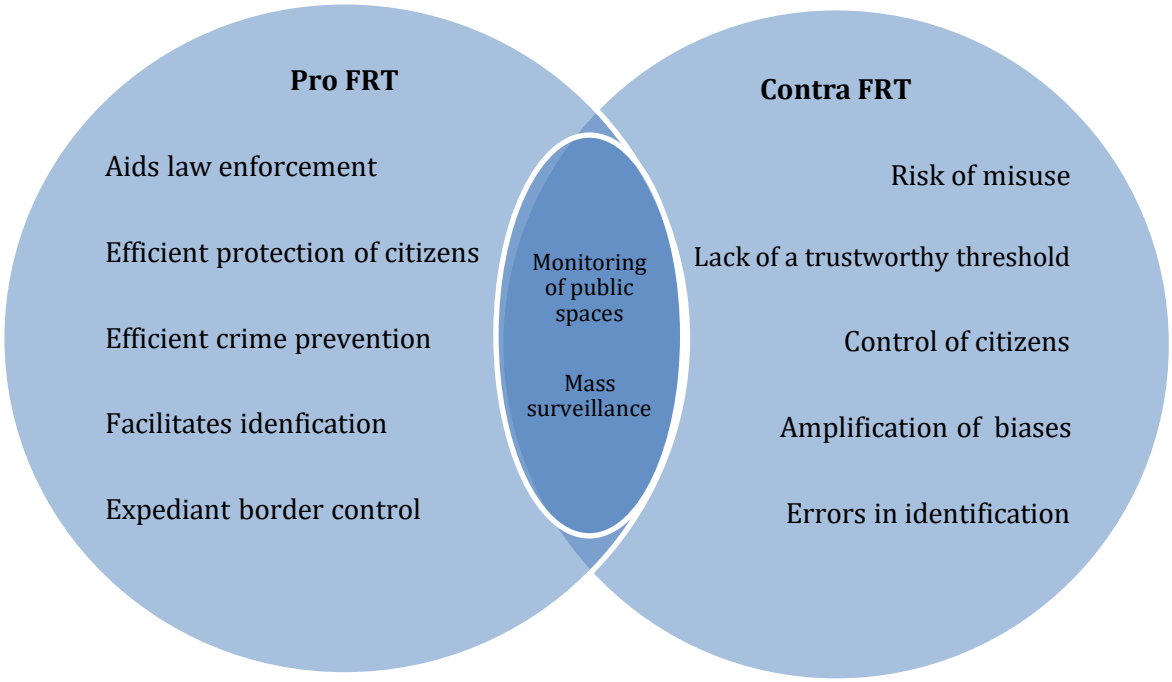

Diagram 1.0 Pro et contra arguments based on the primary material.

6.1 Arguments Pro the Usage of FRT

AI is a new and strong technology that has shown to be a significant advantage in the context of some criminal investigations and border control. Because FRT typically uses automatic processing of data related to physiological, behavioural, or physical characteristics in order to

[52] Malkin, Contextual Integrity, 62.

uniquely identify a natural person, its use falls under the definition of processing biometric data as defined by GDPR Article 4(14) and EU Law Enforcement Directive (LED) Article 3(13).[53] Law enforcement today relies heavily on FRT to identify criminals and victims not just in publicly accessible areas but also on the internet.[54] The 1.5 million police officers in the EU stand to gain a great deal from FRT in their efforts to combat crime. It can identify criminals who are on the run, anticipate criminal behaviour, and detect counterfeit items and currency at speeds better than previous means.[55] Investigators' ability to identify, locate, and apprehend the suspects is made possible in part by this artificial intelligence and facial recognition approach.[56] Police and judges are able to deploy technology that stop sophisticated cybercrime or terrorism.[57] Nonetheless, Member States may make exceptions in accordance with Article 13(3) LED in order to preserve national and public security or to prevent impeding or harming current investigations. Since giving the suspect access to FRT might jeopardize their efforts to enforce the law, these exclusions might be very helpful to law enforcement. The implementation of such exclusions requires compelling explanations, as this would prevent data subjects from exercising their rights.[58] FRT increases border control, so it has a net-positive effect on migration to and through Europe, making it more efficient to control and it is not advisable that future AI legislation negate such possibilities.[59]

Crimes such as money laundering, financing of terrorism, distribution of terrorist materials, human trafficking for the purpose of various forms of exploitation (including sexual and labour), and the proliferation of content related to child sexual abuse all require significant

---

[53] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 11.

[54] European Parliament Multimedia Centre. Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters - MEPs debate. European Parliament. 2021. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-in-criminal-law-and-its-use-by-the-police-and-judicial-authorities-in-criminal-matters-meps-debate_I211311. 00.06.06.

[55] Ibid., 00.19.23.

[56] European Parliament. AI in Criminal Law, 00.33.54.

[57] Ibid., 00.35.37.

[58] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 13.

[59] European Parliament Multimedia Centre. Artificial Intelligence Act - MEPs debate (Part 2). European Parliament. 2023. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-meps-debate-part-2_I242707.00.23.16.

efforts to identify the victims, offenders, and abuse locations.[60] FRT is an expedient means for security forces in the search for victims of kidnapping or ongoing terrorist crimes. 76 percent of abducted children that tragically do not survive the abduction die within the first three hours of their disappearance, therefore FRT can be lifesaving. This reflects the importance and creates the need for the use of faster technologies available to security services to prevent tragedies from happening.[61] Impunity would constitute a degradation of society's right to justice, particularly for the victims. FRT is very powerful and should only be utilized under strict judicial control. Such judicial control and oversight is essential to preserve the general privacy of people.[62] Privacy is a dynamic concept and therefore it cannot be categorized information as 'secret' or 'not secret' or as 'private' or 'public' and as long as the data is used for its purpose. As in this case use to catch criminals or missing persons the data and information collected does not violate privacy if the data in handled correctly and not shared. The data should one be available for the parties involved and is not for sharing to other parties.[63]

The police and judicial fields are not immune to technological developments and among these FRT is a powerful technology to use.[64] Arguments state that law enforcement must adopt AI as a core instrument to combat cybercrime more effectively.[65] Since law enforcement can identify potential attacks before inception, prevention is more successful than treatment, it is vital to build strong barriers against hackers and deploy artificial intelligence as a kind of infiltrator.[66] FRT have ten times greater accuracy than non-AI technologies, and in recent years, these systems' total accuracy has grown dramatically. Before taking any action, each possible match need to be verified by professionals in tandem with FRT in its current state. AI is a vital tool that law enforcement personnel need to assist them make fast and appropriate decisions. The

---

[60] Ibid., 00.26.57.

[61] European Parliament Multimedia Centre. Artificial Intelligence Act: MEPs Debate (Part 1) European Parliament. 2023. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-meps-debate-part-1_I242315. 00.15.57.

[62] European Parliament. AI in Criminal Law, 00.35.57.

[63] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 59-60.

[64] Artificial Intelligence in Criminal Law [29/04/24]. 00.33.54

[65] Ibid., 00.09.21.

[66] Ibid., 00.25.43.

more invasive the impacts, the more robust the protections that are required. In the fields of justice and law enforcement, artificial intelligence used as FRT is a source of innovation and advancement both in public accessible spaces and online environments.[67]

The principle of data security states that personal data must be processed in a way that guarantees adequate security, including protection against unauthorised or unlawful processing as well as against unintentional loss, destruction, or damage, using the necessary organizational or technical safeguards (Article 4(1)(f) LED and Article 5(1)(f) GDPR).[68] When the law is followed FRT makes daily routines and business more productive and pleasant. Consider unlocked phones as an example of basic security precautions.[69] When it comes to technology, trust is everything. Control is made possible by embracing technology. On the other hand, control becomes illusive when it is kept at a distance. Promoting legal clarity and trust promotes AI's good growth, which benefits a range of sectors, enterprises, and industries while also helping society.[70] FRT aims to raise our standard of living that can enhance the quality of life for European citizens and the resilience of vital infrastructure.[71]

The reality is that widespread digital surveillance has already arrived. FRT can have a significant advantage to prevent combat crimes and even if FRT presents a risk as well as an opportunity for improved times ahead.[72] As Article 13 (3) LED[73] states that Member States may make exceptions to safeguard public and national security or to prevent impeding or

---

[67] Ibid., 00.00.13.

[68] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 17.

[69] European Parliament Multimedia Centre. Artificial Intelligence Act: Opening Statements by Brando Benifei and by Dragoş Tudorache (rapporteurs), by Eva Maydell, Marcel Kolaja, Axel Voss, by Margrethe Vestager, Thierry Breton, and by Susana Solís Pérez and Josianne Cutajar. European Parliament. 2021. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-opening-statements-by-brando-benifei-and-by-dragos-tudorache-rapporteurs-by-eva-maydell-marcel-kolaja-axel-voss-by-margrethe-vestager-thierry-breton-and-by-susana-solis-perez-and-josianne-cutajar_I242314. 00.27.12.

[70] European Parliament Multimedia Centre. Artificial Intelligence Act: Extracts from the Debate. European Parliament. 2023. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-extracts-from-the-debate_I242459 00.02.08.

[71] European Parliament Multimedia Centre. Artificial Intelligence Act - MEPs debate. European Parliament. 2024. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-meps-debate_I254282. 00.03.59.

[72] European Parliament. AI (Part 2). 00.08.00.

[73] Directive (EU) 2016/680.

undermining current investigations. Strong arguments are required for the implementation of such exclusions as doing so would prevent data subjects from exercising their rights and makes FRT free for states to use. The usage of FRT needs to bear in mind that contextual norms can be identified by type of data, data subject, sender, recipient, and transmission principle. The data collected should be disclosed to the user if one is unaware of the nature of the information or the subject of it. [74] A warning sign need to be provided and placed in a way in a way that makes it easy for the data subject to understand the monitoring situation before they approach the monitored area.[75] Even if the person of matter has accepted the data to be collected, it should not be used for other purposes.[76]

6.2 Arguments Contra the Usage of FRT

Opposition of FRT in Europe proport that the EU should be free from biometric mass monitoring to avoid living in a culture of fear. Living with mass surveillance rejects a society defined by complete compliance by constraining freedom, diversity, and disagreement. FRT lacks evidence in its accuracy and has led to unacceptable risks of errors and violations that would only be discovered after the fact by the supervisory authorities. [77] FRT has algorithmic bias which in combination with lack of training data, can have a significant effects on basic rights.[78] Speakers at the European Parliamentary debates used as the primary material argued that the employment of AI systems for mass surveillance and remote biometric facial recognition has already resulted in far too many instances of misidentification. System abuses create a loophole for people to give up their right to privacy in favour of technology[79] and that police work should not progressively adopt the comparison of biometric face traits as regular procedure. Law enforcement's use of AI is frequently regarded as having a significant danger to civil rights. The deployment of such fundamentally intrusive technology should not be

[74] Malkin, Contextual Integrity, 61.

[75] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 13.

[76] Malkin, Contextual Integrity, 61.

[77] European Parliament. AI in Criminal Law, 00.06.06.

[78] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 6.

[79] European Parliament. AI in Criminal Law, 00.06.06.

routine, even if it were practical and made police work easier.[80] Innovation that improves our lives while upholding our rights ought to be the focus of FRT.[81]

In the USA, Boston have replaced AI-driven predictive policing with community policing, which has reduced crime rates. Boston has also already banned FRT in public spaces, so not only is a ban perfectly feasible, but AI is not a cost related fix to fight crime such as terrorism. Arguments underlines that automating police work is not a substitute for police funding and community workers.[82] Fundamentally, FRT should only be used in carefully controlled situations and within specific, bounding parameters.[83] Mass biometric monitoring and security in public spaces effect on peoples' fundamental rights cannot be sacrificed when fighting crime.[84] Ethical, safe, dependable, and environmentally friendly nature of innovative technologies in Europe through establishing standards for development needs to be guaranteed.[85] These issues must be addressed in proposed rules, particularly with regard to the high danger of discrimination associated with technological and predictive methodologies used in law enforcement.[86]

There are several uses of AI that are strictly prohibited in Europe, such as mass monitoring and personal control.[87] Article 8 in Charter of Fundamental Rights of the European Union states that everyone is entitled to the protection of personal information about them and such data must be treated fairly, for the intended uses, and with the subject's permission or another legal justification permitted by law. Everyone has the right to see the information that has been gathered about them and the right to have it updated.[88] It should be transparent to individuals that personal data concerning them is gathered, used, examined, or otherwise processed. The

---

[80] Ibid., 00.03.24

[81] European Parliament. AI (Part 2). 00.30.04.

[82] European Parliament. AI in Criminal Law, 00.11.41.

[83] Ibid., 00.16.22.

[84] European Parliament. AI in Criminal Law, 00.06.06.

[85] Ibid., 00.19.51.

[86] Ibid., 00.06.06.

[87] European Parliament. AI (Part 2). 00.25.43.

[88] Official Journal of the European Union Charter 326/391, Article 8.

extent that personal data is or will be processed, is stated in the GDPR's transparency principle Article 5(1)(a). This does not automatically prevent relevant authorities from conducting secret investigations or using video surveillance.[89] The privacy, autonomy, dignity, and personal data are all significantly impacted by FRT. Since FRTs are widely used and imply mass monitoring, new social difficulties may emerge as a result, such as the inability to move anonymously in public places and an reduced conformity to free will.[90] There is a worry that FRT gives authoritarian governments unprecedented tool of oppression, as under constant surveillance, people are no longer free.[91] Arguments underline that democracy should be protected and ensured that technology is used in the service of people and the environment, not the other way around.[92] One spokesperson in the debates expressed his worries and asked the question "Imagine your favourite example of the worst politician in your country. Now, would you want them to have a remote control to such spying? I do not"[93]. Predictive policing is not the solution and therefore should FRT in public spaces be banned.[94]

Public authorities are required to conduct effective research on fundamental rights in order to provide safeguards for vulnerable groups due to the employment of high-risk AI systems.[95] Video surveillance in public areas have the potential to negatively impact people's freedom of assembly and association, as well as their ability to freely express their opinions and ideas.[96] In theory, it should be illegal to process biometric data for the purpose of uniquely identifying people unless the strictest guidelines are followed.[97] Numerous instances of identity mistakes

---

[89] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 13.

[90] Ibid., 16.

[91] European Parliament. AI (Part 1). 00.36.53.

[92] European Parliament Multimedia Centre. Artificial Intelligence: Impact on Culture - Ambiance shots of the CULT Committee Meeting and statement by Sabine Verheyen (EPP, DE), rapporteur. European Parliament 2021. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-impact-on-culture-ambiance-shots-of-the-cult-committee-meeting-and-statement-by-sabine-verheyen-epp-de-rapporteur_I203299 00.00.00.

[93] AI Act: Poening Statements 00.12.09- 00.12.38.

[94] European Parliament. AI (Part 1),00.04.38.

[95] AI Act: Opening Statements 00.02.28.

[96] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 13.

[97] European Parliament. AI in Criminal Law, 00.00.13.

and system abuse have resulted from the deployment of AI systems for mass surveillance and remote biometric FRT.[98] False positive and false negative rates can be quite high for FRT, and gender and racial biases can result in various forms of discrimination against specific groups as women, people of colour, and children, especially in disadvantaged communities. FRT's accuracy vary significantly and being less accurate for women and persons of colour than for white males, has been particularly well-documented. It is more likely that persons of colour and those with darker skin tones will face discrimination in the context of law enforcements use of FRT.[99] Algorithms may reinforce remaining social and racial prejudices, which might lead to the perpetuation of discriminatory behaviours through AI.[100] The Council of Europe's Guidelines on FRT, states that its necessary for organizations utilizing FRT, as well as for developers or manufacturers of such technologies, to take precautions to guarantee the accuracy of facial recognition data. They must refrain from mislabelling in order to adequately test their systems, detect and eliminate discrepancies in accuracy, particularly with regard to demographic variances in skin colour, age, and gender, and so prevent unintentional prejudice.[101]

The use of closed-circuit television (CCTV) has not shown any improvements in security measures.[102] The deployment of CCTV have instead increases the possibility of misuse and a great number of innocent individuals have been detained based on erroneous accusations.[103] It is unadvisable to cede the right to privacy to technology.[104] The European Union needs a regulatory tool that states that not all infrastructures are equally dangerous and that values such as democracy, freedom of expression, human dignity, security, or fundamental rights as intellectual property, privacy, and consumer protection, cannot be compromised.[105] Opponents

---

[98] European Parliament. AI (Part 2), 00.30.04.

[99] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 7.

[100] European Parliament. AI (Part 2), 00.25.43.

[101] Council of Europe, Guidelines on Facial Recognition, 2021, 9.

[102] AI Act: Opening Statements 00.03.32.

[103] European Parliament. AI (Part 1). 00.36.53.

[104] European Parliament. AI (Part 2), 00.30.04.

[105] Ibid., 00.04.22.

to FRT state that a balance must be struck between innovation and preventing threats to fundamental rights. Citizens' fundamental rights cannot be sacrificed in the sake of security and crime prevention.[106] To ensure the ethical and moral application of AI, safety, dependability, and trustworthiness must be given top priority during development and use. Protecting people' fundamental rights during its implementation and use is essential under EU legal framework.[107] The use of biometric data for identification in public spaces runs the potential of gravely violating people's right to privacy and other fundamental democratic values. [108] Not only is FRT dangerous, but it is a false equivalence that a calculation is intrinsically more moral than a person.[109] AI technologies used as FRT will directly prevent people from exercising their rights to free speech, association, assembly, and even mobility. [110] Even publicly available information, like a visit to a business or a purchase we make there, may be considered private if it is taken out of its original context and coupled with other information to create a detailed profile of our habits and preferences. The anonymity and transparency of a specific data type and the information flow needs to be considered. Improper information flow causes privacy violations.[111]

An ethical quandary surrounding FRT, and other biometric techniques is the question over the transparency of 'who' owns the data. In the absence of such safeguards, there is a chance that private information might end up in the hands of the dark web.[112] Hackers and criminal organizations in Europe have shown the ability access to computer systems used by public and private organizations and healthcare, targeting facilities in Italy, France, Germany, and Spain, and their ability to operate.[113] There is also a worry regarding deepfakes which are manipulated data in which a person appears to say or do something they did not truly say or do using AI

---

[106] European Parliament. AI in Criminal Law, 00.03.24

[107] European Parliament. AI (Part 1). 00.15.57.

[108] European Parliament. AI in Criminal Law, 00.11.41.

[109] Ibid., 00.11.41.

[110] Ibid., 00.06.60.

[111] Malkin, Contextual Integrity, 59.

[112] AI: Impact on Culture, 00.01.00.

[113] European Parliament. AI in Criminal Law, 00.25.43.

tools use of previous data. People walk the streets unaware that facial recognition cameras are tracking, following, and identifying individuals.[114] Facial data may be acquired remotely without the subject's awareness, and when the technology is used in public areas, getting the subject's consent is extremely challenging. As data sets increase, the use of deep learning techniques makes it very hard to do human verification and labelling, which allows for the collection of extremely sensitive information on a very large number of individuals.[115]

The assumption of innocence, a fundamental component of our democratic institutions, is undermined by the substantial possibility of misuse in such circumstances.[116] Information should flow in a way that respects the norms of the specific informational environment in which it is presented, emphasizing the notion of contextual integrity. Information that is disseminated in a way that deviates from these firmly embedded standards is considered improper and violates privacy. Privacy is maintained when information complies with the dominant contextual standards. On the other hand, violating these standards compromises privacy. Privacy concerns do not just dismiss because a person agrees to accept terms and conditions of FRT.[117] These factors constitute a context, respective roles, activities, purposes, and information types do not exist in a context.[118]

7 FRTs Potential Effects on Privacy

Privacy has many definitions and can vary from different contexts and cultures. Norms can derive different ethical qualities and standards based on previous history, cultures, religions, and geopolitics. For example, they might be ‘strict’ or ‘loose’, come from different places, be required or emergent, be codified in laws, change over time and throughout cultures, and be widely or locally recognized.[119] There is no simple answer to the potential effect on privacy of

[114] Ibid., 00.11.41.

[115] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 5.

[116] European Parliament. AI in Criminal Law, 00.06.06.

[117] Malkin, Contextual Integrity, 60.

[118] Nissenbaum, Contextual integrity, 227.

[119] Malkin, Contextual Integrity, 60.

individuals as the individual's personal conception of privacy varies. The indetermined complexity of privacy when applied to different situations is a core tenant of this paper, and how privacy may affect individuals in different ways.[120]

The usage of FRT in public domains as mass surveillance is the most common violation of the right to privacy under EU law. FRT surveillance can affect, individuals' sense of privacy, the presumption of innocence and give unwarranted suspicion, while others may not perceive to be affected by it.[121] FRT in public areas may impede someone's ability to freely act, express their thoughts and opinions, as well as negatively impact their ability to assemble and form associations.[122] Transparency and privacy protection are emphasized as core values in the European approach.[123] There constant juxtaposition between security and privacy, the ownership of data and the misuse of data, deepfakes and manipulation of data.[124] Contextual norms are described or identified according to several criteria, including data type, data topic, sender, recipient, and transmission principle. Data might be collected to develop FRT, anticipating that the information would be used for offering services. In such cases individuals would likely find it invasive if personal information was used for commercial gain. If one is unaware of the nature or subject matter of the material, they are unable to consent how it should be shared.[125]

As AI and FRT become more integrated, more personal data is continuously collected and analysed by surveillance cameras or closed-circuit television (CCTV) networks. The application of enhanced AI technology as FRT results in invasive consequences for data protection and individual privacy.[126] The usage of FRT can give an element of controlling citizens and effect individuals' sense of freedom of expression, human dignity, security and

---

[120] European Parliament. AI in Criminal Law, 00.31.58

[121] European Parliament. AI in Criminal Law, 00.06.06.

[122] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 8.

[123] European Parliament. AI (Part 2), 00.12.14.

[124] European Parliament. AI in Criminal Law, 00.16.22.

[125] Malkin, Contextual Integrity, 60-61.

[126] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 6.

fundamental rights as privacy, intellectual property, and consumer protection.[127] Contextual Integrity (CI) rejects strict categorizations like "secret" against "not secret" or "private" versus "public," and states that privacy should be seen as a fluid concept. The perception of privacy varies from situation to situation. Publicly available information such as a visit to a store or a purchase made, can be viewed as private information if taken out of its original context. This is reflected in the example of when information is combined to create a comprehensive profile of our travel or purchasing habits.[128]

Facial data may be collected remotely, and personal data collected without the subject's awareness or consent. According to the GDPR's transparency principle Article 5(1)(a), people must be informed about the purposes, means, and extent of the collection, use, consultation, and processing of their personal data.[129] However, people ought to be made aware of monitoring by means of an inconspicuously or clearly placed warning sign, informing citizens so that they may identify the conditions surrounding surveillance before accessing the observed area. Obtaining the subject's consent can be complicated when the technology is used in public areas.[130] Privacy is preserved when information that is created by a practice or activity that conforms to the "acceptable" CI standards, and privacy is "damaged" when such rules are violated. Privacy concerns don't just disappear, even if one chooses to "accept" FRT in a situation.[131] Consideration must be given to the objectives, values, and roles within a context, as well as the interests of the parties involved and the political and moral principles at stake. Prioritizing the interests of all parties involved is followed by a more thorough examination of ethical considerations, which includes ideals such as justice, equality, freedom of expression, personal autonomy, and privacy.[132]

---

[127] European Parliament. AI in Criminal Law, 00.16.22.

[128] Malkin, Contextual Integrity, 59.

[129] General Data Protection Regulation. Art. 5(1)(a), GDPR. Principles relating to processing of personal data. 2024. https://gdpr-info.eu/art-5-gdpr/.

[130] Madiega & Mildebrath. Regulating Facial Recognition in the EU, 5.

[131] Malkin, Contextual Integrity, 59.

[132] Malkin, Contextual Integrity, 59,62.

The EU requires legislation that regulates AI in form of FRT to protect individuals right to privacy. European governments legal responsibility is not limited to legislation. For it to be genuinely successful, it also needs innovation, investment, and education.[133] The significance of assessing data flows and developing standards within their specific settings is emphasized by CI. The interests of the parties affected and reflected concerns should be prioritized, and then wider ethical considerations, such as equality, fairness, freedom of speech, and individual autonomy are examined.[134] Freedom of expression, exploration, innovation, and other positive qualities and results are made possible by privacy.[135] As the debate in the European parliament pointed out, FRT in public areas is unacceptable due to the technology is not free from errors and the many instances of misidentification. System abuses involving the use of FRT, and mass monitoring is another risk that violates the right to privacy.[136] AI can reinforce discriminatory practices and endanger people's right to privacy in various ways.[137] Several standards may emerge from the interaction of various situations, cultures, and values; some of these standards may even be in opposition to one another. As a result, perspectives of the recognized norm could differ, and CI could not be able to provide a solution in such circumstances.[138]

8 Discussion and Conclusion

The usage of FRT is complex. The commentary made during the European Parliamentary debates on the AI Act demonstrate how the arguments for and against FRT overlap depending on one’s perception, bias, and gains from the technology. FRT is efficient to identify persons in public spaces when looking for a suspect or a missing person. At the same time, the citizens are being watched on a grand scale and thus it can be defined as mass surveillance which comes with many risks of violation of fundamental rights. On the other hand, it is each governments duty to protect its citizens. In addition to showing how fundamental rights and security efforts

[133] European Parliament. AI, MEPs debate, 00.07.41.

[134] Malkin, Contextual Integrity, 62.

[135] Ibid., 64.

[136] European Parliament. AI (Part 2), 00.30.04.

[137] European Parliament. AI in Criminal Law, 00.35.37

[138] Malkin, Contextual Integrity, 60.

might lie in opposition, this paper underpins the necessity for a balance between privacy rights and surveillance, as well as how digital surveillance can impact the privacy of individuals.

The previous research adds different viewpoints and set of insights to the discussion about the implications of FRT. The study by Andrejevic and Selwyn highlights concerns about the invasion of privacy, the erosion of civil liberties, and the normalization of surveillance technology in schools as it critically explores the usage of FRT in educational settings.[139] Dauvergne's study, advocates for the outlawing of FRT in surveillance and law enforcement because of the grave dangers it presents to civil society. These include the possibility of biased enforcement, activity suppression, and threats to individual safety.[140] The study "Policy designs for adaptive governance of disruptive technologies, the case of facial recognition technology in China" holds a focus on stakeholder engagement, policy mix, and regulatory sandbox techniques in its discussion of the necessity for adaptive governance frameworks to regulate disruptive technologies like FRT.[141] Bu Qingxiu in contrast, provides a comprehensive analysis of the privacy, legal, and ethical concerns surrounding Automated Facial Recognition (AFR) technology, emphasizing the absence of established legal frameworks and the necessity of global governance structures and AFR-specific laws.[142] The authors Nikki Stevens and Os Keyes study the political aspects of FRT technology and the discriminatory effects of monitoring. Databases are shared across sectors, eclipsing barriers and encapsulating power dynamics with their massive picture and information contents. Portraying FRT as a mechanism upholding governmental power structures via monitoring.[143] Nesterova et al. looks at how FRT affects fundamental rights and values, with a focus on privacy issues, prejudice, and discrimination, as well as the requirement for extensive global governance mechanisms to control its use.[144] Naker and Greenbaum examines legislative frameworks and consumer advocacy to address concerns about data breaches, the removal of anonymity, and privacy

[139] Andrejevic & Selwyn, Facial recognition technology in schools: critical questions and concerns,116–126.

[140] Dauvergne, Facial recognition technology for policing and surveillance in the Global South, 2325–2328.

[141] Zhizhao et. Al. Policy designs for adaptive governance of disruptive technologies, 27–40.

[142] Qingxiu, The global governance on automated facial recognition, 113–118.

[143] Stevens & Keyes, Seeing Infrastructure, 833-835.

[144] Nesterova, Mass Data Gathering and Surveillance, 1-8.

infringement. It additionally discusses privacy problems pertaining to FRT technology.[145] Kostka et al, inspects public perception of FRT in several nations, pointing out differing levels of acceptance and worries about privacy infringement and discriminatory behaviours.[146] Jacques, analyses how the five permanent members of the UN Security Council use FRT, delving into uses in national security and exploring privacy and equity concerns, especially with regard to discrimination based on race and gender.[147] E. Roy, surveys the possible threat that FRT poses to free expression, how it affects constitutional rights and suggests strict regulation to lessen First Amendment violations.[148] Throughout previous studies the usage and consequences of FRT is examined and considered in a variety of situations and standards. Overall, the studies draw attention to worries about invasions of privacy, transgressions of civil rights, and the possibility of bias and discrimination brought on by the widespread use of FRT. The findings highlight the necessity of ethical deliberations, regulatory frameworks, and public education on the use of FRT. They generally highlight the significance of addressing the ethical, legal, and social consequences of FRT to protect fundamental rights and values in society, despite variations in geographic focus, methodological approach, and specific areas of concern.

There are many similarities between the paper´s result and the results of previous studies, such as the significant societal risks associated with FRT surveillance, biased law enforcement, activity suppression, safety threats, concerns about privacy infringement, the erosion of civil liberties, and the normalization of surveillance technology. The debate over the need for adaptive governance frameworks to control disruptive technologies such as FRT to handle the myriad of privacy, legal, and ethical issues surrounding FRT is an ongoing discussion open for the readers interpretation based on the material provided. This paper has contributed arguments pro et contra FRT in Europe, how privacy is expected to be affected by FRT, and how complexities of privacy. It gives a detailed understanding of FRT and difficulties to draw a line between the pro et contra arguments since arguments flows overlap depending on the users perspective and affects. Privacy as a concept is hard to define, and this study emphasises the complexity of how rights can be in opposition to each other when debated from different point

---

[145] Naker & Greenbaum,Now You See Me: Now You Still Do, 88-122.

[146] Kostka et. Al. Under big brother's watchful eye, 1-20.

[147] Jacques, Facial Recognition Technology and Privacy,111-156.

[148] Roy, Defrosting the Chill, 185-210.

of views. Dictionary definitions and other sources abound, but when it comes to practical application, privacy is a complex theory to scrutinize and define.

The first question in this paper is "What is the context of human rights mentioned when discussing pro et contra of Facial Recognition Technology (FRT) in the context of European Union (EU) law?". The question is answered in the paper under two different topics, "arguments pro the usage of FRT" and "arguments pro the usage of FRT".

The main pro reasoning in the usage of FRT are for law enforcement to prevent crime, identify missing persons and suspected criminals, protect citizens, and create a greater threshold of safety. FRT is an efficient tool and law enforcement currently rely heavily on FRT both in public spaces and online.[149] FRT is an useful aid to battle crime such as money laundering, the financing of terrorism, the organisation of terrorism, human trafficking for the purpose of various forms of exploitation, including sexual and labour, and viral content pertaining to child sexual abuse to identify victims, offenders, and abuse location.[150] The technology is relatively new, and therefore it should be developed in order to be as trustworthy as possible.[151] Preventive measures are significantly more effective since law enforcement may detect possible crimes before they occur.[152] Within the parameters of strict oversight, the use of FRT must be limited, appropriate, and always accompanied by human supervision. As long as data is kept properly and not shared, it does not intrinsically violate privacy when used for its original purpose, such as finding missing people or apprehending criminals. Only the parties directly engaged should have access to this data; it should not be distributed to outside parties.[153]

The contra reasoning holds that mass monitoring and controlling citizens are strictly prohibited in Europe. The usage of FRT can be a way for states to 'control' citizens, creating a standard of constantly being monitored and followed that violates fundamental rights. The technology is not advanced enough, misidentifications occur and have led to unacceptable risks of errors and violations that would only be discovered after the fact by the supervisory authorities. In the

---

[149] European Parliament. AI in Criminal Law, 00.00.13.

[150] Ibid., 00.26.57.

[151] Ibid., 00.09.21.

[152] Ibid., 00.25.43.

[153] Malkin, Contextual Integrity, 59-60.

worst case it can lead to convictions, and detainments on wrongful accusations.[154] Surveillance limits freedom, diversity, and dissent, rejecting a society characterized by total obedience.[155] The European Union need laws that declares that values that cannot be sacrificed include, human dignity, democracy, freedom of speech, and security, as well as basic rights like intellectual property, privacy, and consumer protection.[156] Even publicly accessible data may be considered private if it is taken out of its original context and integrated with other data to create a comprehensive behavioural profile.[157] Even if someone accepts the terms and conditions of FRT, privacy problems still exist, consent cannot be acquired without proper transparency and education on FRT. Individual roles, activities, goals, and data kinds are all part of a context.[158]

The second research question is "in regards to Facial Recognition Technology (FRT) what are the expectations of any effects on privacy of the individual?" This paper shows the complexity of the understanding of privacy. Privacy has many definitions and can vary from different contexts and cultures; norms can hold different qualities. For example, they might be strict or loose, come from different places, be required or emergent, be codified in laws, change over time and throughout cultures, and be widely or locally recognized.[159] As a result, several norms may emerge from the interaction of various situations, cultures, and values. Some of these norms may even be in opposition to one another. As a result, perspectives of the recognized norm could differ, and it might be hard to provide a solution in some circumstances.[160] In terms of context and the lack of a precise definition of privacy, there is a cultural, individual, and political dimension. It is a multifaceted issue where different aspects come into play. The paper highlights the challenges that arise when trying to introduce expectations of protections for privacy. It is difficult to refer to expectations of something concrete when there is no clear

[154] European Parliament. AI in Criminal Law, 00.06.06.

[155] European Parliament. AI (Part 1), 00.36.53.

[156] European Parliament. AI (Part 2), 00.04.22.

[157] Malkin, Contextual Integrity, 60.

[158] Nissenbaum, Contextual integrity, 227.

[159] Malkin, Contextual Integrity, 60.

[160] Ibid., 60.

definition to start from. Privacy is complex, it affects individuals but does not have to affect individuals, it depends on their perception.

There is yet no specific law safeguarding privacy from FRT. Even in a scenario where citizens are in agreement that their privacy has not been infringed thus far, it might be a good idea to enact regulations to attempt and modify the norm to safeguard the right to privacy in the future. Technology is developing rapidly, and it is a challenge to keep up both on a legal and technical level, as underscored by this paper. The issue of privacy has significant social relevance and will probably grow to more prominence in the future. It is crucial that human rights researchers are ever present and continue to ask questions based on humanitarian and international law principles. For future research an interesting possibility would be to analyse what people's experience of privacy is based on juxtaposing cultural norms within Europe. How do individuals view privacy and Facial Recognition Technology in Europe? Though not the focus of this paper, further interesting questions such as these remain.

Bibliography

Amnesty International. Ban the Scan. Amnesty International 2024. https://www.amnesty.se/agerahub/ban-scan/. (Access 17-04-2024).

Amnesty International. Decode: A New AI Tool to Detect Facial Recognition in Your Photos. Amnesty International 2024. https://banthescan.amnesty.org/decode/ (Access 17-04-2024).

Andrejevic, Mark & Selwyn, Neil. Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, vol. 45:2, 2020:115-128.

Bélanger, France & Crossler, Robert E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *Management Information Systems Research Center, University of Minnesota. MIS Quarterly,* Vol. 35, No. 4 2011:1017-1041.

Björnsson, Gunnar & Kihlbom, Ulrik & Ullholm, Anders. Argumentationsanalys, färdigheter för kritiskt tänkande. *Natur & Kultur Akademisk*, 2009:1-204.

Boréus, Kristina & Bergström, Göran. Textens mening och makt, metodbok i samhällsvetenskaplig text- och diskursanalys. *Studentlitteratur AB*, 2018:1-144.

Clarke, Roger. A Framework for Analysing Technology's Negative and Positive Impacts on Freedom and Privacy. *Datenschutz und Datensicherheit*. Volume 40, 2016:79–83

Clarke, Roger. Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM.* Vol. 42:2, 1999:60.

Convention 108. Guidelines on Facial Recognition. Council of Europe. 2021, 1-16.

Crumpler, William & A. Lewis James. How Does Facial Recognition Work? A Primer. *Center for strategic and International Studies (CSIS).* 2021:1-16.

Directive (EU) 2016/680 of the European Parliament and of the Council. *Official Journal of the European Union*, L 119/89, 27 April 2016. https://eur-lex.europa.eu/eli/dir/2016/680/oj (Access 14-03-2024).

Dauvergne, Peter. Facial recognition technology for policing and surveillance in the Global South: a call for bans. *Third World QuarTerly*, Vol. 43, No. 9, 2022:2325–2328.

European Data Protection Supervisor. *Data Protection*. 2024. https://edps.europa.eu/data-protection/data-protection_en (Access 14-03-2024).

European Court of Human Rights. Council of Europe. European Convention on Human Rights. https://www.echr.coe.int/documents/d/echr/Convention_ENG (Access 14-03-2024).

European Parliament Multimedia Centre. Artificial Intelligence Act: Extracts from the Debate. European Parliament. 2023. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-extracts-from-the-debate_I242459 (Access 30-04-2024).

European Parliament Multimedia Centre. Artificial Intelligence Act - MEPs debate. *European Parliament.* 2024. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-meps-debate_I254282. (Access 27-04-2024).

European Parliament Multimedia Centre. Artificial Intelligence Act: MEPs Debate (Part 1) *European Parliament.* 2023. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-meps-debate-part-1_I242315. (Access 30-04-2024).

European Parliament Multimedia Centre. Artificial Intelligence Act - MEPs debate (Part 2). *European Parliament.* 2023. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-meps-debate-part-2_I242707. (Access 27-04-2024).

European Parliament Multimedia Centre. Artificial Intelligence: Impact on Culture - Ambiance shots of the CULT Committee Meeting and statement by Sabine Verheyen (EPP, DE), rapporteur. *European Parliament.* 2021. https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-impact-on-culture-ambiance-shots-of-the-cult-committee-meeting-and-statement-by-sabine-verheyen-epp-de-rapporteur_I203299 (Access 29-04-2024).

European Parliament Multimedia Centre. Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters - MEPs debate. *European Parliament.* 2021 https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-in-criminal-law-and-its-use-by-the-police-and-judicial-authorities-in-criminal-matters-meps-debate_I211311. (Access 25-04-2024).

European Parliament Multimedia Centre. Artificial Intelligence Act: Opening Statements by Brando Benifei and by Dragoș Tudorache (rapporteurs), by Eva Maydell, Marcel Kolaja, Axel Voss, by Margrethe Vestager, Thierry Breton, and by Susana Solís Pérez and Josianne Cutajar. *European Parliament. 2021.* https://multimedia.europarl.europa.eu/en/video/artificial-intelligence-act-opening-statements-by-brando-benifei-and-by-dragos-tudorache-rapporteurs-by-eva-maydell-marcel-kolaja-axel-voss-by-margrethe-vestager-thierry-breton-and-by-susana-solis-perez-and-josianne-cutajar_I242314. (Access 30-04-2024).

General Data Protection Regulation. Art. 5 GDPR. Principles relating to processing of personal data. 2024. https://gdpr-info.eu/art-5-gdpr/ (Access 14-03-2024).

General Data Protection Regulation. Art. 17 GDPR. Right to erasure (‘right to be forgotten’) 2024. https://gdpr-info.eu/art-17-gdpr/ (Access 14-03-2024).

Harry Aniulis, "Facial Recognition Technology, Privacy and Administrative Law," *University of New South Wales Law Journal 45*, no. 4, 2022: 1513-1555.

International Covenant on Civil and Political Rights, General Assembly resolution 2200A (XXI). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (Access 14-03-2024).

Jacques, Lindsey. Facial Recognition Technology and Privacy: Race and Gender - How to Ensure the Right to Privacy Is Protected, *San Diego International Law Journal*. Vol. 23, no. 1, 2021: 111-156.

Kostka, Genia & Steinacker, Léa & Meckel, Miriam. Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly* Vol. 40, Issue 1, 2022:1-20.

Li Qinjun, Cui Tianwei, Zhao Yan & Wu Yuying, Facial Recognition Technology: A Comprehensive Overview. *Academic Journal of Computing & Information Science*. Vol. 6, Issue 7, 2023:15-26.

Lixiang, Li & Xiaohui, Mui & Siying, Li & Haipeng, Peng. 2016. A Review of Face Recognition Technology. *Information Security Center.* Vol. 4, 2016:27-40.

Madiega, Tambiama & Mildebrath, Hendri. Regulating Facial Recognition in the EU. European Parliamentary Research Service. *Brussels, European Union.* 2021. 1-37.

Malkin, Nathan. Contextual Integrity, Explained: A More Usable Privacy Definition. Usable Security and Privacy for Security and Privacy Workers. *University of Maryland and University of California, Berkeley.* 2023:58-65.

Naker, Sharon & Greenbaum, Dov. 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*. Vol. 23, no. 1, 2017: 88-122.

Nesterova, Irena. Mass Data Gathering and Surveillance: The fight against facial recognition technology in the globalized world. *Globalization and its Socio-Economic Consequences.* 2019:1-8.

Nissenbaum, Helen. Contextual integrity up and down the data food chain. *Theoretical Inquiries Law*. Vol. 20, no. 1, 2019: 221–256.

Official Journal of the European Union C 326/391. *Charter of Fundamental Rights of the European Union* (2012/C 326/02). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN (Access 14-03-2024).

Olszewska, Joanna Isabelle. Automated Face Recognition: Challenges and Solutions. *University of Gloucestershire.* 2016. https://www.intechopen.com/chapters/52911 (Access 14-03-2024).

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

Roy, Kirsten E. Defrosting the Chill: How Facial Recognition Technology Threatens Free Speech. *Roger Williams University Law Review.* Vol. 27, no. 1, 2022:185-210.

Stevens, Nikki & Keyes, Os. Seeing Infrastructure: Race, Facial Recognition and the Politics of Data. 833-835. *Routledge Taylor & Francis group*. Vol. 35, 2021:833–853

Universal Declaration of Human Rights. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf (Access 14-03-2024).

Vetenskapsrådet. Ethics in research and good research practice. 2019. https://www.vr.se/english/mandates/ethics/ethics-in-research.html (Access 14-03-2024).

Vetenskapsrådet. Good Research Practice. 2017. https://www.vr.se/analys/rapporter/vara-rapporter/2017-08-29-god-forskningssed.html (Access 14-03-2024).

Zhizhao, Lia & Yuqing, Guoa & Masaru, Yarimea & Xun, Wu. Policy designs for adaptive governance of disruptive technologies: the case of facial recognition technology (FRT) in China. *Policy Design and Practice*. 2023. Vol. 6, NO. 1, 2023:27–40.