CLARA MAIA PINTO RIBEIRO

The Exchange of Biometric Data Across Borders in the EU: An Area of Security or Mass Surveillance?

Assessing the Implications of the Inclusion of Facial Images in Regulation Prüm II to the Fundamental Rights to Privacy and Data Protection

Dissertation to obtain a Master's Degree in Law, in the specialty of International and European Law

Supervisor:

Dr. Graça Canto Moniz, Professor of the NOVA School of Law

December 2024

Anti-Plagiarism Statement

I, Clara Maia Pinto Ribeiro, hereby declare that I am the sole author of this dissertation and that all contributions, ideas, or texts of others used within this work have been appropriately referenced. I am fully aware that plagiarism constitutes a serious ethical and academic offence.

Para os meus avós

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Professor Graça Canto Moniz, for her guidance, availability, and support throughout this process. Her expertise was essential for this dissertation to achieve the desired outcome.

To Cindy, Cláudia, Mariana, and Theresa, my sincerest thanks for standing by my side over these past two years, motivating and inspiring me to always give my best. It was an immense privilege to get to know you and to share this journey with you!

To my friends and Tomás, who are a source of strength and inspiration, thank you for motivating me to always embrace the difficult path, just as you do, and for always being there, supporting me along the way.

Finally, I wish to convey my most heartfelt gratitude to my family, who have always unconditionally encouraged me. Thank you for believing in me, for helping me pursue my dreams, and above all, for always showing me that I am capable of achieving more than I imagine.

Quoting

The citations, references and bibliography in this dissertation are formatted according to the OSCOLA (Oxford University Standard for Citation of Legal Authorities). The dissertation is written in British English.

Abbreviations

AI	Artificial Intelligence
AI Act	Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act)
The Charter	Charter of Fundamental Rights of the European Union
CCTV	Closed-Circuit Television
CJEU	Court of Justice of the European Union
Convention 108	Convention 108+ Convention for the Protection of Individuals with regard to the Processing of Personal Data
DNA	Deoxyribonucleic acid
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EPRIS	European Police Records Index System
EU	European Union
EUDPR	Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018
eu-LISA	European Union Agency for the Operational Management of Large-Scale Information Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
FRA	European Union Agency for Fundamental Rights
FRT	Facial Recognition Technology
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)
LED	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive)
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MEP	Member of the European Parliament
TELEFI	Towards the European Level Exchange of Facial Images
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
U.S.	United States
WP29	Article 29 Working Party

The body of this dissertation, including notes and spaces, contains a total of 163 004 characters.

‘The welfare of the people in particular has always been the alibi of tyrants, and it provides the further advantage of giving the servants of tyranny a good conscience’

Albert Camus, *Resistance, Rebellion, and Death* (Knopf 1966)

Abstract

Regulation Prüm II, adopted on 13 March 2024, aims to enhance information exchange between Member States' law enforcement authorities for the prevention, detection, and investigation of criminal offences. To achieve this, the Regulation establishes conditions and procedures for the automated search and exchange of DNA profiles, dactyloscopic data, vehicle registration data, facial images, and police records.

This dissertation argues that the inclusion of facial images, given their sensitive nature and ease of collection in public spaces, raises profound concerns regarding fundamental rights, particularly the rights to privacy and data protection. Additionally, the employment of facial recognition technology to process these images risks enabling mass surveillance, thereby amplifying the tension between security imperatives and individual freedoms.

The analysis explores the characteristics of facial images and the role of facial recognition technology in their processing, emphasising the resulting limitations on fundamental rights and the facilitation of mass surveillance. Through a comparative approach, this dissertation assesses the types of facial images collected and stored in national databases across different Member States, alongside the types of crimes that justify the exchange of such images.

Ultimately, the dissertation critically assesses whether the inclusion of facial images in Regulation Prüm II complies with Article 52(1) of the Charter of Fundamental Rights of the European Union, which requires that limitations on fundamental rights be legally provided, necessary, and proportionate. It concludes with recommendations to mitigate the impact on fundamental rights while preserving the Regulation's internal security objectives.

Keywords: Prüm II, Facial Images, Facial Recognition, Mass Surveillance, Fundamental Rights, Article 52(1), Proportionality

Resumo

O Regulamento Prüm II, adotado a 13 de março de 2024, visa potenciar a troca de informações entre as autoridades responsáveis pela aplicação da lei dos Estados-Membros para a prevenção, deteção e investigação de infrações penais. Para o efeito, o Regulamento estabelece condições e procedimentos para a pesquisa e a troca automáticas de perfis de ADN, dados dactiloscópicos, dados relativos ao registo de veículos, imagens faciais e registos policiais.

A presente dissertação argumenta que a inclusão de imagens faciais, dado o seu caráter sensível e a facilidade de recolha em espaços públicos, suscita profundas preocupações no que respeita aos direitos fundamentais, nomeadamente os direitos à privacidade e à proteção de dados. Além disso, a utilização da tecnologia de reconhecimento facial para processar essas imagens acarreta o risco de viabilizar a vigilância em massa, amplificando, assim, a tensão entre as exigências de segurança e as liberdades individuais.

A análise explora as características das imagens faciais e o papel da tecnologia de reconhecimento facial no seu processamento, salientando as limitações daí resultantes para os direitos fundamentais e a facilitação da vigilância em massa. Através de uma abordagem comparativa, a presente dissertação avalia os tipos de imagens faciais recolhidas e armazenadas em bases de dados nacionais de diferentes Estados-Membros, bem como os tipos de crimes que justificam a troca dessas imagens.

Em última análise, a dissertação avalia criticamente se a inclusão de imagens faciais no Regulamento Prüm II está em conformidade com o Artigo 52(1) da Carta dos Direitos Fundamentais da União Europeia, que exige que as limitações aos direitos fundamentais sejam legalmente previstas, necessárias e proporcionais. A análise conclui com recomendações para mitigar o impacto sobre os direitos fundamentais, preservando simultaneamente os objetivos de segurança interna do Regulamento.

Palavras-chave: Prüm II, Imagens Faciais, Reconhecimento Facial, Vigilância em Massa, Direitos Fundamentais, Artigo 52(1), Proporcionalidade

Introduction

"You are being watched. The government has a secret system, a machine that spies on you every hour of every day." These frightening words pronounced in the TV series *Person of Interest*[1] echo deeply in an era where the use of surveillance technologies by law enforcement authorities has become a reality.

Globalisation, free movement, and digital transformation have provided multiple benefits, such as wealth, well-being, and innovation. Nevertheless, these advancements also carry inherent risks. Terrorism, organised crime, and other security threats exploit cross-border opportunities, switching seamlessly between the physical and digital worlds.[2] In 2021, over 70% of organised crime groups operated in more than three EU Member States. Even crimes that seem local often have international links and connections between these presumably isolated crimes and organised crime networks are not always evident.[3] Addressing these challenges requires consistent cooperation and information exchange between law enforcement authorities of different Member States.[4]

To enhance security while upholding the common European values of the rule of law, equality, fundamental rights, transparency, accountability, and democratic oversight,[5] the EU adopted Regulation Prüm II on 13 March 2024. This Regulation aims to strengthen the internal security of the EU[6] by facilitating information exchange between Member States, and with Europol, focusing on the prevention, detection, and investigation of criminal offences.[7] Building upon the existing Prüm framework, Prüm II introduces new categories of personal data, including facial images and police records alongside DNA, dactyloscopic data, and vehicle registration information.[8]

This increasing reliance on the exchange of personal data in cross-border law

[1] Jonathan Nolan, 'Person of Interest' (CBS 2011)
[2] Commission, 'Communication from the Commission on the EU Security Union Strategy 2020' (Communication) COM(2020) 605 final
[3] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' COM(2021) 784 final
[4] Ramona Cavalli, 'Prüm II and the EPRIS Index in Europe: An Attempt to Balance People's Security and Privacy?' (2024) 14 CS & IT Conference Proceedings 57, 57 < https://doi.org/10.5121/csit.2024.140706> accessed 3 December 2024
[5] COM(2020) 605 final
[6] COM(2021) 784 final
[7] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) [2024] OJ L, 2024/982
[8] Prüm II Regulation (n 7), recital 4

enforcement cooperation raises important questions regarding compliance with fundamental rights, in particular, the rights to data protection[9] and the right to respect for private and family life.[10] Although these rights are not absolute, as stated by the Court of Justice of the European Union (CJEU),[11] any limitations on them must fulfil the requirements of Article 52(1) of the Charter of Fundamental Rights of the European Union (the Charter).

While Proposal Prüm II's compliance with the principles of necessity and proportionality under Article 52(1) of the Charter has been assessed by the European Commission in its Impact Assessment,[12] as well as by the EDPS[13] and EDRi,[14] significant changes were later introduced in the Regulation's final text. These changes, particularly concerning the inclusion of facial images, leave essential aspects for Member States to regulate through national laws, such as the content of criminal databases and the specific criminal offences justifying the exchange of facial images. Despite these developments, there has been no detailed assessment of the final Regulation's compliance with Article 52(1), nor an analysis of Prüm II's potential to facilitate mass surveillance. Moreover, a comparative analysis of Member States' legal frameworks, practices in employing facial recognition, and differing criminal justice systems remains absent, despite its importance for assessing the Regulation's lawfulness. This dissertation seeks to fill these gaps.

As such, it examines whether the automated search and exchange of facial images between Member States' competent authorities, aimed at preventing, detecting, and investigating criminal offences, complies with the requirements of Article 52(1) of the Charter. Specifically, it explores whether the employment of facial recognition inherently

[9] Charter of Fundamental Rights of the European Union [2012] OJ C 326, art 8
[10] ibid, art 7
[11] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen* [2010] ECR I-0000 cited in COM(2021) 784 final
[12] Commission, 'Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation ("Prüm II"), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' (Commission Staff Working Document) SWD(2021) 378 final
[13] European Data Protection Supervisor, 'Opinion 4/2022 on the Proposal for a Regulation on Automated Data Exchange for Police Cooperation ("Prüm II")' (March 2022) <https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2022-03-02-edps-opinion-regulation-automated-data-exchange-police-cooperation> accessed 14 October 2024
[14] European Digital Rights, 'Respecting fundamental rights in the cross-border investigation of serious crimes A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")' (September 2022) <https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf> accessed 18 October 2024

facilitates state mass surveillance. This analysis does not extend to other data categories exchanged under the Regulation, the role of Europol, or the use of information for locating missing persons or identifying human remains.

The research questions guiding this dissertation are: *Does the inclusion of facial images in Regulation Prüm II align with the principle of proportionality in balancing the fundamental rights to privacy and data protection with the imperative of high-level cross-border security? Does the employment of facial recognition technology by law enforcement authorities inevitably lead to state mass surveillance?* To address them, the analysis is structured into six chapters.

The first chapter provides an overview of the Prüm framework, describing its rationale and examining the challenges and successes of its implementation. Chapter two shifts focus to Regulation Prüm II, examining the context of its adoption, its general scope, and its successes and challenges. Chapter three focuses on the inclusion of facial images under Prüm II, providing an in-depth examination of facial recognition technology, its inherent shortcomings, and the safeguards introduced by the Regulation for the search and exchange of facial images. It also conducts a comparative analysis of facial recognition practices outside the EU, specifically in China and the United States.

Chapter four develops the topic of mass surveillance, providing an examination of remote biometric identification, the implications of mass surveillance for fundamental rights and freedoms, and a critical analysis of biometric surveillance practices currently employed within EU Member States. Following this, chapter five provides a comparative analysis of national legal frameworks, focusing on Member States' differing approaches to the employment of facial recognition technology in law enforcement and the differences in their criminal justice systems. Finally, chapter six conducts a proportionality assessment of the inclusion of facial images under Prüm II, critically verifying its compliance with the requirements of Article 52(1) of the Charter.

Ultimately, this dissertation concludes whether the inclusion of facial images under Prüm II constitutes a lawful limitation of the fundamental rights to data protection and privacy, considering the potential of facial recognition to enable mass surveillance, thereby addressing the research questions.

Methodology

To address the identified gap in the literature, this dissertation provides analytical legal research conducted through systematic legal and literature reviews.

The legal analysis begins with an in-depth examination of Regulation Prüm II, focusing on the provisions governing the search and exchange of facial images. To complement this analysis, other relevant legal instruments were scrutinised, including the Law Enforcement Directive[15] and the Artificial Intelligence Act,[16] both of which intersect with the Regulation's implications for fundamental rights and data governance. Foundational EU legal documents, such as the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union were also addressed due to the impact of the topic on fundamental rights and objectives of general interest.

A comparative analysis of selected Member States' national legal frameworks further enriches the study. Criminal Codes from Portugal, France, the Netherlands, Sweden, Poland, and Germany were reviewed to highlight diverse approaches to the use of facial recognition technology and its alignment with the Regulation.

This systematic legal review was conducted through online platforms such as *EUR-lex*, the *Legislative Train Schedule*, and official Member States governments' *websites*.

The dissertation also draws upon secondary sources, including institutional guidelines, opinions, and reports. Key contributions from institutions such as the European Parliament, European Commission, European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB), European Digital Rights Association (EDRi), and the European Union Agency for Fundamental Rights (FRA) were examined. Additionally, relevant academic articles and case law from the CJEU and the European Court of Human Rights (ECtHR) were analysed to substantiate the arguments presented.

The systematic literature review involved targeted searches on the official

[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2008] OJ L 119

[16] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, 2024/1689

websites of these institutions and academic databases such as *Springer*, *Georgetown Law*, *Google Scholar*, and *SSRN*. In many cases, references found within initial documents led to the identification and analysis of additional relevant sources.

The literature and legal searches employed keywords tailored to the research topic, including *Facial Images, Facial Recognition, Law Enforcement, Prüm II, Databases, Mass Surveillance* and *Proportionality*.

For the comparative analysis, the Member States were selected based on their diversity in legal traditions, criminal justice systems, and approaches to facial recognition technology. This analysis provided critical insights into the interplay between national laws and the implementation of Prüm II, particularly the challenges arising from the Regulation's deferral of certain aspects to Member States.

By combining doctrinal legal analysis, systematic literature review, and comparative analysis, this methodology ensures a comprehensive examination of the research questions.

I. Prüm I

1. Context

In 1999, the European Council recognised the need to enhance information exchange between Member States' authorities for the detection and investigation of criminal offences.[17] This conviction was reinforced in 2004 in the Hague Programme,[18] where the Council stated that law enforcement authorities in one Member State should be able to access the information necessary to perform their duties from authorities in other Member States.[19]

On 27 May 2005, seven EU Member States[20] signed the Treaty of Prüm, which aimed at strengthening efforts to combat terrorism, cross-border crime, and illegal immigration. It established provisions for exchanging DNA, dactyloscopic data, vehicle registration data, and additional measures to improve cross-border police cooperation.[21]

Parallel to this, the Council Framework Decision 2006/960/JHA[22] provided rules for the prompt exchange of information and intelligence among law enforcement authorities for the purpose of criminal investigations. However, these rules fell short of satisfying the requirements of the Hague Programme, which the Treaty of Prüm more effectively addressed.[23]

Given the European Council's deadline to achieve the goals of the Hague Programme, the Treaty of Prüm was formally incorporated into the EU legal framework on 23 June 2008 through Council Decision 2008/615/JHA.[24] To ensure the implementation of this decision, the Council set up the necessary technical and administrative procedures on Decision 2008/616/JAI ("Implementing Decision").[25]

---

[17] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L 210, recital 2
[18] ibid, recital 3
[19] ibid, recital 4
[20] Belgium, Germany, France, Luxembourg, the Netherlands, Austria and Spain.
[21] European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Working document on a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime' (April 2007) <https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824en.pdf> accessed 16 September 2024
[22] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386
[23] Council Decision 2008/615/JHA (n 17), recital 9
[24] ibid, recital 5
[25] Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L 210

These legal instruments required all EU Member States to join the network, thereby reinforcing cooperation across borders in the fight against crime.[26] Since the Prüm Decisions entered into force before the Lisbon Treaty, the European Parliament had a very limited role in their review.[27]

2. Legal Basis and Structure

Prüm I is, as such, composed of two key decisions: 2008/615/JHA and 2008/616/JHA, which together outline the main provisions of the Treaty of Prüm. The framework was established to enhance cross-border cooperation between Member States' authorities responsible for preventing and investigating criminal offences, through the exchange of information. To achieve this goal, decision 2008/615/JHA introduced rules for the automated exchange of DNA profiles, dactyloscopic data and vehicle registration data. Additionally, it addressed the supply of data related to major events with cross-border implications, the prevention of terrorist offences and measures to strengthen police cooperation.[28]

This exchange would occur through automated searches via national contact points, using a "hit/no-hit" procedure[29] to compare data in individual cases. When a match was identified, the Member States involved would share additional personal data and any relevant information, in accordance with national law.[30]

The implementation of the Prüm Decisions required Member States to ensure the availability of data stored in their national databases to other Member States. Those that did not have databases in place had to establish them and enact national legislation to regulate them.[31]

Data searches and exchanges were conducted through a network of bilateral connections between the national databases of Member States. To effectively implement these decisions, each Member State needed to establish a connection with every other

[26] Victor Toom, Rafaela Granja and Anika Ludwig, 'The Prüm Decisions as an Aspirational Regime: Reviewing a Decade of Crossborder Exchange and Comparison of Forensic DNA Data' (2019) 41 Forensic Science International: Genetics 50, 51 <https://doi.org/10.1016/j.fsigen.2019.03.023> accessed 28 October 2024
[27] European Digital Rights (n 14), 4
[28] Council Decision 2008/615/JHA (n 17), art 1
[29] ibid, recital 10
[30] ibid, art 2 to 12
[31] Niovi Vavoula, 'Police Information Exchange - The Future Developments Regarding Prüm and the API Directive' (Think Tank European Parliament 2020), 18 <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)658542> accessed 4 May 2024.

Member State, amounting to 26 connections per Member State per data category.[32]

This comprehensive approach under Prüm I sought to overcome time-consuming, complex, and bureaucratic procedures usually employed in traditional information exchange channels by streamlining data exchange and improving police cooperation.[33]

3. Successes and Challenges

The Prüm framework represented a significant advancement in strengthening cross-border cooperation and information exchange among EU Member States for law enforcement. By optimising intelligence-gathering processes, it enabled the early identification of serious offenders, facilitating preventive actions against lives and property loss. This framework also enhanced the resolution of cold cases, as increased data sharing improved the likelihood of matching unsolved crime data with new information.[34]

However, upon reaching the implementation deadline, the Prüm framework revealed limitations, leading the EU to introduce new measures to improve information exchange. Advances in technology and evolving crime-fighting needs exposed gaps within the initial framework, necessitating updates to its technical and legal standards. Additionally, several Member States delayed the steps required to implement the decisions, creating a lack of bilateral connections and impeding data queries between countries.[35] This was largely due to the technical complexity and resource demands of establishing 26 separate connections per Member State and data category. The absence of complete connectivity hindered effective data exchange across the EU.[36]

A notable gap of Prüm I was its exclusion of Europol, which limited cross-checking of Member States' data with third-country information held by the Agency, potentially leaving connections to serious crime undetected.[37] The framework also did not set out clear procedures for Member States to follow after confirming a match, leaving the process to national laws. This led to inconsistencies in information quality,

[32] COM(2021) 784 final, recital 15
[33] Oriola Sallavaci, 'Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange' (2017) European Journal on Criminal Policy and Research 24(3) 219, 220 <https://doi.org/10.1007/s10610-017-9355-0> accessed 27 October 2024
[34] ibid, 229
[35] COM(2021) 784 final
[36] SWD(2021) 378 final
[37] ibid.

communication channels, and response times,[38] with data sometimes taking weeks or even months to be shared effectively.[39]

Moreover, implementing the framework was complicated by several requirements, such as establishing searchable databases for DNA, dactyloscopic data, and vehicle registration data, meeting minimum data protection standards, and adopting technical specifications. Differences in national legal and administrative frameworks, especially regarding data protection also hindered the implementation.[40]

Prüm I's scope was limited by the lack of effective access to other critical data categories, such as facial images, driving licenses, police records, and ballistics information. Exchanging these categories often required manual proceedings, significantly slowing law enforcement's ability to fight cross-border crime.[41]

Finally, the adoption of Directive 2016/680[42] ('Law Enforcement Directive' or 'LED') in 2016 introduced new data protection standards for law enforcement, necessitating revisions to the Prüm framework to align it with these updated rules.[43]

[38] European Commission Directorate-General for Migration and Home Affairs, 'Study on the Feasibility of Improving Information Exchange under the Prüm Decisions' (Publications Office 2020), 7 <https://data.europa.eu/doi/10.2837/104991> 28 October 2024
[39] COM(2021) 784 final
[40] Sallavaci (n 33), 222 and 225
[41] SWD(2021) 378 final
[42] Directive (EU) 2016/680 (n 15)
[43] Commission 'Way forward on aligning the former third pillar acquis with data protection rules' (Communication) COM(2020) 262 final.

II. Prüm II

1. Context

A decade after implementing Prüm I, the Council underscored the critical role of the automated exchange of DNA, dactyloscopic data and vehicle registration data to combat crime and terrorism across the EU. Prüm I established shared rules, standards, and requirements, improving interoperability among diverse national systems. However, Prüm I's limitations became evident during implementation, revealing several structural and procedural shortcomings.[44]

In 2020, the European Commission introduced the EU Security Union Strategy for 2020 - 2025, aimed at enhancing the security of the EU against evolving physical and digital threats.[45] This strategy seeks to ensure that EU security policies evolve alongside new threats, develop sustainable resilience, promote a comprehensive societal approach, and combine policy areas directly impacting security.[46] It aligns with the Union's objective of offering its citizens an area of freedom, security and justice, which requires swift and effective data exchange between law enforcement agencies.[47]

In this context, Regulation (EU) 2024/982 of the European Parliament and of the Council on the automated search and exchange of data for police cooperation (the Prüm II Regulation) was introduced.

2. General Scope

Prüm II builds on and modernises the Prüm I framework to enhance law enforcement cooperation across the EU.[48] The Regulation's main objective is to improve, streamline and facilitate information exchange between Member States' authorities and with Europol for the prevention, detection and investigation of criminal offences.[49]

To achieve it, Prüm II outlines the conditions and procedures for automated data searches and specific rules for the exchange of core data following a confirmed match. It covers a wider range of data categories than its predecessor, including DNA profiles,

---

[44] COM(2021) 784 final
[45] Commission, 'A New Way Forward on Internal Security' (*European Commission*) <https://home-affairs.ec.europa.eu/policies/internal-security/new-way-forward-internal-security_en> accessed 18 September 2024
[46] Commission, 'European Security Union' (*European Commission* 24 Jul 2020) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en> accessed 18 September 2024
[47] Prüm II Regulation (n 7), recital 1
[48] COM(2021) 784 final
[49] Prüm II Regulation (n 7), recital 2

dactyloscopic data, vehicle registration data, facial images, and police records.[50]

Considering the increasing role played by Europol in receiving biometric data of suspects and persons convicted of terrorism and criminal offences from third countries, Prüm II allows Member States' competent authorities to access data stored by Europol.[51] It also enables Europol to search Member States' databases with third-country data[52] to establish connections between the criminal cases for which the Agency is responsible.[53]

Unlike Prüm I, which relied on a network of bilateral connections between national databases, Prüm II establishes two central connection points: the router and the European Police Records Index System (EPRIS).[54] This hybrid model, balancing decentralisation with centralisation,[55] allows each Member State to establish a single connection regarding biometric data and police records, respectively, facilitating data exchange without any central-level storage.[56]

The Regulation also introduces rules regarding information exchange after a hit,[57] replacing the national-level follow-up system of Prüm I, which was inconsistently applicable across Member States.[58]

3. Legal Basis

Prüm II is legally grounded in Articles 16(2), 87(2)(a) and 88(2) of the Treaty on the Functioning of the European Union (TFEU),[59] which collectively empower the EU to legislate on information exchange and data processing in the context of cross-border cooperation.[60]

The Prüm II framework's core function is the exchange of data, which directly impacts the right to personal data protection, enshrined in Article 8 of the Charter and Article 16 of the TFEU. This right is intrinsically linked to the right to respect for private and family life, protected under Article 7 of the Charter and Article 8 of the European Convention on Human Rights (ECHR).

---

[50] ibid, recital 10.
[51] ibid, recital 20.
[52] According to the provisions of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L 135
[53] Prüm II Regulation (n 7), recital 21
[54] ibid, recital 24
[55] COM(2021) 784 final
[56] Prüm II Regulation (n 7), recital 24
[57] ibid, art 1(b)
[58] COM(2021) 784 final
[59] Prüm II Regulation (n 7)
[60] Treaty on the Functioning of the European Union [2012] OJ C 326

In addition, the Regulation builds on a foundation of EU laws that govern data protection, police cooperation, and the role of Europol, so as to facilitate secure and lawful data exchanges across Member States. In its preamble, the Regulation explicitly states that any personal data processing or exchange shall comply with Directive (EU) 2016/680[61], Regulation (EU) 2018/1725,[62] Regulation (EU) 2016/794[63] and Regulation (EU) 2016/679[64], as applicable regarding the nature and purpose of the data involved.[65]

Regarding the processing of personal data by competent authorities for the prevention, detection and investigation of criminal offences, the applicable data protection legislation is the Law Enforcement Directive (LED).[66]

Moreover, since Prüm II involves coordination with EU institutions, including Europol and eu-LISA, Regulation 2018/1725 sets data protection standards for processing activities conducted by these bodies.[67]

Europol's role in Prüm II is significant, as it facilitates cross-border data sharing and supports Member States by identifying links between criminal cases across national boundaries. This role is supported by Regulation (EU) 2016/794, which establishes Europol's mandate to support and strengthen action by competent authorities of the Member States and their cooperation in preventing and combating serious crime, terrorism and other forms of crime.[68]

Finally, Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR), establishes rules for the protection of persons regarding the processing of personal data[69] for purposes other than law enforcement.[70] Under Prüm II, this regulation applies to personal data processed to locate missing persons or identify human remains outside of criminal investigations.[71]

[61] Directive (EU) 2016/680 (n 15)
[62] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295
[63] Regulation (EU) 2016/794 (n 52)
[64] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119
[65] Prüm II Regulation (n 7), recital 7
[66] Directive (EU) 2016/680 (n 15), art 1(1)
[67] Regulation (EU) 2018/1725 (n 62), art 1(1)
[68] Regulation (EU) 2016/794 (n 52), art 3(1)
[69] Regulation (EU) 2016/679 (n 64), art 1(1)
[70] Directive (EU) 2016/680 (n 15), recital 11
[71] Prüm II Regulation (n 7), recital 7

Overall, Prüm II's legal basis not only empowers the EU to build an integrated law enforcement information-sharing framework but also embeds critical safeguards to protect individual rights, supporting the regulation's dual goals of enhancing security and upholding data protection principles.

4. Successes and Challenges of the Regulation

Prüm II builds on and addresses many limitations of its predecessor, Prüm I. However, some challenges persist, both inherited from the initial Proposal Prüm II and arising from changes made during legislative development.

Regarding the successes, Prüm II introduces a central router, streamlining connectivity by implementing a single connection per Member State without centralised data storage. This hybrid approach significantly reduces the number of connections, simplifying implementation and enabling the collection of statistical data.[72]

The introduction of facial images of suspects and convicted criminals provides an efficient means of data search and comparison, which previously had to be conducted manually. This improvement is particularly useful in investigations where a suspect's image is the only lead captured from the crime scene, thus enhancing the identification process.[73]

Finally, Prüm II regulates the follow-up procedure with a semi-automated exchange of core data corresponding to a match. Once a match between data used for the search and data stored in the database of the requested Member State is verified, a limited set of core data identifying the person is returned to the requesting Member State. The regulation of this step at the EU level is crucial, as it optimises the response time and ensures consistency across jurisdictions. This standardisation of follow-up procedures constitutes a critical improvement in the speed and efficiency of cross-border law enforcement cooperation.[74]

Prüm II, while resolving many issues present in Prüm I, retains several significant shortcomings. Many of them stem from criticisms initially raised by the EDPS during the proposal phase and persist in the adopted text.

The Regulation permits automated searches for the prevention, detection, and investigation of criminal offences punishable by a maximum prison term of at least one

[72] SWD(2021) 378 final
[73] ibid.
[74] ibid.

year, according to the law of the requesting Member State.[75] This approach diverges from the EDPS's recommendation to limit automated searches to serious crimes.[76] Prüm II uses an imprisonment threshold that may or may not reflect serious criminality, depending on the Member State concerned,[77] undermining a uniform, objective search criterion within the EU. This situation can contribute to inequalities among Member States.

Moreover, Prüm II requires Member States to ensure the availability of facial image reference data of suspects, convicted individuals, and, if allowed under national law, victims.[78] It refers to the LED for defining a "suspect"[79] as someone reasonably believed to have committed or be about to commit a criminal offence.[80] However, it provides no definitions for "convicted persons" or "victims," leaving room for interpretation. If following similar reasoning, a "convicted person" would be someone convicted of a criminal offence,[81] and a "victim" could broadly include victims of a criminal offence or any individual reasonably believed to be at risk of criminal harm.[82] The inclusion of victims in searchable categories and the absence of clear definitions of the data subjects contradict the EDPS's guidance to limit searches to suspects and convicted criminals. [83]

Additionally, the Regulation does not specify the sources of facial images, only determining their origin in national databases.[84] While Prüm II assigns the responsibility for image quality to Member States, it does not establish minimum standards within the text, instead deferring these to future implementing acts by the European Commission.[85] This lack of clarity on data sources and quality safeguards, combined with broad access for offences punishable by a maximum term of imprisonment of at least one year, leaves the scope undefined and susceptible to inconsistent implementation, concerns previously raised by the EDPS.[86]

The EDPS also highlighted the need for harmonisation between data protection

[75] Prüm II Regulation (n 7), art 20(1)
[76] European Data Protection Supervisor (n 13), 11
[77] Prüm II Regulation (n 7), art 20(1)
[78] ibid, art 19(1)
[79] ibid, art 4(23)
[80] Directive (EU) 2016/680 (n 15), art 6(a)
[81] ibid, art 6(b)
[82] ibid, art 6(c)
[83] European Data Protection Supervisor (n 13), 11
[84] Prüm II Regulation (n 7), art 19(1)
[85] ibid, art 22(2)
[86] European Data Protection Supervisor (n 13), 10 and 11

frameworks and Prüm II to avoid regulatory ambiguity and ensure cohesive oversight.[87] However, the relationship between Prüm II, the LED, and the EUDPR remains ambiguous, lacking clear guidance on how each framework applies within Prüm II. Although the Regulation mentions the LED and EUDPR at various points, the lack of explicit delineation requires separate consultations of each regulation to interpret their applicability in different contexts.

Finally, Prüm II maintains a decentralised, horizontal governance structure, with each Member State independently managing data exchanges.[88] The Regulation does not assign a centralised EU entity to oversee or coordinate data exchanges, which the EDPS criticised as inadequate, considering the scale and sensitivity of facial images.[89]

Some of these persistent shortcomings will be further developed in the next chapter, together with other issues, particularly related to the search and exchange of facial images within Prüm II.

[87] ibid, 7
[88] This is particularly visible in articles 4, 6, 33 and 52 of the Regulation. These provisions illustrate a decentralised framework where each Member State maintains its own systems, ensures compliance, and is accountable to its national authorities rather than to a central EU body.
[89] European Data Protection Supervisor (n 13), 15

III. Facial Images in Prüm II

1. Inclusion of Facial Images

One of the key innovations introduced by Regulation Prüm II is the inclusion of facial images as a category of personal data that can be searched to prevent, detect, and investigate criminal offences.[90] This development reflects a concerted effort by the law enforcement sector to adapt to technological advances in order to address emerging security threats.[91]

The search and exchange of facial images of convicted criminals, suspects and, potentially, victims aim to equip competent authorities with the necessary information for identifying criminals and fighting crime. Searches are limited to criminal offences punishable by a maximum term of imprisonment of at least one year under the requesting Member State's law. [92]

The Prüm II Impact Assessment underscores the transformative potential of this addition to significantly increase the possibilities of identifying convicted criminals or suspects, as these images are often the only evidence retrieved from a crime scene. Although several EU Member States already maintain national databases for storing facial images of suspects and criminals, the methods vary widely.[93] Some Member States are still in the early stages of developing centralised electronic image databases or implementing facial recognition systems.[94]

Under the Regulation, a facial image is defined as "a digital image of the face"[95] and may be categorised as identified or unidentified, depending on whether the individual is known at the time of collection.[96] Classified as both personal[97] and biometric data,[98] these images contain the physical characteristics of a natural person, whose processing confirms their unique identification.[99] Given their sensitive nature and potential ease of collection in public spaces, the use of facial images raises significant privacy and

[90] Prüm II Regulation (n 7), art 1(a)
[91] Desara Dushi, 'The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications' (Global Campus of Human Rights 2020), 5 <http://dx.doi.org/10.25330/528> accessed 16 October 2024
[92] Prüm II Regulation (n 7), recital 16
[93] SWD(2021) 378 final
[94] Vavoula (n 31), 31
[95] Prüm II Regulation (n 7), art 4(11)
[96] ibid, art 4(14)
[97] Directive (EU) 2016/680 (n 15), art 3(1)
[98] Prüm II Regulation (n 7), art 4(15)
[99] Directive (EU) 2016/680 (n 15), art 3(13)

fundamental rights concerns.[100]

Prüm II establishes the conditions and procedures for the automated searching of facial images across Member States and outlines the rules for exchanging core data upon confirming a match.[101] It mandates that Member States allow national contact points from other Member States access facial image databases for automated searches.[102] Member States must uphold the confidentiality and integrity of these images, adhering to encryption and minimum quality standards to be determined by the Commission through implementing acts.[103]

A shared router established by the Regulation facilitates biometric data exchanges between Member States.[104] This router allows the submission of facial images by authorised authorities, which are then forwarded to Member States databases simultaneously, ensuring prompt automated queries.[105] Transmitted data quality must be checked through automated procedures, with unsuitable data flagged to the requesting Member State.[106] Any matches will be automatically sent back to the router, while non-matches trigger an automated notification of the requesting authority.[107]

The router is also equipped to rank results by comparing biometric data used for querying with the data supplied in the replies and returning a list of potential matches, ranked by similarity, to the requesting Member State.[108] In case of a match, the requesting Member State may confirm it, provided they inform the requested Member State and ensure that the review is manually conducted by at least one qualified staff member.[109] Once the match is validated and relevant information on the offence is provided, a set of core data must be returned to the requesting Member State via the router within 48 hours, unless judicial authorisation requires an extension. [110]

2. Overview of Facial Recognition Technology

The automated exchange and comparison of facial images under Prüm II is conducted through facial recognition systems that rely on biometric templates. These templates are created by extracting specific features from biometric samples, such as

[100] Dushi (n 91), 6
[101] Prüm II Regulation (n 7), art 1
[102] ibid, art 19(1) and art 20(1)
[103] ibid, art 22
[104] ibid, art 35 and art 36
[105] ibid, art 37(1) and (2)
[106] ibid, art 38
[107] ibid, art 37(3)
[108] ibid, art 37(4) and (5)
[109] ibid, art 20(2)
[110] ibid, art 47

facial images, as outlined in the Regulation's preamble. Notably, Prüm II mandates that while biometric templates are derived from original biometric data, it must not be possible to reverse-engineer these templates back into the original data, ensuring a degree of data protection.[111]

The Regulation's binding provisions, however, lack specific technical details on how facial image comparisons will be processed, including the exact technologies and procedures for determining a match. The preamble's reference to facial recognition systems suggests that the provisions governing the implementation and development of this technology will be left for the Commission to regulate in the implementing acts.[112]

Facial Recognition Technology (FRT) is a biometric technology that processes digital images of individuals using face templates[113] and compares them to determine their similarity, which is represented using a score.[114] FRT algorithms do not provide definitive results, as they cannot determine whether two templates belong to the same person, only the probability. Under Prüm II, FRT can be used either preventively, to stop an identified individual from committing a crime, or repressively, to identify someone after a crime has been committed.[115] This dual-use approach aligns with the Regulation's objectives for crime prevention, detection, and investigation.[116]

FRT provides a two-step process that starts with the collection and transformation of a biometric sample (e.g., a facial image) into a digital template representing its unique characteristics. Afterwards, in the recognition phase, this template is compared with other stored templates to determine the likelihood of a match. Since FRT provides an estimated match between templates, its results are merely probabilistic.[117]

FRT can be used either for identification, authentication or categorisation

[111] ibid, recital 27
[112] According to recital 35 of the Prüm II Regulation, technical, highly detailed and frequently changing aspects of the Regulation are left for the Commission to regulate using its implementing powers provided by Regulation (EU) No 182/2011. These aspects include technical arrangements and specifications for automated searching procedures, the standards for data exchange, including minimum quality standards, and the data elements to be exchanged.
[113] European Data Protection Board, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' (April 2023), 9 <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en> accessed 16 November 2024
[114] SWD(2021) 378 final
[115] Vera Lúcia Raposo, 'The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal' (2023) 29 European Journal on Criminal Policy and Research 515, 518 <https://doi.org/10.1007/s10610-022-09512-y> accessed 4 October 2024
[116] Prüm II Regulation (n 7), art 19(1).
[117] European Data Protection Board (n 113), 9 and 10

purposes.[118] Identification involves determining an individual's identity by comparing a facial image to templates stored in a reference database,[119] a process referred to as 1-to-many identification. Authentication, or 1-to-1 verification, checks whether a person is who they claim to be by comparing a single image with a pre-recorded template.[120] Finally, categorisation is applied to assign data subjects to specific categories, based on their biometric data, such as sex, age, religion, sexual or political orientation, etc.[121]

In criminal investigations, the predominant use of FRT is retrospective one-to-many identification. This involves comparing an image of an unidentified individual with a database of known individuals' faces to identify potential matches following a criminal incident.[122] As Prüm II explicitly states that the search of facial images of convicted criminals, suspects, and, potentially, victims aims at identifying offenders and combating crime,[123] it is clear that these images will be used for identification purposes. Consequently, this research will limit its analysis to the identification function of FRT.

3. Shortcomings of FRT

The deployment of FRT for public purposes, particularly by law enforcement authorities, has generated many concerns among society. Organisations, privacy authorities, academics and activists all over the world have called for a temporary moratorium on its use until its risks are properly assessed and addressed by robust regulation.[124]

Adding weight to these calls, private companies such as *IBM*, *Amazon* and *Microsoft* have suspended their development and distribution of FRT for law enforcement. These companies have expressed apprehension over the technology's potential for misuse and abuse, underscoring the need for comprehensive legislation before its wider adoption.[125]

The most common and pressing shortcomings appointed to FRT include accuracy, discrimination and bias, transparency and its potential for mass surveillance.

---

[118] Artificial Intelligence Act (n 16), recital 14
[119] ibid, recital 15
[120] European Data Protection Board (n 113), 9 and 10
[121] Artificial Intelligence Act (n 16), recital 16
[122] SWD(2021) 378 final
[123] Prüm II Regulation (n 7), recital 16
[124] Dallas Hill, Christopher D O'Connor and Andrea Slane, 'Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making' (2022) 24/3 Sage Journals 325, 326 <https://doi.org/10.1177/14613557221089558> accessed 13 November 2024.
[125] Rebecca Heilweil, 'Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress' *Vox* (11 June 2020) <https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police> accessed 13 November 2024.

3.1. Accuracy

In FRT, the degree of accuracy is fundamental for minimising the risk of false positives, where an image is falsely matched to another image on the watchlist, or false negatives, where images are deemed not to be matches but in fact are.[126] False positives can be particularly harmful to individuals, potentially subjecting them to unfair police scrutiny, criminal investigations, or discriminatory actions by authorities.[127]

The accuracy of FRT is heavily influenced by the quality of the data used during both the development and deployment of the technology. Images that meet specific quality standards, such as facial images, portraits or mug shots, [128] typically provide more reliable results than probe images, which inherently possess lower quality.[129] This distinction has to do with the environments in which these images are captured and its inherent factors such as lighting, angle, and distance. Images captured in controlled environments, namely police stations, usually have better quality than images captured in non-controlled environments, such as CCTV footage.[130] These differences must be considered when establishing the accuracy requirements.

Additionally, the databases' dimension and composition also play a significant role in system accuracy. Larger databases containing low-quality images are more prone to errors, particularly false matches. Additionally, the age of a stored image also impacts accuracy, as the likelihood of incorrect matches increases over time due to changes in an individual's appearance. [131]

To ensure maximum certainty, the accuracy standards for FRT must be regulated at the EU level, rather than being left to individual Member States.[132] This harmonisation is crucial for achieving transparency and equality in law enforcement applications.

However, the EDPS has pointed out that achieving complete accuracy in FRT is impossible. A flawless system would need to collect vast amounts of sensitive personal data, which is neither ethically nor practically feasible. As a result, FRT will always carry an inherent risk of bias and erroneous results, regardless of the volume or quality of data

[126] European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (Publications Office 2019), 9 <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 29 October 2024
[127] Vavoula (n 31), 32
[128] European Union Agency for Fundamental Rights (n 126), 10
[129] Vavoula (n 31), 32
[130] European Union Agency for Fundamental Rights (n 126), 8
[131] Vavoula (n 31), 33
[132] Dushi (n 91), 9

collected. [133]

Although ensuring image quality and minimising error rates are essential steps toward fairer use of FRT, they do not address all concerns. Even if FRT were perfectly accurate, other issues would persist.[134] The central concern lies in its potential to intensify existing inequalities and civil rights violations, as it raises profound questions about whether the technology aligns with the principles of democracy, freedom, privacy, equality, and social good. At its core, the debate over FRT involves balancing the protection of personal data with the demand for internal security.[135]

3.2. Discrimination and Bias

There is a common perception that computer-generated assessments are inherently accurate and unbiased; however, algorithmic bias is a well-documented issue, particularly within FRT.[136] One of the primary human rights concerns regarding FRT is its tendency toward error. According to the FRA, FRT has higher error rates when used on women and people of colour, resulting in potentially discriminatory outcomes. Discrimination, in this context, refers to treating a person less favourably than others in similar circumstances, based on personal characteristics.

While differential treatment may be permissible if it serves a legitimate aim and is necessary and proportionate, discrimination based on characteristics such as sex, race, colour, ethnicity, social origin, genetic traits, language, religion or belief, political opinions, national minority status, property, birth, disability, age, or sexual orientation is strictly prohibited by Article 21 of the Charter. [137]

FRA's research on people's experiences with police stops in Europe finds that, overall, the police stop men, young people, people belonging to ethnic minorities, Muslims and people who do not identify as heterosexual more often. People from an ethnic minority or immigrant background, in particular, experience more often stops that involve searches or requests for identification documents and are disproportionately

[133] Wojciech Wiewiórowski, 'Facial Recognition: A Solution in Search of a Problem?' (*European Data Protection Supervisor* 2019) <https://www.edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem> accessed 13 November 2024.
[134] European Union Agency for Fundamental Rights (n 126), 20
[135] Ella Jakubowska, 'Facial Recognition and Fundamental Rights 101' (*EDRi,* 4 December 2019) <https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/> accessed 4 November 2024.
[136] Door Luca Montag and others 'The Rise and Rise of Biometric Mass Surveillance in the EU' (EDRi, 7 July 2021), 39 <https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf> accessed 4 November 2024.
[137] European Union Agency for Fundamental Rights (n 126), 4 and 27

stopped while on foot.[138] In some countries, over 80% of ethnic minorities perceive recent police stops as ethnic profiling, and many report feeling disrespected by the police during such interactions.[139] Furthermore, young people from immigrant backgrounds are over-represented in the justice systems of EU Member States. [140]

The perception that minority communities, particularly racial, ethnic and religious groups, are primarily responsible for rising crime and public disorder has long existed in European societies, often rooted in stereotypical views of these communities' inherent characteristics. Despite clear evidence showing that these communities engage in these offences at rates similar to or lower than the majority population, they remain disproportionately subject to police stops. This disparity is often seen as a politically sanctioned response by law enforcement towards groups they inherently 'suspect' of criminal involvement. Discriminatory law enforcement practices are also closely associated with political demands of immigration control, cultural incompatibilities and enhanced crime control. [141]

The introduction of FRT could amplify these disparities, as FRT itself often exhibits inherent biases. A significant cause of discrimination lies in the datasets used to train FRT algorithms. For optimal accuracy, FRT requires a vast, varied, and high-quality image set that represents different demographic groups proportionately. However, European datasets are often biased towards images of white men, with lower representation of women and individuals from other ethnic backgrounds. This imbalance increases the likelihood of false positives for underrepresented groups, who are more prone to misidentification or unjustified stops.[142] Such outcomes reflect and reinforce societal biases, subjecting people of colour to over-policing, and the psychological effects

[138] European Union Agency for Fundamental Rights, 'Your Rights Matter: Police Stops - Fundamental Rights Survey' (Publications Office 2021), 7 and 14 <https://fra.europa.eu/en/publication/2021/fundamental-rights-survey-police-stops> accessed 23 October 2024

[139] European Union Agency for Fundamental Rights, 'Police Stops in Europe: Everyone Has a Right to Equal Treatment' (*FRA*, 25 May 2021) <https://fra.europa.eu/en/news/2021/police-stops-europe-everyone-has-right-equal-treatment> accessed 23 October 2024

[140] Patrick Williams and Eric Kind, 'Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe' (European Network Against Racism 2019), 12 <https://www.enar-eu.org/data-driven-policing-the-hardwiring-of-discriminatory-policing-practices-across-europe/> accessed 23 October 2024

[141] ibid, 9

[142] European Union Agency for Fundamental Rights (n 126), 27

of repeated misidentification.[143]

These discriminatory effects of FRT can also harm social cohesion. When ethnic groups experience frequent and inaccurate stops, their trust in law enforcement may deteriorate, eroding community relationships and fostering distrust of public institutions.[144]

The risk of racialised policing becoming embedded and standardised within law enforcement technologies is high, which may amplify the racialised criminalisation of minority communities and the potential for wrongful convictions, resulting in the over-representation of minority groups within prisons.[145] Even if algorithmic bias in FRT were completely resolved, concerns over structural discrimination would persist due to the ways in which these technologies are often deployed in practice, which can reflect existing biases in policing and surveillance practices.[146]

Although FRT and other technology-driven policing tools are often implemented to enhance efficiency, improve accuracy and reduce bias, automating decision-making can risk overlooking crucial contextual nuances surrounding individual cases. While these tools aim to eliminate problematic uses of human discretion, such as racial bias, they can also diminish positive discretion, such as the capacity for tolerance and empathy, which might otherwise allow officers to issue warnings rather than citations for minor infractions. Over-reliance on automated systems thus risks embedding existing bias and discriminatory practices, transforming them into systematic features of policing.[147]

3.3. Transparency

The above-mentioned concerns are often a consequence of the lack of transparency in the deployment and use of FRT.[148] While transparency is highlighted as a core ethical principle in many policy documents,[149] as well as in the GDPR and the AI Act, there is no specific guidance on the level of transparency required in FRT applications. Transparency enables public scrutiny and accountability of law enforcement's use of FRT, allowing data subjects to challenge outcomes, and ensuring

[143] Ella Jakubowska and Diego Naranjo, 'Ban Biometric Mass Surveillance!' (EDRi 2020), 13 <https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf /> accessed 29 October 2024
[144] European Union Agency for Fundamental Rights (n 126), 28
[145] Williams and Kind (n 140), 28
[146] Montag and others (n 136), 40
[147] Hill, O'Connor and Slane (n 124), 327
[148] ibid, 328
[149] Rita Matulionyte, 'Increasing Transparency around Facial Recognition Technologies in Law Enforcement: Towards a Model Framework' (2023) 33/1 Taylor & Francis, 3 <https://doi.org/10.1080/13600834.2023.2249781> accessed 13 November 2024

access to effective remedies.[150] However, transparency around FRT usage remains insufficient, with some law enforcement agencies denying its use until exposed by the media and others providing minimal information on FRT's purposes, locations, or safeguards.[151]

Five main issues contribute to this lack of transparency. Firstly, the absence of ethical guidelines with clear transparency standards is a major gap. Although the importance of transparency is generally acknowledged, there is no consensus among key organisations, such as Interpol, the Council of Europe and the EDPB, on how much transparency is necessary or how it should be implemented. [152]

Secondly, limited resources within law enforcement often deprioritise transparency initiatives. Developing, implementing and updating frameworks to support transparency in FRT applications require significant organisational and financial resources, which are typically limited. Consequently, law enforcement authorities usually employ these resources in the prevention and investigation of criminal offences, rather than in legitimising their activities and creating paths for their own accountability. This barrier can only be exceeded if policymakers deliberate on the allocation of additional resources to ensure transparency. [153]

Third, balancing transparency with operational secrecy is challenging, as law enforcement relies on confidentiality to ensure effective investigations. The line drawn between secrecy and transparency is, however, controversial: while openness can compromise public security and criminal investigation, secrecy is often broadly claimed to hide serious abuses of power. A balance between both principles must be struck on a case-by-case basis.[154] This tension is well-recognised in policy discussions, with documents like that from the Council of Europe noting that transparency obligations may be proportionately restricted when required to preserve law enforcement purposes, as outlined in Article 11 of Convention 108.[155]

---

[150] Rita Matulionyte, 'Transparency of Facial Recognition Technology and Trade Secrets' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (2023) Cambridge University Press 60, 61 <https://doi.org/10.1017/9781009321211.006> accessed 13 November 2024
[151] Matulionyte (n 149), 3
[152] ibid, 3, 7 and 8.
[153] ibid, 15
[154] ibid, 19
[155] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 'Guidelines on facial recognition' (Council of Europe 2021), 20 <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html#> accessed 17 November 2024

The technical complexity of FRT also complicates transparency. Systems based on “black box” deep learning algorithms produce outputs that are difficult to interpret, making transparency difficult to achieve. Although interpretability tools have been developed to explain the outputs of these systems, they often fall short in terms of accuracy, verifiability, and reliability. [156]

Lastly, legal factors, such as privacy laws and trade secrets, further restrict transparency. Privacy laws and trade secrets protect sensitive personal, technical and commercially valuable information, such as algorithms, source code, and training data, which limits the ability of external stakeholders to verify the accuracy and fairness of FRT. Although trade secret protections have some limits, they effectively prevent public access to critical information, further restricting transparency and accountability. [157]

3.4. Mass Surveillance

FRT is often referred to as a "silent technology" because it can be seamlessly implemented in existing systems, such as CCTV, without requiring the knowledge or consent of those being monitored. This becomes particularly problematic when FRT is used for identification in public spaces or when databases are populated with images from public sources, as it leaves individuals unable to avoid or opt out of surveillance.[158]

These features create an ideal environment for potential misuse, facilitating mass surveillance under the guise of public safety. Since this research focuses on examining whether the inclusion of facial images in Prüm II could shift the EU from an area of security to one of mass surveillance, this concern will be further developed in the following chapter.

4. Safeguards

Prüm II introduces numerous safeguards for exchanging facial images between EU Member States to mitigate the impact on individuals' fundamental rights when processing sensitive data. According to the Regulation, automated searches of facial images are permitted only for individual cases,[159] defined as single files linked to the prevention, detection, or investigation of criminal offences.[160] This restriction aims to ensure that searches are conducted with respect to the principles of due process and the rule of law. Although the search will be conducted for an individual case, if permitted by

[156] Matulionyte (n 149), 16
[157] ibid, 16-18.
[158] Hill, O’Connor and Slane (n 124), 328
[159] Prüm II Regulation (n 7), art 20
[160] ibid, art 4(10)

national law, these searches may extend to any individual linked to that file, such as persons without any criminal suspicion or conviction, including witnesses and family members of victims, whose facial images may nonetheless be included under Prüm II. [161]

Moreover, facial image searches must comply with the national law of the requesting Member State.[162] The Regulation does not impose any safeguards based on the law of the requested Member State, which could lead to situations where citizens' data are treated in ways that contravene their country's protections, if requested by a Member State with weaker safeguards. This situation is justified by the fact that the requesting Member State does not know which country holds the necessary information until conducting the search.[163] However, in the same provision, the Regulation allows the requesting State to confirm a facial image match, while the requested State has no equivalent option.[164] Consequently, the requested Member State cannot assess the necessity and proportionality of the search, nor the accuracy of the data before transferring the biometric profile, meaning that facial images cross borders without confirmation of a match with the search profile.[165]

The Regulation also provides that the confirmation of the match shall be manually conducted, in the requesting Member State, by "at least one qualified member of staff".[166] While this human intervention is intended to enhance the accuracy of results, the lack of a clear definition of what constitutes a "qualified member" provides limited assurance that the review will be conducted rigorously. It would be essential for the Regulation to specify the qualifications of this member, detailing technical expertise in biometric data analysis, and clarifying the member's position within law enforcement to ensure they hold sufficient authority and independence to carry out an impartial review. A detailed outline of the steps involved in this manual confirmation process would also improve transparency, supporting public trust in the process. Including these criteria within the Regulation would add a critical layer of rigour and accountability to biometric verification practices, without prejudice to the development of more technical aspects in the implementing acts.

[161] European Digital Rights (n 14), 22
[162] Prüm II Regulation (n 7), art 20(1)
[163] European Digital Rights (n 14), 19
[164] Prüm II Regulation (n 7), art 20(2)
[165] European Digital Rights (n 14), 20
[166] Prüm II Regulation (n 7), art 20(2)

Biometric matches are returned as a "list,"[167] which includes sensitive data profiles of non-matching individuals shared for comparison purposes. This procedure risks the unauthorised automated exchange of sensitive data.[168] Moreover, although the requesting State's national contact point has the discretion to confirm matches,[169] a confirmed match does not guarantee accuracy. Studies indicate that human reviewers often defer to algorithmic results, a phenomenon known as "automation bias," [170] or override them based on personal stereotypes,[171] further underscoring the need for strict oversight.

Discrimination, a primary concern with FRT, is addressed in the Regulation,[172] which asserts that data processing under Prüm II must not lead to discriminatory outcomes. However, this safeguard is not further developed, nor is it embedded in the Regulation's binding provisions, leaving it without concrete mechanisms for enforcement. Since this is a matter of fundamental rights that touches the EU's core principles, addressing it should not be deferred to implementing acts or merely acknowledged in the preamble of the Regulation. Such safeguards must be explicitly defined and rigorously enforced within the Regulation itself.

The Regulation also mandates that facial images meet "sufficient quality" standards for automated comparison.[173] The Commission is tasked with defining this standard, once more, in the implementing acts, due to its technical, detailed, and rapidly evolving nature.[174] This responsibility is crucial, as image quality significantly influences the accuracy of FRT systems and the reliability of their outcomes. Establishing stringent and precise quality criteria is essential to mitigating inaccuracies – a major shortcoming of FRT. Thus, the Commission's role cannot be overstated, it must account for technological advancements, ethical implications, and the broader impact on fundamental rights and freedoms. Ensuring image quality is not merely a technical matter but a vital safeguard to balance the effective use of FRT with respect for privacy and non-discrimination.

While Prüm II introduces safeguards for using FRT in cross-border law

[167] ibid, art 37(3), (4) and (5)
[168] European Digital Rights (n 14), 20 and 27
[169] Prüm II Regulation (n 7), art 20(2)
[170] Montag and others (n 136), 65
[171] European Union Agency for Fundamental Rights (n 126), 26
[172] Prüm II Regulation (n 7), recital 6
[173] ibid, art 22(2)
[174] ibid, recital 35

enforcement, these measures fall short of fully addressing the technology's risks to privacy, equality, and data protection. Key issues such as the lack of clarity on data accuracy standards, insufficient mechanisms to prevent discrimination, and vague requirements for manual reviews weaken the Regulation's ability to protect fundamental rights. Deferring critical protections to future implementing acts further limits their immediate enforceability, leaving significant gaps in safeguarding individuals against potential misuse of FRT. Strengthening these safeguards is essential to ensure fairness and compliance with fundamental rights.

5. Comparative Analysis of Facial Recognition Technology in China and the United States

FRT has seen extensive adoption globally, with China and the United States taking prominent but distinct approaches to its implementation. While China has normalised the use of FRT in everyday life and governance, the U.S. has seen rising opposition, leading to bans in several jurisdictions.[175] Analysing these countries' implementation and subsequent use of FRT is paramount to assess whether it is possible to circumvent FRT's shortcomings.

China stands as the leading adopter of FRT, integrating it into governance, security, and public life. In cities like Shenzhen, FRT is used to enforce traffic rules, identifying jaywalkers through surveillance cameras and publicly shaming them on large screens. Similarly, in Beijing, police use FRT-equipped smart glasses and body cameras to identify individuals in real time. Suzhou has extended FRT to monitor behaviour deemed "uncivilised," such as wearing pyjamas outdoors. FRT is also deployed for large-scale surveillance, particularly in Xinjiang, home to the Muslim Uyghur population, and to identify criminal suspects through psychological analysis. These technologies are supported by a vast CCTV infrastructure, making China home to 16 of the world's 20 most surveilled cities as of 2021.[176]

In the U.S., FRT adoption by law enforcement has risen sharply, with police using it for real-time identification and for accessing large facial databases. By 2016, half of the U.S. population's images were in law enforcement databases, highlighting the pervasive

[175] Peter Dauvergne, *Identified, Tracked, and Profiled: The Politics of Resisting Facial Recognition Technology* (Edward Elgar Publishing 2022)
[176] ibid, 2

reach of this technology.[177] However, opposition to FRT has grown, particularly over privacy concerns and its potential for surveillance, especially in communities with civil rights histories. In 2019, San Francisco became the first city to ban public FRT, a move followed by over 20 municipalities. Some cities, like Portland, Oregon, extended bans to private businesses. [178]

Portland's ban reflects broader fears about FRT's potential for bias and misuse, with concerns that it disproportionately infringes on civil liberties and exacerbates discrimination. [179]

Among the most controversial examples of FRT misuse in the U.S. is the case of Clearview AI. In 2020, it was revealed that the company had scraped over three billion facial images from the internet and social media platforms without user consent.[180] These images were incorporated into a facial recognition app[181] used by more than 600 law enforcement agencies,[182] including federal bodies such as the FBI and Homeland Security.[183]

Clearview AI's app enabled law enforcement to upload images from security footage and compare them to its extensive database, often linking to personal information online.[184] While this facilitated high-profile investigations, such as identifying suspects in the January 6 Capitol riots, it also raised severe privacy and ethical concerns.[185]

This controversy underscored broader issues with FRT in the U.S., where decisions about its acquisition and use remain largely self-governed, increasing risks of privacy violations and discrimination. [186]

Opposition to FRT is shaped by political and cultural contexts. The anti-FRT movement has more influence in liberal democracies, with strong civil societies, fundamental rights and legal protections than in developing economies and authoritarian

[177] Jennifer Lynch, 'Face Off: Law Enforcement Use of Face Recognition Technology' (Electronic Frontier Foundation 2019), 2 <https://www.eff.org/wp/law-enforcement-use-face-recognition> accessed 14 November 2024.
[178] Dauvergne (n 175), 8, 11 and 33
[179] ibid, 20
[180] Orsolya Reich, 'Clearview AI - The Privacy-Breaching App That Gives Us the Creeps' (*Liberties,* 14 February 2020) <https://www.liberties.eu/en/stories/clearview-privacy-busting-app/18206> accessed 14 November 2024.
[181] Andrew Tarantola, 'Why Clearview AI Is a Threat to Us All' (*engadget*, 12 February 2020) <https://www.engadget.com/2020-02-12-clearview-ai-police-surveillance-explained.html> accessed 14 November 2024.
[182] Reich (n 180)
[183] Dauvergne (n 175), 60
[184] Tarantola (n 181).
[185] Dauvergne (n 175), 64
[186] Hill, O'Connor and Slane (n 124), 325

States like China. In democratic East and Southeast Asian countries, where communal rights often take precedence over individual liberties, resistance remains weak. [187]

The use of FRT in China and the U.S. reveals the technology's potential for societal harm. In China, the extensive use of FRT for surveillance highlights its capacity to erode privacy and reinforce authoritarian control. In the U.S., while FRT has supported law enforcement, cases like Clearview AI demonstrate how unregulated implementation can lead to significant privacy breaches and systemic bias. The growing opposition in the U.S., resulting in municipal bans and heightened scrutiny, suggests an emerging recognition of these risks.

This raises the critical question: are the risks posed by FRT, particularly its potential to enable mass surveillance, an inevitable consequence of its adoption, or can they be effectively mitigated through regulation?

[187] Dauvergne (n 175), 13 and 20

IV. Mass Surveillance

In its impact assessment of the Regulation, the European Commission guarantees that Prüm II will not be used for live scanning purposes, nor to identify groups of people in public spaces. The use will be merely retrospective and related to a specific criminal investigation and, thus, no mass surveillance is involved. According to the Commission, remote biometric identification systems in publicly accessible spaces are not covered by the framework, nor any practice prohibited by the Artificial Intelligence Act (AI Act).[188]

Despite this guarantee provided by the European Commission, Prüm II does not explicitly prevent the use of FRT to identify people in public spaces. Although the Regulation only provides for the exchange of facial images of convicted criminals, suspects and, potentially, victims,[189] it leaves the regulation of law enforcement databases' content to the Member States – they decide which types of facial images they include in their databases, the sources of these data and the data subjects covered.[190]

Moreover, if the reasoning of Prüm II were to differ the regulation of this use to its implementing acts, it would anticipate such intention in the Regulation's text, as it did for the minimum quality standard.[191] Besides, the implementing acts cover technical and operational details, and this safeguard goes beyond that, so it would be crucial to incorporate it in the binding provisions of the Regulation.

As such, this chapter aims to problematise the possible consequences of Member States using FRT to identify people in public spaces for law enforcement purposes.

1. Remote Biometric Identification

A remote biometric identification system is an Artificial Intelligence (AI) system that identifies natural persons at a distance, without their active involvement, by comparing their biometric data with the biometric data contained in a reference database.[192]

These systems are "real-time" if they involve the use of live or near-live material (live video footage) and the capturing of biometric data, the comparison and the identification occur instantaneously, nearly instantaneously or in an event without a significant delay. In the case of "post" systems, biometric data has already been captured and the comparison and identification occur after a significant delay (image and video

[188] SWD(2021) 378 final
[189] Prüm II Regulation (n 7), art 19(1)
[190] European Data Protection Supervisor (n 13), 2
[191] Prüm II Regulation (n 7), art 22(2)
[192] Artificial Intelligence Act (n 16), recital 17

footage generated by CCTV cameras).[193]

Real-time systems used in publicly accessible places for law enforcement purposes are very intrusive to the rights and freedoms of the data subjects, as they may cause a feeling of constant surveillance. Additionally, these systems may be flawed with technical inaccuracies, leading to biased results and discrimination.[194] Due to all these factors, the use of real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is prohibited by the AI Act.[195]

This prohibition, however, includes several exceptions that allow the use of real-time remote biometric identification in specific scenarios. For instance, it may be employed to address imminent threats to life or physical safety. It can also be used to locate or identify perpetrators or suspects involved in serious crimes listed in the Regulation,[196] including terrorism, human and drug trafficking, sexual exploitation of children, and murder, [197] provided these offences are punishable by a maximum custodial sentence of at least four years under the Member State's law.[198]

Post-remote biometric identification systems, in turn, are considered intrusive by the provisions of the AI Act, according to which their use must be proportionate, legitimate, strictly necessary and subject to safeguards. These systems must be targeted regarding the individuals subject to identification, the location and temporal scope and their use must be based on a closed data set of legally acquired data.[199]

As such, unlike real-time systems, post-remote ones are not prohibited under the AI Act, nor is their use restricted to certain types of crimes. This technology may be employed in any offences and even minor crimes, as long as it complies with the requirements above.[200] Additionally, its application requires prior authorisation from either a judicial or an administrative authority.[201]

According to Svenja Hahn, a German Member of the European Parliament, (MEP) this permission regarding post-remote FRT constitutes "an attack on civil rights" that is only comparable to what "we otherwise only know from authoritarian States such

[193] ibid, recital 17.
[194] ibid, recital 32.
[195] ibid, recital 33.
[196] ibid, recital 33.
[197] ibid, annex II.
[198] ibid, recital 33.
[199] ibid, recital 95.
[200] ibid, recital 95.
[201] ibid, art 26(10).

as China." MEP Patrick Breyer also considered this policy option an instrument of "high-tech repression".[202]

In their joint opinion, the EDPB and EDPS emphasised that the intrusiveness of biometric processing is not solely determined by whether identification occurs in real-time or as post-remote analysis. For instance, using post-remote identification in the context of a political protest could have a substantial "chilling effect" on the exercise of fundamental rights and freedoms, such as freedom of assembly and association.[203]

In conclusion, both real-time and post-remote biometric identification systems may be used by Member States provided that the referred conditions are satisfied. While real-time systems are subject to stricter prohibitions and limited exceptions due to their high intrusiveness, post-remote systems face fewer restrictions. Therefore, facial images collected by these systems may be used under Prüm II as long as they are part of Member States' databases.

2. Mass Surveillance

Mass surveillance is broadly defined by the Council of Europe as any monitoring conducted in an untargeted manner, meaning without reasonable suspicion, consent, knowledge or opt-out options for those monitored, and directed at unspecified subjects. This practice operates irrespectively of any link between the monitored individuals and any crime or threat to public security.[204] According to this definition, both real-time and post-remote biometric identification systems could lead to mass surveillance, as no live FRT is required.

In the context of Prüm II, there is a concern that the untargeted application of facial recognition could enable mass surveillance by allowing indiscriminate processing of facial images.[205]

A person's facial image is one of the key attributes of their personality, revealing unique characteristics and distinguishing an individual from others.[206] A face is distinct from other biometric data because it is impossible to avoid being subject to face

[202] Gian Volpicelli, 'EU Set to Allow Draconian Use of Facial Recognition Tech, Say Lawmakers' *Politico* (16 January 2024) <https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns/> accessed 13 November 2024.
[203] Andrea Jelinek and Wojciech Rafał Wiewiórowski, 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (European Data Protection Board 2021), 11 <https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en> accessed 17 October 2024.
[204] Jakubowska and Naranjo (n 143), 10
[205] European Digital Rights (n 14), 26
[206] European Union Agency for Fundamental Rights (n 126), 23

surveillance when FRT is used in public spaces. A person's face can be easily surveilled and analysed without their knowledge.[207] As such, the targeted use of FRT, especially for surveillance purposes, raises critical concerns regarding several fundamental rights enshrined in the Charter.

Increasing surveillance networks allow permanent records of individuals' behaviours and characteristics, often without their consent or the possibility to opt-out. Ultimately, this excessive and coercive data collection can lead people to avoid public places or events.[208] This situation has the potential to provoke a "chilling effect," deterring individuals from exercising freedoms of thought, conscience, religion,[209] expression,[210] and assembly and association[211]. [212] They may feel inhibited from participating in public gatherings or expressing dissenting views out of fear of negative consequences.

This processing of facial images, revealing identifying features of a person's identity, represents a direct infringement of the rights to privacy and to the protection of personal data. These rights, although distinct, are closely related as they aim at preserving individual autonomy and dignity. Together, they provide a personal sphere in which individuals can develop their personalities without unwarranted surveillance, fostering the exercise of other freedoms. The right to privacy does not cover only private spaces but also one's reasonable expectation of privacy in public settings. This means that individuals should not be subjected to arbitrary surveillance or monitoring in public spaces.[213]

When used for law enforcement, large-scale facial recognition disproportionately impacts over-policed communities, including migrants, racial minorities, and people living in poverty. This is exacerbated by the fact that data used to train this technology reflects the biases and discrimination present in its source societies, leading to inaccuracies in recognising people of colour, particularly women.[214] These biases constitute a clear violation of the fundamental rights to equality[215] and non-discrimination,[216] making it difficult for law enforcement authorities to justify the

[207] Jakubowska (n 135)
[208] Jakubowska and Naranjo (n 143), 15 and 22
[209] Charter of Fundamental Rights of the European Union (n 9), art 10
[210] ibid, art 11
[211] ibid, art 12
[212] European Union Agency for Fundamental Rights (n 126), 23 and 30
[213] ibid, 23
[214] Jakubowska and Naranjo (n 143), 10 and 13
[215] Charter of Fundamental Rights of the European Union (n 9), art 20.
[216] ibid, art 21

necessity of the application of these technologies. [217]

Increased accuracy of this technology might address some of its negative consequences, but it does not eliminate the inherent risks to privacy and security.[218]

When people are being surveilled in public places, they are not aware that their personal data is being processed. Awareness and transparency are preconditions for the exercise of the right to an effective remedy and to a fair trial,[219] the right of access, correction and deletion of personal data[220] and the right to good administration.[221] They are also fundamental for data subjects to lodge an administrative complaint before a supervisory authority, a right provided by the LED.[222] Although these rights may be restricted to ensure confidentiality and secrecy crucial to the authorities' work, the affected individuals must be notified of the processing as soon as such notification is no longer capable of jeopardising the investigation.[223]

Other fundamental rights such as the presumption of innocence and right of defence[224] and the right to equality before the law[225] are also affected by this perceived power imbalance created between people and the State where "the powerful watch and the powerless are watched".[226] Despite EU law upholding the principle of innocence until proven guilty, widespread biometric mass surveillance effectively treats citizens as suspicious until proven innocent.[227]

Moreover, the LED underscores the importance of treating convicted criminals and suspects differently from individuals who are neither convicted nor suspected of crimes.[228] As such, whilst it may be legitimate and lawful for facial recognition to target a suspect, it is not to target the general public indiscriminately. The LED mandates enhanced protection for processing facial images for the purpose of uniquely identifying a natural person,[229] as it could reveal sensitive personal attributes, such as race, gender,

[217] Jakubowska and Naranjo (n 143), 28
[218] ibid, 10
[219] Charter of Fundamental Rights of the European Union (n 9), art 47.
[220] ibid, art 8(2)
[221] ibid, art 41
[222] Directive (EU) 2016/680 (n 15), art 52
[223] European Union Agency for Fundamental Rights (n 126), 31 and 32
[224] Charter of Fundamental Rights of the European Union (n 9), art 48
[225] ibid, art 20
[226] Jakubowska and Naranjo (n 143), 13
[227] Ella Jakubowska, 'New EDRi Report Reveals Depths of Biometric Mass Surveillance in Germany, the Netherlands and Poland' (*EDRi*, 7 July 2021) <https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/> accessed 5 November 2024.
[228] Directive (EU) 2016/680 (n 15), art 6
[229] ibid, art 10

or religion. [230]

Mass surveillance infringes fundamental rights regardless of whether it relies on machine learning or human oversight.[231] Though Prüm II does not specify whether facial recognition involved in the comparison of facial images uses AI, the technology's capacity to infringe on these rights is clear.

Therefore, untargeted processing of biometric data in publicly accessible spaces cannot be deemed necessary or proportionate under the Charter, the ECHR, or the LED to ensure public security or combat crime. [232] Mass surveillance of people's activities through indiscriminate collection and processing of biometric data infringes the essence of the above-mentioned fundamental rights, as it occurs irrespective of any link between the majority of surveilled people and any crime or threat to public order. [233] Besides, the significant risks to sensitive personal data, alongside the restrictions on fundamental rights and freedoms, mean that this approach is never the least intrusive option.[234]

Many studies have shown that – despite claims by law enforcement and private companies – there is no link between surveillance and crime prevention. Even when studies have concluded that "at best" CCTV may help deter petty crime in parking garages, this has only been with exceptionally narrow, well-controlled use, and without the need for facial recognition.[235]

3. Biometric Surveillance in EU Member States

Many EU Member States have been utilising FRT for many years, particularly in law enforcement, with its deployment in mass surveillance systems now expanding considerably.[236]

In Germany, biometric mass surveillance has become increasingly prevalent. FRT is frequently applied to previously collected footage, and CCTV cameras equipped with in-built biometric analysis are increasingly deployed. These cameras, sold to state police forces, are installed in public spaces across German cities. Video surveillance and subsequent biometric processing, conducted either in real-time or retrospectively, amount

[230] Jakubowska and Naranjo (n 143), 12
[231] ibid, 18
[232] ibid, 19
[233] ibid, 21
[234] ibid, 19
[235] Ella Jakubowska, 'The Many Faces of Facial Recognition in the EU' (*EDRi*, 18 December 2019) <https://edri.org/our-work/the-many-faces-of-facial-recognition-in-the-eu/> accessed 13 November 2024
[236] Ante Novokmet, Zvonimir Tomičić and Ivan Vidaković, 'Facial recognition technology in EU criminal justice - human rights implications and challenges' (2023) 7 EU and Comparative Law Issues and Challenges Series (ECLIC) 525, 541 <https://doi.org/10.25234/eclic/27461> accessed 4 November 2024

to biometric mass surveillance.[237]

For instance, in Cologne, police installed live facial recognition cameras in low-crime areas, impacting individuals and businesses conducting lawful activities, as well as LGBTQIA+ venues and places of worship. Thousands were subjected to surveillance while less than 0.1% of the footage deemed probative. This raises concerns about proportionality, as broad surveillance measures affect all passers-by indiscriminately. Furthermore, this biometric surveillance has continued in areas with stable or decreasing crime rates, undermining the necessity for such intrusive practices.[238]

In Hamburg, during the G20 Summit protests in 2017, German police collected facial images of over 100.000 people storing this data indefinitely on departmental hard drives. These images were then cross-referenced against a database of convicted criminals and suspects using FRT.[239] Despite this extensive data collection, only three individuals were ultimately identified.[240]

In the Netherlands, another EU Member State dedicated to safeguarding individual rights, FRT is also widely used. Since 2016, Dutch police have used a facial recognition system called CATCH to identify suspects and convicted individuals by comparing footage with a database containing millions of images.[241] The Dutch police have also encouraged individuals and businesses to share footage from security cameras and smart doorbells for investigative purposes if a crime occurs nearby. Non-compliance with police's requirement to submit footage can result in criminal charges or jail time. Despite these extensive measures, the technology's effectiveness in crime reduction is unproven.[242]

Additionally, Dutch authorities retain biometric data of millions of foreign nationals in a "Foreign National Database," treating them as inherently suspicious due to nationality. Concerns are heightened by documented racial and ethnic profiling practices within the Dutch police. Certain municipalities are also using FRT at large events for crowd control and crime prevention.[243]

---

[237] Montag and others (n 136), 16
[238] ibid, 20 and 21
[239] 'Hamburg G20 Summit protests facial analysis database legality' (*AIAAIC*, February 2023) <https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/hamburg-g20-protests-facial-recognition-surveillance> accessed 13 November 2024
[240] Matthias Monroy, 'G20 in Hamburg: Data Protection Commissioner Considers Face Recognition Illegal' (*digit.site36.net*, 15 August 2018) <https://digit.site36.net/2018/08/15/g20-in-hamburg-data-protection-commissioner-considers-face-recognition-illegal/> accessed 13 November 2024
[241] Novokmet, Tomičić and Vidaković (n 236), 545
[242] Montag and others (n 136), 60, 72 and 75
[243] ibid, p 67, 56 and 77

In Italy, the city of Como has introduced video surveillance systems in public areas that enable real-time image display and facial recognition, managed by the local police. These measures, framed as security enhancements, have emerged alongside anti-begging and anti-migration ordinances. However, the Como Police Headquarters has described the city as "one of the safest in the country", raising questions about the necessity and justification of these systems. As such, basis for the deployment of this system, the perimeter of usage and concerns regarding privacy and personal data protection remain inadequately addressed. Consequently, the Guarantor for the protection of personal data has deemed this processing to be unlawful.[244]

In Greece, the police are using smart devices with FRT during patrols and identity checks to photograph individuals up close and match their images with central databases. This approach aims to streamline the identification of individuals, particularly third-country nationals residing in Greece. Given the Hellenic Police's regular practice of mass identity checks targeting individuals suspected of irregular migration, the deployment of such technology is likely to disproportionately affect migrant communities.[245]

Post-remote biometric identification systems, while not prohibited under the AI Act, present significant risks to fundamental rights. These systems, whose employment is not restricted to specific types of crimes, are highly susceptible to enabling mass surveillance. The dangers of this form of surveillance extend beyond privacy violations: they threaten individual autonomy and dignity, amplify systemic biases and discrimination, and create a chilling effect on the exercise of fundamental freedoms.

The deployment of FRT in several EU Member States underscores the inevitability of mass surveillance when these technologies are used without adequate safeguards. Cases across Germany, the Netherlands, Italy, and Greece illustrate the disproportionate impact on over-policed communities, the ineffectiveness of identifying significant numbers of criminals or suspects, and the invasive monitoring of individuals unconnected to any criminal activity. This raises serious concerns about the proportionality and necessity of FRT in the context of law enforcement.

Given the profound implications for privacy, equality, and democratic freedoms,

[244] Laura Carrer, Riccardo Coluccini, Philip Di Salvo, 'Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale' *Wired* (9 June 2020) <https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/> accessed 5 November 2024.

[245] Eleftherios Chelioudakis, 'Greece: Technology-Led Policing Awakens' (*about:intel*, 29 June 2020) <https://aboutintel.eu/greece-policing-border-surveillance/> accessed 5 November 2024

the inclusion of FRT within Prüm II necessitates careful proportionality assessment. Without robust safeguards, the Regulation risks entrenching mass surveillance across the EU, undermining the fundamental rights and principles enshrined in its legal framework.

V. Differing National Legislations

Under Prüm II, automated facial image searches by Member State authorities are limited to databases established for criminal prevention, detection, and investigation.[246] While the Regulation emphasises compliance with national laws and the LED in the creation of such databases,[247] it delegates their regulation to individual Member States.[248]

Notably, although Prüm II requires Member States to ensure the availability of facial image reference data for suspects, convicted persons, and, where permitted, victims,[249] it does not explicitly confine database access to these categories. Instead, these groups seem to present a minimum threshold, leaving room for broader inclusion if permitted under national laws.

Moreover, Prüm II determines that automated searches are permitted only for criminal offences punishable by a maximum term of imprisonment of at least one year under the laws of the requesting Member State.[250] However, variations in national penalties for similar offences complicate the establishment of consistent criteria for determining the seriousness of an offence.

To address these issues, a thorough comparison of legal systems is essential to understand how the Regulation is applied across Member States. This chapter begins by examining the national facial image databases of various EU Member States and their use of facial recognition for law enforcement purposes. It then evaluates which crimes in different jurisdictions are punishable by a maximum term of at least one year to determine whether they qualify as serious crimes. Finally, the chapter concludes by assessing whether significant differences exist among Member States based on these comparisons.

1. Differing National Approaches to Facial Recognition in Law Enforcement

The inclusion of facial images within Prüm II underscores the need for a thorough understanding of national facial image databases across Member States and the varying applications of facial recognition by law enforcement. There is no specific EU legal framework governing the use of facial recognition for processing facial images under the scope of the LED.[251] This regulatory gap highlights the importance of examining how

[246] Prüm II Regulation (n 7), art 19(1)
[247] ibid, recital 37.
[248] ibid, recital 16.
[249] ibid, art 19(1).
[250] ibid, art 20(1).
[251] TELEFI project, 'Towards the European Level Exchange of Facial Images Legal Analysis for TELEFI project' (February 2020), 22 <https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf> accessed 18 November 2024.

Member States have approached the collection, storage, and employment of facial images in criminal investigations.

To facilitate a meaningful comparison of national approaches, this subchapter analyses the reports issued by the TELEFI project, an EU-funded initiative designed to assess the use of FRT in crime investigations across Member States.[252]

According to the report on the project, as of 2020, Latvia was the only Member State with explicit legislation on the collection and use of facial images in criminal proceedings. In contrast, other Member States regulate these practices indirectly through broader legal instruments, such as Criminal Codes or Personal Data Protection Acts. Although these frameworks address the issue of facial images in the context of criminal proceedings, no Member State has enacted laws exclusively focusing on the collection, processing, or use of facial images specifically for law enforcement purposes.[253]

The deployment of facial recognition for criminal investigations varies significantly across the EU. Some Member States have not yet considered adopting the technology, while others are in the early stages of implementation or have well-established systems in place. As of December 2020, facial recognition had been implemented in eleven EU Member States, namely Austria, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands and Slovenia. Meanwhile, countries like Croatia, Czech Republic, Romania, Spain, Sweden, Cyprus and Estonia were expected to implement FRT between 2021 and 2022. Although Portugal is within the nine EU Member States with no firm decision on implementing FRT, the planning process for introducing the technology has begun.[254]

In the Member States where FRT has been adopted, its primary use for criminal investigations is retrospective. After a crime, investigators typically extract a facial image of a person of interest from surveillance camera footage. This image, classified as an "uncontrolled image", is then searched using facial recognition tools against a facial image database containing images of individuals with known identities, known as "controlled images". The system performs one-to-many identification, generating a list of the most likely matches, which a human operator subsequently reviews. The operator evaluates the similarities between the searched image (probe) and the candidate images

[252] https://www.telefi-project.eu/
[253] TELEFI project (n 251), 12 and 23.
[254] TELEFI project, 'Summary Report of the Project "Towards the European Level Exchange of Facial Images"' (January 2021), 10 <https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf> accessed 18 November 2024.

to determine the outcome of the search. [255]

This chapter will compare the EU Member States that had implemented facial recognition in their databases in 2020, due to the availability of detailed data. It will assess various aspects of their facial recognition systems, including the databases used, categories of data subjects covered, image quality standards, personnel training and oversight, the legal scope of search results, the use and storage of uncontrolled images, and match criteria.

1.1. Databases Used for Facial Recognition Searches

Facial recognition searches across EU Member States primarily rely on databases designed to store and process facial images collected during criminal investigations.[256] These databases generally include images of suspects, convicts, and victims. However, there are significant variations in the types of databases used and the sources of the data they contain, reflecting different national legal frameworks and practices.

Some Member States extend their facial recognition searches beyond criminal databases to include civil databases. For example, facial recognition searches in Finland and the Netherlands also cover civil databases containing data on asylum seekers, foreigners, and visa applicants.[257] Austria, while permitting searches in a civil database of foreigners under national law, had not connected this database to the facial recognition system as of 2020.[258] Conversely, Hungary does not maintain a dedicated criminal database for facial recognition searches and instead relies exclusively on a civil database for document applicants.[259]

Other Member States, such as Germany, France, Italy, Slovenia, and Lithuania restrict searches to criminal databases. However, these databases include images of individuals whose data is not collected explicitly for criminal investigations, such as missing persons, unidentified deceased individuals, immigrants, asylum seekers, [260] and, in Italy's case, foreigners, who account for 90% of the database. Although these databases are criminal in nature, the presence of facial images of individuals who are not directly included for the purpose of solving crimes complicates the distinction between civil and

[255] ibid, 24
[256] ibid, 31
[257] ibid, Appendix 3
[258] ibid, 39
[259] ibid Appendix 3
[260] ibid Appendix 3

criminal data usage.[261]

This issue is a main concern highlighted by the EDPS in its Opinion on the Proposal for the Prüm II Regulation. The EDPS underscores the importance of adhering to Article 6 of the LED, which requires a clear distinction between different categories of data subjects, such as convicted criminals, suspects, victims, and witnesses. The EDPS stresses that Prüm II should restrict searches to the facial images of convicted criminals and suspects, as these categories of individuals are more likely to be involved in serious crimes for which facial recognition searches are guaranteed. The inclusion of facial images from other categories of individuals whose data is typically collected for more limited and specific purposes, would require detailed justification.[262]

Consequently, Member States such as Germany, France, Italy, Slovenia, Finland, Austria, the Netherlands, Lithuania, Latvia, and Hungary, which extend their searches to include facial images of individuals beyond convicted criminals and suspects, diverge from the EDPS recommendations and interpretation of the LED. This practice raises significant concerns about proportionality, highlighting the need for stricter alignment with data protection standards.

The overlap between criminal and non-criminal data raises significant concerns from a data protection perspective. Specifically, this practice may violate key principles outlined in EU law, such as purpose limitation[263] and data minimisation.[264]

1.2. Image Quality Standards

The reliability of facial recognition systems depends heavily on the quality of the images stored and processed. Despite the critical role of image quality, standards and compliance mechanisms vary significantly across Member States.

Austria leads with a structured approach, combining centralised quality checks of photographs, a best practice manual, and personnel training on the collection of facial images to maintain consistency.[265] Similarly, Germany enforces rigorous controls, requiring compliance with technical and quality standards during image registration, supported by extensive training for personnel responsible for image collection.[266] Latvia implemented a built-in quality assessment tool that automatically rejects images of

[261] ibid, 32
[262] European Data Protection Supervisor (n 13), 9 and 10
[263] Directive (EU) 2016/680 (n 15), art 4(1)(b)
[264] ibid, art 4(1)(c)
[265] TELEFI project (n 254), 42
[266] ibid, 76

insufficient quality, ensuring that only high-quality images are searchable within its system.[267]

In France and Greece, written guidelines outline requirements for image capture, including specifications for pose, lighting, and background conditions.[268] The Netherlands takes a different approach, integrating basic training for police officers collecting biometric data, as well as software tools to assess crime scene image quality and ensure compliance with facial recognition requirements.[269] Hungary adopts a regulatory approach, enforcing quality standards through legal frameworks and providing personnel with training on image capture techniques.[270]

Conversely, some countries adopt less formalised methods. Lithuania relies on non-binding recommendations, and poor-quality images, while stored, cannot be processed by the facial recognition module.[271] Italy imposes basic requirements for mugshots but lacks explicit standards for probe image quality, leaving low-quality images subject to system rejection.[272] Slovenia imposes minimum quality criteria for probe images but does not provide specialised personnel training.[273] Finland allows adjustments to probe images either before or after uploading but does not enforce specific quality restrictions.[274]

The European Parliament's LIBE committee has underscored the importance of high-quality images to ensure the accuracy of facial recognition systems. It has pointed out that substandard data quality increases the risk of false matches, highlighting the need for Member States to prioritise high standards for image capture and processing.[275]

As such, considering the role of facial recognition in cross-border law enforcement, as seen with the inclusion of these systems under Prüm II, there is a clear need for harmonisation of these quality standards. Achieving uniformity in image quality across Member States is essential to ensuring that facial recognition systems provide accurate outcomes.

[267] ibid, 92
[268] ibid, 72 and 80
[269] ibid, 109
[270] ibid, p 84
[271] ibid, 100
[272] ibid, 89
[273] ibid, 123 and 124
[274] ibid, 67
[275] Vavoula (n 31), 32

1.3. Training and Oversight

Training and oversight play a pivotal role in ensuring the effective use of facial recognition systems. Across the EU, Member States demonstrate diverse approaches to personnel training and operation monitoring.

While in Germany, Greece, Slovenia, Austria, the Netherlands and Hungary facial recognition searches are restricted to a limited number of specialists, Member States such as France, Italy, Finland, Latvia and Lithuania permit a broader range of police officers to carry out these searches. [276]

Germany sets a notable standard with an 11-week training programme for facial image examiners, covering facial recognition techniques and image comparison methods.[277] Austria requires qualified specialists to perform searches,[278] while Hungary provides practical training on database software and facial recognition systems.[279] The Netherlands also emphasises expertise, requiring searches to be conducted by facial experts.[280]

In contrast, Latvia adopts a more flexible approach, offering training as needed to ensure that personnel conducting searches have the necessary skills.[281] France and Italy provide basic training but lack systematic oversight or proficiency monitoring.[282] Finland requires officers to obtain authorisation to conduct searches, with additional permissions needed for accessing civil databases.[283] Lithuania and Slovenia offer minimal training provisions for personnel. While Lithuania initially trained a small group when facial recognition was introduced, searches can now be performed by any registered officer without further instruction.[284] Slovenia, in contrast, offers in-house training through a mentoring system.[285]

The diversity of training approaches underscores the disparities in how Member States prepare personnel for facial recognition tasks. Some countries ensure comprehensive training and oversight, while others take a more flexible or minimal approach. This range highlights the importance of establishing uniform standards for

[276] TELEFI project (n 254), 30 and 31
[277] ibid, 77
[278] ibid, 39
[279] ibid, 84
[280] ibid, 108
[281] ibid, 101
[282] ibid, 72 and 90
[283] ibid, 67
[284] ibid, 30 and 31
[285] ibid, 124

training and oversight, especially as Prüm II seeks to extend cross-border cooperation in facial recognition searches.

1.4. Legal Scope of Search Results

The admissibility of facial recognition search results in judicial proceedings varies widely across Member States. In most countries, results are strictly limited to investigative purposes and are not admissible as evidence in court.

Austria, Finland, France, Hungary, Lithuania, and Slovenia adhere to this approach, using search results solely as investigative leads rather than admissible evidence in court. Latvia follows a similar framework, restricting results to intelligence and operative purposes, explicitly barring their use as standalone evidence.[286]

In some Member States, facial recognition results can be used judicially under specific conditions. In Italy, while facial recognition results generally cannot be used directly in court, a 1:1 facial image verification performed by a forensic expert can validate the results, making them admissible. Similarly, in Germany and Greece, results are primarily used for investigative purposes but can be admitted as evidence if deemed necessary. In the Netherlands, although results are investigative leads, their inclusion in court proceedings can be determined by the public prosecutor.[287]

1.5. Use and Storage of Uncontrolled Images

Member States have adopted different approaches regarding the integration of uncontrolled images into facial recognition databases. Uncontrolled images, as defined in the TELEFI study, are those not captured according to specific facial recognition standards or guidelines, such as CCTV footage or crime scene photographs.[288]

In some Member States, uncontrolled images are directly stored in criminal facial recognition databases. For example, Germany allows the storage of uncontrolled images, when no other alternatives are available. Similarly, France and Slovenia incorporate uncontrolled images, including surveillance footage and photo-robot sketches into their criminal databases. Austria also includes crime scene images within its criminal database.[289]

Lithuania stores uncontrolled images in a separate crime scene register called

[286] ibid, Appendix 5
[287] ibid.
[288] ibid, 8
[289] ibid, Appendix 7

Iniciativa rather than incorporating them into criminal facial recognition databases.[290] On the other hand, both Greece and Hungary allow uncontrolled images to be searched against existing criminal databases without storing them permanently.[291]

Countries like Italy, Finland, and Latvia adopt a more restrictive approach, excluding uncontrolled images entirely from their facial recognition databases.[292] This ensures that only controlled, quality-assured images are processed, mitigating the risks associated with low-quality or non-compliant data. The Netherlands, as of 2020, did not store uncontrolled images in its databases but planned to do so in the future. While these images are not yet stored, they can already be searched against the database.[293]

These variations highlight the differing levels of regulation and data handling within Member States, with some prioritising broader data inclusion and others focusing on restricting the types of images used to maintain higher data quality standards.

1.6. Match Criteria in Facial Recognition Searches

The evaluation of candidate lists in facial recognition systems involves assessing the likelihood that a probe image corresponds to an individual within the database. This process varies in structure and methodology across Member States, with some relying heavily on investigator discretion and others employing more standardised frameworks. The number of candidates in the list differs among Member States, varying from 10 to 1,000, with the reported match rate for searches varying from 1% to 8.2%.[294]

In France, Hungary, Italy and Greece, there are no standardised criteria for determining a match. The decision is left to investigators or examiners, relying heavily on human discretion.[295]

Other countries have adopted more structured approaches to evaluation. Austria provides investigators with additional details for each candidate, including a match percentage and a reference number linking to the database for further inquiry.[296] The Netherlands does not provide for a match threshold, instead, it implements a rigorous double-verification process. Here, facial comparison experts review potential matches, and their findings are confirmed by additional experts, reducing the likelihood of errors

[290] ibid, Appendix 7
[291] ibid, 80 and 82
[292] ibid, 66, 89 and 92
[293] ibid, 108
[294] ibid, 31
[295] ibid, 72, 84, 90 and 80
[296] ibid, 42

and enhancing accountability.[297] Slovenia follows a similar model, where the individual conducting the search assesses the candidate list and determines whether a match is present.[298] In Lithuania, match scores are used to rank candidates based on the likelihood of a match.[299]

1.7. Main Findings

The analysis of the topics discussed above reveals significant differences in Member States' approaches to facial recognition in law enforcement. It underscores how the absence of a unified EU framework leads to diverse approaches in database content, image quality standards, personnel training, and oversight. Moreover, the analysis reveals low match rates for searches, with the best-case scenario reaching only 8.2% and the worst 1%. It is important to note that this comparison is limited to eleven Member States, and as more countries adopt facial recognition systems, these disparities are likely to increase.

Since the criteria for conducting searches under Prüm II are based on compliance with the national law of the requesting State, a search deemed lawful under one Member State's legal framework might still conflict with the legal standards or fundamental rights protections of the requested State.

The extension of facial recognition searches beyond their intended use in criminal investigations, particularly when involving the inclusion of data from non-criminal categories infringes with the purpose limitation principle. Similarly, the data minimisation principle is compromised in Member States that store and process large volumes of data that are not directly relevant to the investigation. Transparency and accountability may also be violated in systems where there is insufficient oversight, personnel training, lack of standardised match criteria and inconsistent handling of search results.

This analysis underscores the potential for legal uncertainty and highlights the need for harmonised frameworks or safeguards that respect the diverse legal traditions and privacy expectations across Member States while enabling effective cross-border collaboration.

[297] ibid, 108
[298] ibid, 123
[299] ibid, 100

2. Comparative Analysis of Criminal Penalties across the EU

2.1. Serious Criminal offences

Assessing which crimes, across the EU, are punished by a maximum term of imprisonment of at least one year is an essential component of determining the proportionality of Prüm II, specifically regarding the search and exchange of facial images. Effectively, the seriousness of the crimes involved may or may not justify such a measure.

In the same Opinion, the EDPS underscored that automated searches of facial images should be possible only in the context of individual investigations of serious crimes. It recalls case law of the CJEU, according to which serious interferences with fundamental rights can only be justified when related to a serious crime.[300]

Article 83(1) of the TFEU identifies areas of crime considered particularly serious and having a cross-border dimension. These include terrorism, human trafficking, sexual exploitation of women and children, illicit drug and arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime. Based on these categories, the TFEU delegates to the European Parliament and the Council the task of defining "serious criminal offences".[301]

Building on this framework, Regulation (EU) 2019/818 provides a specific definition of a “serious criminal offence.”[302] It refers to acts that correspond to or are equivalent to those listed in Article 2(2) of the Council Framework Decision 2002/584/JHA.[303] In addition to the offences included in the TFEU, this article includes but is not limited to, fraud, environmental crime, murder, kidnapping, racism and xenophobia, organised or armed robbery, and facilitation of unauthorised entry and residence.[304] To qualify as serious under Regulation (EU) 2019/818, these offences must be punishable by national law with a custodial sentence or detention order of at least three years.[305]

Moreover, the AI Act also provides a list of criminal offences based on those listed

[300] European Data Protection Supervisor (n 13), 8 and 10
[301] Treaty on the Functioning of the European Union (n 60), art 83(1)
[302] Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L 135/85, art 4 (22)
[303] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision [2002] OJ L 190/1
[304] ibid, art 2(2)
[305] Regulation (EU) 2019/818 (n 302), art 4 (22)

in the Council Framework Decision 2002/584/JHA. According to the Regulation, such offences are qualified as serious, where they are punishable by a custodial sentence or a detention order for a maximum period of at least four years as defined by that Member State's law.[306]

Thus, regarding the maximum term of imprisonment, the threshold for defining serious crimes under EU legislation is higher than that established by Prüm II. While Prüm II allows the exchange of data, including facial images, for crimes punishable by a maximum term of at least one year, the EU's broader legislative framework requires that offences provided in Article 2(2) are punished by a minimum threshold of three years of imprisonment to qualify as serious. This discrepancy means that certain crimes meeting the Prüm II criteria may fall short of the seriousness standard outlined in other EU instruments, such as Regulation (EU) 2019/818, Council Framework Decision 2002/584/JHA and the AI Act.

To address this inconsistency, a detailed comparison of the criminal legislations of Member States is essential. This analysis will examine penalties for multiple offences to determine whether the broader application of Prüm II remains proportionate and justified under the EU's standards for serious crimes.

2.2. Member States Criminal Penalties

For a criminal offence to be classified as "serious" under EU law, it must satisfy two cumulative requirements: it must fall within the categories listed in Article 2(2) of Council Framework Decision 2002/584/JHA, and it must be punishable by a minimum penalty of three years of imprisonment. This section compares criminal penalties across six EU Member States – Portugal, France, the Netherlands, Sweden, Poland, and Germany – to identify crimes punishable by maximum terms of one, two, and three years. The analysis highlights disparities between crimes considered serious under EU law and those encompassed by Prüm II. The selection of countries, varying in size, geography, and legal traditions, provides a representative framework for evaluating criminal justice systems across the EU.[307] Not all the legislation examined below has up-to-date official English translations, therefore unofficial translations available online or manual translations have been used.

[306] Artificial Intelligence Act (n 16), recital 33

[307] Jörg-Martin Jehle, Marianne Wade and Beatrix Elsner, 'Prosecution and Diversion within Criminal Justice Systems in Europe. Aims and Design of a Comparative Study' (2008) 14 Eur J Crim Policy Res 93, 98 <https://doi.org/10.1007/s10610-008-9074-7> accessed 25 November 2024.

Starting with Portugal, its inclusion in the analysis reflects the familiarity and proximity of its legal system, which provides a basis for comparison with other Member States. According to the Portuguese Criminal Code,[308] crimes punishable by a maximum term of imprisonment of one year include the violation of correspondence or telecommunications,[309] breach of secrecy[310] and issuing false certificates.[311] In contrast, offences such as simple assault,[312] theft,[313] and abuse of trust[314] carry a maximum penalty of three years.

France, with its rich legal heritage and the oldest prosecution service in Europe, exemplifies the Romanic legal tradition. Its system is characterised by a clear separation between prosecution and judicial functions, including the presence of examining magistrates.[315] Under the French Criminal Code,[316] offences punishable by a maximum term of one year include disrespect towards judicial authorities,[317] contracting a second marriage before dissolving the first,[318] and intruding into a school establishment to disturb order.[319] Meanwhile, crimes such as unauthorised entry into someone's home through threats or coercion,[320] misappropriation of collateral,[321] and participation in a combat group,[322] carry maximum penalties of three years.

The Netherlands offers an example of a smaller Western European country with a strong focus on informal case resolution, often bypassing formal court proceedings.[323] Dutch law[324] provides that crimes punishable by a maximum term of one year include unlawful entry or residence in a terminated dwelling,[325] failure to disclose bankruptcy information,[326] and misleading an insurer regarding relevant circumstances.[327] More

[308] Decreto-Lei n.º 48/95, de 15 de março (Código Penal).
[309] ibid, art 194
[310] ibid, art 195
[311] ibid, art 260
[312] ibid, art 143
[313] ibid, art 203
[314] ibid, art 205
[315] Jehle, Wade and Elsner (n 307), 98
[316] Code Pénal
[317] ibid, art 434-24
[318] ibid, art 433-20
[319] ibid, art 433-22
[320] ibid, art 226-4
[321] ibid, art 314-6
[322] ibid, art 431-14
[323] Jehle, Wade and Elsner (n 307), 98.
[324] Wetboek van Strafrecht.
[325] ibid, art 138a
[326] ibid, art 194
[327] ibid, art 327

severe offences, such as falsifying metrological marks,[328] distributing materials inciting criminal acts,[329] and falsifying public service records,[330] carry penalties of up to three years.

Germany is known for its adherence to the principle of mandatory prosecution, although recent decades have seen a greater deviation from this ideal in practice.[331] Under the German Criminal Code,[332] crimes punishable by a maximum term of one year include trespassing,[333] misuse of emergency services,[334] and violation of supervision instructions.[335] On the other hand, offences such as disturbance of religious practices,[336] embezzlement,[337] and unauthorised use of a vehicle[338] are punishable by up to three years.

Sweden represents the Scandinavian legal culture, which significantly differs from the rest of Europe, particularly regarding the police role.[339] The Swedish Criminal Code[340] prescribes that crimes punishable by a maximum term of one year include unlawful dispossession,[341] unlawful diversion of power,[342] and unauthorised use of another's property.[343] Slightly more severe offences, such as intrusive photography,[344] breach of postal or telecommunications secrecy,[345] and improper favouring of a creditor,[346] carry maximum penalties of two years.

Finally, Poland reflects Eastern European legal traditions, marked by a strong adherence to the principle of legality and efforts to decriminalise minor offences.[347] Under the Polish Criminal Code,[348] crimes punishable by a maximum term of one year include

[328] ibid, art 218
[329] ibid, art 132
[330] ibid, art 360
[331] Jehle, Wade and Elsner (n 307), 98
[332] Strafgesetzbuch – StGB
[333] ibid, section 123
[334] ibid, section 145
[335] ibid, section 145a
[336] ibid, section 167
[337] ibid, section 246
[338] ibid, section 248b
[339] Jehle, Wade and Elsner (n 307), 98
[340] Brottsbalken, SFS 1962:700
[341] ibid, chapter 8 section 8
[342] ibid, chapter 8 section 10
[343] ibid, chapter 10 section 7
[344] ibid, chapter 4 section 6a
[345] ibid, chapter 4 section 8
[346] ibid, chapter 11 section 4
[347] Jehle, Wade and Elsner (n 307), 98.
[348] Kodeks karny

disturbing the peace of a home,[349] defamation via mass communication,[350] and insults delivered through media platforms.[351] Offences such as approving the operation of a dangerous vehicle,[352] bigamy,[353] and inducing a minor to drink alcohol [354] are punishable by up to two years.

2.3. Main Findings

This comparative analysis reveals that some non-violent, administrative, and economic offences included under Prüm II fail to meet the stricter criteria for classification as serious crimes under EU law. These offences often fail to align with the categories enumerated in Article 2(2) of Council Framework Decision 2002/584/JHA, highlighting a significant divergence between the broader scope of Prüm II and the more rigorous thresholds established by EU legal standards.

By allowing the automated searching of facial images for offences that may not qualify as serious crimes, Prüm II risks infringing the case law of the CJEU and overlooks critical opinions from EDPS. Considering that the automated exchange of facial images already constitutes a serious intrusion on fundamental rights to privacy and data protection, extending this measure to less severe offences may render the Regulation disproportionate.

This potential breach of the principle of proportionality calls for a thorough evaluation of whether Prüm II's current scope aligns with the requirements set out in Article 52(1) of the Charter. To address this, the next chapter will undertake an in-depth analysis to assess whether automated facial image searches for offences punishable by a maximum term of at least one year meet the proportionality requirements under EU law.

[349] ibid, art 193
[350] ibid, art 212
[351] ibid, art 216
[352] ibid, art 179
[353] ibid, art 206
[354] ibid, art 208

VI. Proportionality Assessment of the Inclusion of Facial Images

The preceding chapters have examined the potential for the inclusion of facial images within the Prüm II framework to infringe upon the fundamental rights and freedoms of data subjects. Automated facial image searches directly interfere with the fundamental right to the protection of personal data,[355] which is intrinsically connected to the fundamental right to respect for private and family life.[356]

Fundamental rights, however, are not absolute and may be limited in accordance with Article 52(1) of the Charter.[357] Such limitations must satisfy the following cumulative criteria: they must be provided by law, respect the essence of the affected rights, and genuinely pursue objectives of general interest recognised by the EU or protect the rights and freedoms of others. Limitations that meet these requirements must also pass the necessity and proportionality tests.[358]

The CJEU case law has consistently held that any processing of personal data constitutes a limitation on the fundamental rights to privacy and data protection, regardless of whether such limitations can be justified.[359] Effectively, the processing of facial images inherently represents a serious interference with these rights, irrespective of the context or outcomes of the processing. [360]

The following sections will assess the compliance of the inclusion of facial images under Prüm II with each one of the requirements provided by Article 52(1) of the Charter, so as to conclude if such limitation is lawful. The assessment is exclusively focused on the automated search and exchange of facial images between Member States for the purposes of criminal investigations

1. Provided by Law

Article 52(1) of the Charter establishes that any limitation on fundamental rights must be provided by law. In this context, the Prüm II Regulation, specifically Article 20, provides a formal legal basis for the limitation of the fundamental rights in question.

[355] Charter of Fundamental Rights of the European Union (n 9), art 8
[356] ibid, art 7
[357] European Data Protection Supervisor, 'EDPS Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (February 2019), 6 <https://www.edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures> accessed 4 May 2024
[358] Charter of Fundamental Rights of the European Union (n 9), art 52(1)
[359] European Data Protection Supervisor, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (April 2017), 7 <https://www.edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en> accessed 10 October 2024
[360] European Data Protection Board (n 113), 5

However, the mere existence of a legal foundation is insufficient – the law must be accessible and foreseeable.[361]

Accessibility requires that individuals be able to access the legal provision.[362] Prüm II satisfies this requirement, as it has been published in the Official Journal of the EU and is readily available to the public.[363] Foreseeability, however, proves more problematic. For a legal measure to be foreseeable, its scope and application[364] must be sufficiently clear, outlining the conditions under which authorities are empowered to act,[365] so that individuals can reasonably anticipate its consequences to their rights.[366]

Prüm II lacks the necessary clarity to meet the foreseeability standard. One of the primary issues lies in its failure to specify which criminal offences justify automated searches of facial images. Instead of providing a definitive list of offences or categories, the Regulation defers this determination to the national laws of the requesting Member State.[367] This approach creates significant legal uncertainty, as the crimes that could trigger such searches vary from one jurisdiction to another. Individuals cannot reasonably foresee how the Regulation might impact their rights without detailed knowledge of the differing national laws.

Prüm II also fails to establish harmonised criteria for the composition of national facial image databases, delegating this responsibility to Member States. In particular, the Regulation allows each Member State to decide on the availability of victims' reference data based on its own national laws. This lack of harmonisation results in varying levels of protection for individuals across the EU, further undermining foreseeability.

Another significant concern is the lack of clarity regarding the categories of data subjects that the requesting Member State's searches aim to identify. As previously highlighted, Prüm II's restriction of facial image searches to individual cases[368] allows them to be conducted regarding single files.[369] As such, searches may encompass any

[361] European Data Protection Supervisor (n 357), 7
[362] *Weber and Saravia v Germany* ECHR 2006-XI 54934/00, para 84 cited in European Data Protection Supervisor (n 357)
[363] European Union Agency for Fundamental Rights, 'Applying the Charter of Fundamental Rights of the European Union in Law and Policymaking at National Level - Guidance' (Publications Office 2018), 71 <https://fra.europa.eu/en/publication/2018/applying-charter-fundamental-rights-european-union-law-and-policymaking-national> accessed 27 November 2024
[364] European Data Protection Supervisor (n 357), 10
[365] European Data Protection Board (n 113), 15
[366] *Weber and Saravia* (n 338), para 84
[367] Prüm II Regulation (n 7), art 20(1)
[368] ibid, art 20(1) 2nd part
[369] ibid, art 4(10)

individual covered by that file, including suspects, victims, witnesses, and others.[370] This ambiguity creates the potential for excessively broad targeting, encompassing a wide range of individuals without clear limitations.

Therefore, while Prüm II provides a formal legal basis for limiting fundamental rights, it lacks the necessary foreseeability. For this reason, the first requirement of Article 52(1) cannot be considered satisfied. Nonetheless, this research will proceed to analyse the remaining requirements to provide a comprehensive assessment and contribute to the literature on this topic.

2. Respect the Essence of Fundamental Rights

The second requirement under Article 52(1) stipulates that any limitation on fundamental rights must respect their essence. This means that the rights to privacy and to the protection of personal data cannot be deprived of their basic content in a way that renders them meaningless or impossible to be effectively exercised.[371] A violation of this principle occurs namely when a measure imposes limitations irrespective of individual conduct or specific circumstances.[372]

Prüm II explicitly restricts facial image searches to the prevention, detection, and investigation of specific criminal offences.[373] While this research has contended that the threshold for qualifying criminal offences is relatively low, Article 20(1) confines the limitation on fundamental rights to narrowly defined circumstances.[374] However, this framework is broadened by Article 50(1), which allows the processing of personal data for purposes beyond those for which it was supplied, if the Member State that provided the data grants prior authorisation. This provision significantly broadens the scope of allowed data processing, enabling its use for any authorised purpose and violating the principle of purpose limitation, enshrined in the Charter[375] and the LED,[376] which requires that personal data are processed only for specified purposes, explicitly defined by law.[377]

As such, Prüm II's failure to clearly and narrowly define those purposes violates the essence of the fundamental right to the protection of personal data. As a result, the Regulation does not comply with the second requirement of Article 52(1).

[370] European Digital Rights (n 14), 22
[371] European Data Protection Supervisor (n 357), 8
[372] European Data Protection Board (n 113), 16
[373] Prüm II Regulation (n 7), art 20(1).
[374] European Union Agency for Fundamental Rights (n 363), 72
[375] Charter of Fundamental Rights of the European Union (n 9), art 8(2)
[376] Directive (EU) 2016/680 (n 15), art 4(1)(b)
[377] European Union Agency for Fundamental Rights (n 126), 25

3. Meet Objectives of General Interest

Under article 52(1), limitations on fundamental rights must be justified by objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.[378]

Prüm II aims to improve, streamline, and facilitate the exchange of criminal information between Member States for the prevention, detection, and investigation of criminal offences.[379] As such, the Regulation's general objective is to safeguard the internal security of the EU,[380] thereby ensuring the protection of individuals' rights to life[381] and security.[382]

In this regard, Prüm II meets an objective of general interest recognised by the TFEU[383] and the TEU[384] while simultaneously upholding fundamental rights enshrined in the Charter. As such, the Regulation meets the third requirement of Article 52(1).

4. Necessity

The principle of necessity requires assessing the effectiveness of a measure in achieving its intended objective and the existence of less intrusive alternatives that could achieve the same goal.[385] The LED reinforces this requirement, stipulating that the processing of biometric data for the unique identification of individuals– such as in the case of Prüm II – is permissible only when it is strictly necessary.[386]

This strict necessity standard, firmly rooted in the CJEU case law, applies to any measures restricting fundamental rights to privacy and data protection. It demands that limitations be strictly necessary, not merely necessary, thereby narrowing the judicial system's discretion when reviewing such measures.[387] According to the Article 29 Working Party (WP29), the concept of "strict necessity" requires a "rigorous and particularly solid justification for the processing of sensitive data".[388] It goes beyond the necessity requirement by insisting that no less intrusive means must exist to achieve the

[378] European Data Protection Board (n 113), 16
[379] Prüm II Regulation (n 7), recital 2 and art 2
[380] SWD(2021) 378 final
[381] Charter of Fundamental Rights of the European Union (n 9), art 2
[382] ibid, art 6
[383] Treaty on the Functioning of the European Union (n 60), art 67(3)
[384] Treaty on European Union [2012] OJ C 326, art 4(2)(j)
[385] European Data Protection Supervisor (n 357), 10
[386] Directive (EU) 2016/680 (n 15), art 10
[387] European Data Protection Supervisor (n 359), 7
[388] Article 29 Working Party on Data Protection, 'Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)' (European Commission 2017), 9 <https://ec.europa.eu/newsroom/article29/items/610178/en> accessed 17 October 2024

intended purpose, thereby safeguarding fundamental rights.[389]

4.1. Detailed Factual Description

The first stage of the necessity test involves providing a detailed factual description of the purposed measure.[390] Prüm II facilitates the automated search and exchange of facial image reference data for the prevention, detection and investigation of criminal offences, punishable by a maximum term of imprisonment of at least one year, as determined by the law of the requesting Member State.[391]

To enable this, Member States must grant other Member States access to the facial image reference data of suspects, convicted persons and, where permitted by national law, victims from their national databases created for this purpose.[392] The processing is conducted by public authorities with the relevant competencies.[393]

The processing of facial images operates through facial image recognition systems.[394] A list of the matches generated by the system is returned in an automated manner, accompanied by a ranking[395] based on the comparison of the biometric data used in the query against the biometric data supplied by the requested Member State.[396]

4.2. Fundamental Rights Affected

To evaluate the necessity of the proposed measure, it is also crucial to identify the fundamental rights impacted by the limitation.[397] As previously established, the processing of biometric data under Prüm II constitutes a significant limitation on the fundamental rights to privacy and data protection. However, the potential impact of the measure extends beyond these rights to others intrinsically linked to them.

One area of concern is the potential impact on freedoms central to democratic society. The deployment of FRT, with its capacity for mass surveillance, risks undermining the freedom of thought, conscience, and religion,[398] the freedom of expression and information,[399] and the freedom of assembly and association.[400] The presence of this pervasive technology provides an environment in which individuals may

[389] Raposo (n 115), 520
[390] European Data Protection Supervisor (n 359), 9
[391] Prüm II Regulation (n 7), art 20(1)
[392] ibid, art 19(1)
[393] ibid, art 4(26)
[394] ibid, recital 27
[395] ibid, art 37(5)
[396] ibid, art 37(4)
[397] European Data Protection Supervisor (n 359), 9
[398] Charter of Fundamental Rights of the European Union (n 9), art 10
[399] ibid, art 11
[400] ibid, art 12

feel inhibited from openly expressing themselves, protesting, seeking information or practising their beliefs.

In addition to its impact on these freedoms, inaccuracies in FRT, particularly in the identification of minority groups, exacerbate the risk of unfair treatment and discrimination, thus infringing with the rights to equality[401] and non-discrimination[402].

Finally, the rights to good administration,[403] an effective remedy, and a fair trial[404] are compromised when facial images are collected and processed without individuals' knowledge. This lack of transparency diminishes data subjects' capacity to challenge violations or seek redress, thereby eroding the safeguards necessary for the protection of their fundamental rights.

4.3. Legitimacy of the Objective

Assessing the legitimacy of the objective pursued by the measure constitutes another key stage of the necessity test. The purpose of the processing of personal data must be sufficiently and clearly described and supported by objective evidence, such as facts and statistical data. Additionally, it must be real, present and imminent, and address a critical need for the functioning of society.[405]

As previously outlined, Prüm II pursues the objective of general interest recognised by the EU of enhancing cross-border cooperation in criminal and judicial matters through the exchange of information.[406] This objective is driven by several pressing concerns. Among them, the European Commission has cited the rise in organised crime, especially cybercrime, the growing threat of violent right-wing extremism, and recent racially motivated attacks as critical motivators. Additionally, concerns about the potential exploitation of AI by criminals have underscored the urgency of coordinated action.[407] Serious crimes such as sexual violence, fraud[408] and human trafficking reached their highest values in 2022,[409] while data from 2021 revealed that over 70% of organised

[401] ibid, art 20
[402] ibid, art 21
[403] ibid, art 41
[404] ibid, art 47
[405] European Data Protection Supervisor (n 359), 14 and 15
[406] Prüm II Regulation (n 7), art 2
[407] COM(2020) 605 final
[408] Eurostat, 'Crime Statistics' (*eurostat*, April 2024) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics> accessed 28 November 2024.
[409] Eurostat, 'Trafficking in Human Beings Statistics' (*eurostat*, January 2024) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Trafficking_in_human_beings_statistics> accessed 28 November 2024.

crime groups operated in more than three Member States.[410]

Prüm II thus arises to address both persistent and emerging cross-border criminal threats and to prevent the escalation of future criminal activity. It aims to tackle challenges that cannot be adequately managed by individual Member States acting alone, reinforcing the need for a harmonised and cooperative approach at the EU level.[411]

The Regulation establishes a concrete and legitimate objective supported by substantial evidence from EU bodies, which highlights an increase in serious criminality across Member States. This rise poses a considerable threat to the safety and security of EU citizens, undermining their perception of safety[412] while also jeopardising the functioning of society due to the significant economic losses caused by such crimes.[413]

While the objective pursued by Prüm II of enhancing cross-border cooperation to combat criminal offences is both real and urgent, it is not sufficiently supported by evidence. The facts and statistical data cited above highlight the pressing need to combat serious criminality, which has been increasing. However, Prüm II does not address exclusively serious criminality, it also aims at fighting minor crimes, a need that is not sufficiently supported by evidence. Therefore, the objective lacks legitimacy.

4.4. Effectiveness and Intrusiveness of the Limitation

Finally, the fourth step of the necessity test involves assessing the effectiveness and intrusiveness of the limitation, ensuring it is the least intrusive measure capable of achieving the intended purpose.[414]

To satisfy this requirement, the measure must be genuinely effective, meaning that it is essential for achieving its purpose – mere convenience or cost-effectiveness is not enough. When sensitive data is involved, such as facial images, a higher threshold must be applied to evaluate the measure's effectiveness.[415]

In criminal investigations, facial images are often the only lead captured from a crime scene. Consequently, their processing is critical for identifying suspects or

[410] Europol, 'European Union Serious and Organised Crime Threat Assessment A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime' (December 2021), 19 <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021> accessed 28 November 2024.
[411] Prüm II Regulation (n 7), recital 45.
[412] COM(2020) 605 final.
[413] Katrien Luyten and Alessia Rossi, 'Understanding the EU's Response to Organised Crime' (Think Tank European Parliament 2022), 2 <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)652043> accessed 28 November 2024.
[414] European Data Protection Supervisor (n 359), 16
[415] ibid, 17

convicted criminals. Comparing these facial images against those stored in databases of other Member States significantly increases the likelihood of accurate identification.[416] However, the purpose of fighting crime can only be effectively achieved if the processing of facial images ensures the accurate identification of suspects and convicted criminals.

As previously highlighted, FRTs are prone to accuracy issues, including false positives and false negatives. Prüm II does not specify the technology to be employed for facial image comparisons, particularly regarding its accuracy rates.[417] Additionally, the Regulation fails to establish minimum quality standards for the comparison of facial images.[418] As these critical aspects are deferred to the implementing acts,[419] it is not currently possible to fully assess the effectiveness of the measure.

Moreover, the measure must be the least intrusive option, considering the rights at stake. This requires considering alternative measures that are real, sufficient, comparably effective, and less threatening to fundamental rights.[420] Under current national laws, Member States already collect facial images of suspects and convicted criminals and store them in national criminal databases. These images are frequently shared across borders for the purpose of criminal investigations. Nevertheless, under Prüm I, such exchanges were conducted manually due to limitations in the types of data that could be shared, such as DNA, dactyloscopic data, and vehicle registration data. This process proved inefficient and time-consuming.[421]

The only alternative to Prüm II is to maintain the Prüm I framework in force and continue the manual exchange of facial images.[422] This method is not sufficiently effective compared to the streamlined procedures proposed under Prüm II, which enable automatic and efficient sharing. Thus, there is no viable, less intrusive alternative that achieves comparable outcomes.

Lastly, this assessment must justify the necessity of the proposed measure by highlighting the insufficiency of existing measures, supported by evidence.[423] In this regard, it has been proven that the lack of an efficient procedure for exchanging facial images has led to errors, information gaps and reluctance among law enforcement

[416] SWD(2021) 378 final
[417] Prüm II Regulation (n 7), recital 27
[418] ibid, art 22(2)
[419] ibid, art 31
[420] European Data Protection Supervisor (n 359), 17
[421] SWD(2021) 378 final
[422] ibid
[423] European Data Protection Supervisor (n 359), 18

authorities to initiate exchanges. To maximise efficiency, Member States would restrict their queries to countries they believed to be most likely to hold relevant data. However, experience has demonstrated that other Member States often possess pertinent information.[424] Integrating facial image exchanges within the Prüm II framework eliminates such gaps and ensures that all relevant data is accessible to law enforcement officers.[425]

Although the necessity test remains incomplete due to the absence of critical information required to assess the effectiveness of the limitation, the inclusion of facial images under Prüm II emerges as the least intrusive and most viable measure currently available to achieve the objective of combating criminality.

5. Proportionality

Proportionality, in a narrow sense, encompasses the appropriateness of a measure, specifically the extent to which a clear connection exists between the measure and its intended objective.[426] The principle requires a careful balance between the intensity of the interference and the purpose it aims to achieve. A measure is deemed proportionate when the benefits resulting from it are not outweighed by disadvantages on fundamental rights.[427] Convention 108[428] articulates this principle, stating that data processing must align with the legitimate interests pursued, balancing the interests, rights, and freedoms at stake.[429]

Assessing proportionality also entails examining the safeguards accompanying the measure to reduce potential risks.[430] A prior assessment, conducted in Chapter II, concluded that the safeguards provided by the Regulation are inadequate, failing to protect the rights and interests of data subjects.

5.1. Scope, Extent and Intensity of the Interference

In addition to the requirements previously evaluated, the proportionality test also demands a thorough assessment of the scope, extent and intensity of a measure's interference with fundamental rights.[431]

[424] SWD(2021) 378 final
[425] ibid.
[426] European Data Protection Supervisor (n 359), 5
[427] European Data Protection Supervisor (n 357), 9
[428] Convention 108+ Convention for the Protection of Individuals with regard to the Processing of Personal Data, art 5
[429] European Data Protection Supervisor (n 357), 11
[430] ibid, 10
[431] ibid, 20

Regarding the scope of the measure, this evaluation requires identifying the individuals affected, whether data subjects or others.[432] While the impact may appear minor for the individual concerned, it can still carry significant consequences for society at large.[433]

Prüm II facilitates the exchange of facial images stored in databases established under national laws.[434] These databases vary substantially across Member States, with some including non-criminal data, such as images of document applicants, immigrants, asylum seekers, and even victims, where national laws permit. Moreover, Prüm II does not specify which individuals may be identified by the requesting Member State through automated searches, thereby allowing the identification of any individual with a connection to the offence.[435] Additionally, facial image matches are returned to the requested Member State as a list containing sensitive data of non-matching individuals, therefore promoting the unauthorised exchange of biometric data.[436] The Regulation thus has an expansive scope, with the potential for further broadening depending on individual Member States' practices.

Furthermore, the extent of the interference must be evaluated, considering the volume of information gathered, the duration of data retention, and whether special categories of data are processed.[437] Facial images, classified as sensitive data under the LED, warrant heightened protection due to the significant risks they pose to fundamental rights and freedoms.[438] The Regulation does not set requirements for how these images are captured, permitting collection in both controlled and uncontrolled environments, often without the data subjects' knowledge. Depending on the circumstances, such images may reveal intimate details about an individual's personal intimacy, health, family life, sexuality,[439] religion, political affiliation, etc.

Key aspects such as the time frame for data collection and the scope of the data gathered remain at the discretion of Member States. However, these must comply with EU legislation on the matter, particularly the principles of purpose limitation and data

[432] ibid, 23
[433] ibid, 20
[434] Prüm II Regulation (n 7), art 19(1)
[435] ibid, art 20(1)
[436] European Digital Rights (n 14), 27
[437] European Data Protection Supervisor (n 357), 23
[438] Directive (EU) 2016/680 (n 15), recital 37
[439] Joined cases C-465/00, C-138/01, and C-139/01, *Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* [2003] ECR I-04989, para 52 cited in European Data Protection Supervisor (n 357)

minimisation.

The intensity of the interference is amplified when profiling and automated decision-making systems are involved.[440] In this regard, the Regulation specifically prohibits profiling[441] that results in discrimination,[442] therefore permitting other forms of profiling. Profiling, in this context, entails the automated processing of facial images to assess certain attributes of the data subjects to analyse or predict their behaviour, location, preferences, or personal characteristics.[443] Moreover, searches under Prüm II are conducted in an automated manner, producing matches that are also returned through automated processes.[444] At this stage, human oversight in confirming these matches is optional,[445] which raises concerns about the reliability of such systems, given the well-documented accuracy issues of FRTs. Additionally, as previously highlighted, the employment of facial recognition by law enforcement authorities has the potential to enable mass surveillance, through the indiscriminate processing of facial images, as practices from multiple EU Member States have shown.

In conclusion, this thorough analysis of scope, extent, and intensity reveals that the Regulation constitutes a serious interference with fundamental rights to privacy and data protection.

5.2. Fair Balance Evaluation

The next step in the proportionality test involves evaluating whether the measure strikes a fair balance between its importance and effectiveness and its interference with fundamental rights.[446]

This balance begins with addressing information asymmetry: it is necessary to determine whether all the relevant information has been collected and whether the benefits and costs of the measure have been properly assessed.[447] As noted in the necessity test, the Regulation defers critical aspects of facial image processing to implementing acts, complicating a comprehensive evaluation of the measure's effectiveness. This lack of clarity undermines the assessment of whether the benefits outweigh the costs.

[440] European Data Protection Supervisor (n 357), 23 and 24
[441] Prüm II Regulation (n 7), art 20(1) in fine
[442] Directive (EU) 2016/680 (n 15), art 11(3)
[443] ibid, art 3(4)
[444] Prüm II Regulation (n 7), art 20(1) and art 37(3)
[445] ibid, art 20(2)
[446] European Data Protection Supervisor (n 357), 27 and 28
[447] ibid, 28

Then, the constraints on fundamental rights shall be compared with the benefits.[448] Improved information exchange between law enforcement authorities has the potential to facilitate successful investigations, enhancing public safety[449] and upholding the fundamental rights to life and security. However, the effectiveness of such benefits depends on the accuracy of identification, otherwise, the claimed security advantages are diminished. Furthermore, the processing of facial images for identification purposes risks interfering with multiple fundamental rights, ultimately creating a constant fear of surveillance among citizens.[450]

Balancing the potential benefits of increased internal security with the serious interference with multiple rights, this analysis concludes that only the objective of combating serious crime could justify such a measure.[451] This aspect was also emphasised by the EDPB, according to which Prüm II must define the types of crimes it covers and establish a clear severity threshold to exclude petty offences, particularly given the sensitive nature of biometric data.[452]

5.3. Conclusion on the Proportionality of the Measure

Finally, the proportionality test must conclude on the proportionality of the measure. If the measure does not comply with the principle, it should be revised to ensure compliance.[453]

Prüm II fails to restrict the processing of facial images to the prevention, detection, and investigation of serious crimes. Instead, it sets a low threshold, allowing the employment of intrusive measures to fight minor crimes, as well as economic and administrative offences. This broad application exacerbates the risk of disproportionate interference with fundamental rights.

Although Prüm II lacks sufficient information regarding the effectiveness of FRTs for identification purposes, even in a scenario where such technologies achieve high levels of accuracy, their application to minor offences remains highly problematic.

Consequently, this research concludes that permitting the processing of facial images for the prevention, detection, and investigation of criminal offences punishable

[448] ibid
[449] Commission, 'Inception impact assessment - Ares(2020)4214748' (August 2020), 5 <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12563-Strengthening-the-automated-data-exchange-under-the-Prum-framework_en> accessed 29 November 2024.
[451] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970 [2016] Court reports – general cited in European Data Protection Supervisor (n 357)
[452] European Data Protection Board (n 113), 16
[453] European Data Protection Supervisor (n 357), 32

by a maximum term of imprisonment of at least one year under the law of the requesting Member State renders Regulation Prüm II disproportionate.

Conclusion

This dissertation concludes that Prüm II, in its current form, fails to meet the requirements of Article 52(1) of the Charter. Specifically, the limitation under analysis is not sufficiently provided by law, infringes upon the essence of the fundamental right to data protection, and is disproportionate. As such, the Regulation cannot be deemed lawful in its current form.

By deferring the regulation of national databases' content to Member States' laws, Prüm II introduces significant risks. For instance, it allows Member States to include facial images captured through remote biometric identification systems in their databases. Such practice facilitates mass surveillance, deterring individuals from exercising their fundamental rights and freedoms in public spaces[454] and undermining the presumption of innocence,[455] since all individuals are treated as potential suspects.[456] In addition, many Member States' criminal databases contain data belonging to asylum seekers, migrants, and foreign nationals. Integrating such data into the Prüm II framework risks exacerbating the criminalisation of migration and potentially contravenes international humanitarian obligations.[457]

These concerns are further heightened by the rise of far-right governments and authoritarian regimes within the European Union.[458] Discriminatory law enforcement practices, often rooted in political narratives surrounding immigration control, cultural incompatibilities, and crime prevention,[459] could be amplified by the misuse of facial recognition as a state surveillance tool.

A revision of the Regulation is, therefore, essential to ensure its compliance with the Charter. To begin with, the limitation should be clearly restricted to a specific list of serious crimes. In this context, a reference could be even made to those criminal offences established under Article 83(1) of the TFEU or to those listed in Article 2(2) of the Council Framework Decision 2002/584/JHA. The maximum term of imprisonment threshold should also be modified, aligning with the three years threshold provided by

[454] European Union Agency for Fundamental Rights (n 126), 30
[455] European Digital Rights (n 14), 3
[456] Jakubowska (n 227)
[457] European Digital Rights (n 14), 12
[458] Ruth Green, 'The Year of Elections: The Rise of Europe's Far Right' (2024) International Bar Association <https://www.ibanet.org/The-year-of-elections-The-rise-of-Europes-far-right> accessed 6 December 2024
[459] Williams and Kind (n 140), 9

Regulation (EU) 2019/818[460] or the four years threshold provided by the AI Act,[461] through an in-depth analysis of these two options.

Moreover, the Regulation should exclude the availability of victim's facial images from the databases, to avoid differing protection levels across Member States. Similarly, it should explicitly restrict the content of criminal databases to facial images of suspects and convicted criminals, excluding non-criminal data entirely.

A revision of Article 50(1) is also imperative, as it significantly broadens the scope of the Regulation. Ultimately, this provision should be removed to ensure respect for the essence of the fundamental right to data protection.

In addition, Prüm II must establish requirements for facial recognition technology, specifically regarding accuracy, to enable an evaluation of its effectiveness and necessity. It should also provide clear criteria regarding which data subjects can be identified by the Member States and under what conditions, substituting the 'individual case' requirement and ensuring that the use of such invasive technology is both precise and justified.

Lastly, the safeguards within the Regulation also require strengthening to effectively and adequately protect the rights and interests of the data subjects. This includes prohibiting any form of profiling and including human oversight, with manual confirmation of matches, as a mandatory requirement. In this regard, it is important to emphasise that, even if all those changes are incorporated, the potential of facial recognition for enabling mass surveillance renders the Regulation disproportionate. As previously highlighted, mass surveillance cannot be deemed necessary or proportionate under the Charter, the ECHR, or the LED.[462] As such, Prüm II should additionally prohibit the inclusion of facial images captured through remote biometric identification systems in national criminal databases used for the search and exchange under the Regulation.

While implementing these changes is critical to ensure that Prüm II aligns with the requirements of Article 52(1) of the Charter, they remain insufficient in addressing the broader challenges posed by facial recognition. The absence of harmonised and robust regulatory frameworks at the EU level has already prompted calls for a moratorium on the use of such technology, particularly in law enforcement contexts.[463] Given Prüm II's scope, a regulatory framework established at the EU level is essential to provide legal

[460] Regulation (EU) 2019/818 (n 302), art 4 (22)
[461] Artificial Intelligence Act (n 16), recital 33
[462] Jakubowska and Naranjo (n 143), 19
[463] Hill, O'Connor and Slane (n 124), 326

certainty and coherence across Member States.[464]

The precautionary principle enshrined in the TFEU[465] provides a solid basis for such a moratorium. By allowing the suspension of policies where potential harm is uncertain, this principle ensures that societal risks are minimised.[466] This position is supported by the EDPS, who argues that the precautionary principle justifies a ban, even if temporary, on facial recognition until its risks to society and individual freedoms are thoroughly assessed.[467]

Therefore, this dissertation concludes that Prüm II fails to comply with the principle of proportionality in balancing the protection of personal data and privacy with the imperative of high-level cross-border security. Although the employment of facial recognition by law enforcement authorities has enabled state mass surveillance within the EU, such a reality is not inevitable and can be avoided if proper safeguards are enforced.

[464] Dushi (n 91), 9
[465] Treaty on the Functioning of the European Union (n 60), art 191
[466] Publications Office of the European Union, 'Precautionary principle' (*EUR-Lex*) <https://eur-lex.europa.eu/EN/legal-content/glossary/precautionary-principle.html> accessed 6 December 2024
[467] Wojciech Wiewiórowski, 'AI and Facial Recognition: Challenges and Opportunities' (*European Data Protection Supervisor* 2020) <https://www.edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities> accessed 6 December 2024

Cases

Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others EU:C:2016:970 [2016] Court reports – general

Joined Cases C-465/00, C-138/01, and C-139/01, Rechnungshof v Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk [2003] ECR I-04989

Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen [2010] ECR I-0000

Weber and Saravia v Germany ECHR 2006-XI 54934/00

Legislation

Brottsbalken, SFS 1962:700

Charter of Fundamental Rights of the European Union [2012] OJ C 326

Code Pénal

Convention 108+ Convention for the Protection of Individuals with regard to the Processing of Personal Data

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L 210

Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L 210

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision [2002] OJ L 190/1

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L 386

Decreto-Lei n.º 48/95, de 15 de março (Código Penal)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2008] OJ L 119

Kodeks karny

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L 135

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 [2019] OJ L 135/85

Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) [2024] OJ L, 2024/982

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L, 2024/1689

Strafgesetzbuch – StGB

Treaty on European Union [2012] OJ C 326

Treaty on the Functioning of the European Union [2012] OJ C 326

Wetboek van Strafrecht

Bibliography

--‘Hamburg G20 Summit protests facial analysis database legality’ (*AIAAIC*, February 2023) <https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/hamburg-g20-protests-facial-recognition-surveillance> accessed 13 November 2024

Article 29 Working Party on Data Protection, ‘Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)’ (European Commission 2017) <https://ec.europa.eu/newsroom/article29/items/610178/en> accessed 17 October 2024

Carrer L, Coluccini R, Di Salvo P, ‘Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale’ *Wired* (9 June 2020) <https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/> accessed 5 November 2024

Cavalli R, ‘Prüm II and the EPRIS Index in Europe: An Attempt to Balance People’s Security and Privacy?’ (2024) 14 CS & IT Conference Proceedings 57 <https://doi.org/10.5121/csit.2024.140706> accessed 3 December 2024

Chelioudakis E, ‘Greece: Technology-Led Policing Awakens’ (*about:intel*, 29 June 2020) <https://aboutintel.eu/greece-policing-border-surveillance/> accessed 5 November 2024

Commission, ‘A New Way Forward on Internal Security’ (*European Commission*) <https://home-affairs.ec.europa.eu/policies/internal-security/new-way-forward-internal-security_en> accessed 18 September 2024

Commission, ‘Communication from the Commission on the EU Security Union Strategy 2020' (Communication) COM(2020) 605 final

Commission, ‘European Security Union’ (*European Commission* 2020) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en> accessed 18 September 2024

Commission, ‘Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council’ (Commission Staff Working Document) SWD(2021) 378 final

Commission, ‘Inception impact assessment - Ares(2020)4214748’ (August 2020) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12563-Strengthening-the-automated-data-exchange-under-the-Prum-framework_en> accessed 29 November 2024

Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on automated data exchange for police cooperation (“Prüm II”), amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, 2019/817 and 2019/818 of the European Parliament and of the Council' COM(2021) 784 final

Commission, ‘Way forward on aligning the former third pillar acquis with data protection rules’ (Communication) COM(2020) 262 final

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), ‘Guidelines on facial recognition’ (Council of Europe 2021) <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html#> accessed 17 November 2024

Dauvergne P, *Identified, Tracked, and Profiled: The Politics of Resisting Facial Recognition Technology* (Edward Elgar Publishing 2022)

Dushi D, ‘The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications’ (Global Campus of Human Rights 2020) <http://dx.doi.org/10.25330/528> accessed 16 October 2024

European Commission Directorate-General for Migration and Home Affairs, ‘Study on the Feasibility of Improving Information Exchange under the Prüm Decisions’ (Publications Office 2020) <https://data.europa.eu/doi/10.2837/104991> 28 October 2024

European Data Protection Board, ‘Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement' (April 2023) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en> accessed 16 November 2024

European Data Protection Supervisor, ‘Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (April 2017) <https://www.edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en> accessed 10 October 2024

European Data Protection Supervisor, ‘EDPS Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (February 2019) <https://www.edps.europa.eu/data-protection/our-

work/publications/guidelines/edps-guidelines-assessing-proportionality-measures> accessed 4 May 2024

European Data Protection Supervisor, 'Opinion 4/2022 on the Proposal for a Regulation on Automated Data Exchange for Police Cooperation ("Prüm II")' (March 2022) <https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2022-03-02-edps-opinion-regulation-automated-data-exchange-police-cooperation> accessed 14 October 2024

European Digital Rights, 'Respecting fundamental rights in the cross-border investigation of serious crimes A position paper by the European Digital Rights (EDRi) network on the European Union's proposed Regulation on automated data exchange for police cooperation ("Prüm II")' (September 2022) <https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf> accessed 18 October 2024

European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Working document on a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime' (April 2007) <https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824en.pdf > accessed 16 September 2024

European Union Agency for Fundamental Rights, 'Applying the Charter of Fundamental Rights of the European Union in Law and Policymaking at National Level - Guidance' (Publications Office 2018) <https://fra.europa.eu/en/publication/2018/applying-charter-fundamental-rights-european-union-law-and-policymaking-national> accessed 27 November 2024

European Union Agency for Fundamental Rights, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement' (Publications Office 2019) <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law> accessed 29 October 2024

European Union Agency for Fundamental Rights, 'Police Stops in Europe: Everyone Has a Right to Equal Treatment' (*FRA*, 25 May 2021) <https://fra.europa.eu/en/news/2021/police-stops-europe-everyone-has-right-equal-treatment> accessed 23 October 2024

European Union Agency for Fundamental Rights, 'Your Rights Matter: Police Stops - Fundamental Rights Survey' (Publications Office 2021) <https://fra.europa.eu/en/publication/2021/fundamental-rights-survey-police-stops> accessed 23 October 2024

Europol, 'European Union Serious and Organised Crime Threat Assessment A corrupting influence: the infiltration and undermining of Europe's economy and society by organised

crime' (December 2021) <https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021> accessed 28 November 2024

Eurostat, 'Crime Statistics' (*eurostat*, April 2024) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics> accessed 28 November 2024

Eurostat, 'Trafficking in Human Beings Statistics' (*eurostat*, January 2024) <https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Trafficking_in_human_beings_statistics> accessed 28 November 2024

Green R, 'The Year of Elections: The Rise of Europe's Far Right' (2024) International Bar Association <https://www.ibanet.org/The-year-of-elections-The-rise-of-Europes-far-right> accessed 6 December 2024

Heilweil R, 'Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress' *Vox* (11 June 2020) <https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police> accessed 13 November 2024

Hill D, O'Connor C D and Slane A, 'Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making' (2022) 24/3 Sage Journals <https://doi.org/10.1177/14613557221089558> accessed 13 November 2024

Jakubowska E and Naranjo D, 'Ban Biometric Mass Surveillance!' (EDRi 2020) <https://edri.org/our-work/blog-ban-biometric-mass-surveillance/> accessed 29 October 2024

Jakubowska E, 'Facial Recognition and Fundamental Rights 101' (*EDRi,* 4 December 2019) <https://edri.org/our-work/facial-recognition-and-fundamental-rights-101/> accessed 4 November 2024

Jakubowska E, 'New EDRi Report Reveals Depths of Biometric Mass Surveillance in Germany, the Netherlands and Poland' (*EDRi,* 7 July 2021) <https://edri.org/our-work/new-edri-report-reveals-depths-of-biometric-mass-surveillance-in-germany-the-netherlands-and-poland/> accessed 5 November 2024

Jakubowska E, 'The Many Faces of Facial Recognition in the EU' (*EDRi*, 18 December 2019) <https://edri.org/our-work/the-many-faces-of-facial-recognition-in-the-eu/> accessed 13 November 2024

Jehle J M, Wade M and Elsner B, 'Prosecution and Diversion within Criminal Justice Systems in Europe. Aims and Design of a Comparative Study' (2008) 14 Eur J Crim

Policy Res 93 < https://doi.org/10.1007/s10610-008-9074-7 > accessed 25 November 2024

Jelinek A and Wiewiórowski W R, 'EDPB-EDPS Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)' (European Data Protection Board 2021) <https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en> accessed 17 October 2024

Luyten K and Rossi A, 'Understanding the EU's Response to Organised Crime' (Think Tank European Parliament 2022) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)652043> accessed 28 November 2024

Lynch J, 'Face Off: Law Enforcement Use of Face Recognition Technology' (Electronic Frontier Foundation 2019) <https://www.eff.org/wp/law-enforcement-use-face-recognition> accessed 14 November 2024

Matulionyte R, 'Increasing Transparency around Facial Recognition Technologies in Law Enforcement: Towards a Model Framework' (2023) 33/1 Taylor & Francis, 3 <https://doi.org/10.1080/13600834.2023.2249781> accessed 13 November 2024

Matulionyte R, 'Transparency of Facial Recognition Technology and Trade Secrets' in Monika Zalnieriute and Rita Matulionyte (eds), The Cambridge Handbook of Facial Recognition in the Modern State (2023) Cambridge University Press 60, 61 <https://doi.org/10.1017/9781009321211.006> accessed 13 November 2024

Monroy M, 'G20 in Hamburg: Data Protection Commissioner Considers Face Recognition Illegal' (*digit.site36.net*, 15 August 2018) <https://digit.site36.net/2018/08/15/g20-in-hamburg-data-protection-commissioner-considers-face-recognition-illegal/> accessed 13 November 2024

Montag D L and others 'The Rise and Rise of Biometric Mass Surveillance in the EU' (EDRi 2021) <https://edri.org/wp-content/uploads/2021/11/EDRI_RISE_REPORT.pdf> accessed 4 November 2024

Novokmet A, Tomičić Z and Vidaković I, 'Facial recognition technology in EU criminal justice - human rights implications and challenges' (2023) 7 EU and Comparative Law Issues and Challenges Series (ECLIC) 525 <https://doi.org/10.25234/eclic/27461> accessed 4 November 2024

Publications Office of the European Union, 'Precautionary principle' (*EUR-Lex*) <https://eur-lex.europa.eu/EN/legal-content/glossary/precautionary-principle.html> accessed 6 December 2024

Raposo V L, 'The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal' (2023) 29 European Journal on Criminal Policy and Research 515 <https://doi.org/10.1007/s10610-022-09512-y> accessed 4 October 2024

Reich O, 'Clearview AI - The Privacy-Breaching App That Gives Us the Creeps' (*Liberties,* 14 February 2020) <https://www.liberties.eu/en/stories/clearview-privacy-busting-app/18206> accessed 14 November 2024

Sallavaci O, 'Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange' (2017) European Journal on Criminal Policy and Research 24(3) 219 <https://doi.org/10.1007/s10610-017-9355-0> accessed 27 October 2024

Tarantola A, 'Why Clearview AI Is a Threat to Us All' (*engadget*, 12 February 2020) <https://www.engadget.com/2020-02-12-clearview-ai-police-surveillance-explained.html> accessed 14 November 2024

TELEFI project, 'Summary Report of the Project "Towards the European Level Exchange of Facial Images"' (January 2021) <https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf> accessed 18 November 2024

TELEFI project, 'Towards the European Level Exchange of Facial Images Legal Analysis for TELEFI project' (February 2020) <https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf> accessed 18 November 2024

Toom V, Granja R and Ludwig A, 'The Prüm Decisions as an Aspirational Regime: Reviewing a Decade of Crossborder Exchange and Comparison of Forensic DNA Data' (2019) 41 Forensic Science International: Genetics 50 <https://doi.org/10.1016/j.fsigen.2019.03.023> accessed 28 October 2024

Vavoula N, 'Police Information Exchange - The Future Developments Regarding Prüm and the API Directive' (Think Tank European Parliament 2020) <https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)658542> accessed 4 May 2024

Volpicelli G, 'EU Set to Allow Draconian Use of Facial Recognition Tech, Say Lawmakers' *Politico* (16 January 2024) <https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-

late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns/> accessed 13 November 2024

Wiewiórowski W, ‘AI and Facial Recognition: Challenges and Opportunities' (*European Data Protection Supervisor* 2020) <https://www.edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities> accessed 6 December 2024

Wiewiórowski W, ‘Facial Recognition: A Solution in Search of a Problem?' (*European Data Protection Supervisor* 2019) <https://www.edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem> accessed 13 November 2024

Williams P and Kind E, ‘Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe' (European Network Against Racism 2019) <https://www.enar-eu.org/data-driven-policing-the-hardwiring-of-discriminatory-policing-practices-across-europe/> accessed 23 October 2024

Index

Introduction 1

Methodology 4

I. Prüm I 6
1. Context 6
2. Legal Basis and Structure 7
3. Successes and Challenges 8

II. Prüm II 10
1. Context 10
2. General Scope 10
3. Legal Basis 11
4. Successes and Challenges of the Regulation 13

III. Facial Images in Prüm II 16
1. Inclusion of Facial Images 16
2. Overview of Facial Recognition Technology 17
3. Shortcomings of FRT 19
3.1. Accuracy 20
3.2. Discrimination and Bias 21
3.3. Transparency 23
3.4. Mass Surveillance 25
4. Safeguards 25
5. Comparative Analysis of Facial Recognition Technology in China and the United States 28

IV. Mass Surveillance 31
1. Remote Biometric Identification 31
2. Mass Surveillance 33
3. Biometric Surveillance in EU Member States 36

V. Differing National Legislations 40
1. Differing National Approaches to Facial Recognition in Law Enforcement 40
1.1. Databases Used for Facial Recognition Searches 42
1.2. Image Quality Standards 43
1.3. Training and Oversight 45
1.4. Legal Scope of Search Results 46
1.5. Use and Storage of Uncontrolled Images 46
1.6. Match Criteria in Facial Recognition Searches 47
1.7. Main Findings 48
2. Comparative Analysis of Criminal Penalties across the EU 49

2.1. Serious Criminal offences 49
2.2. Member States Criminal Penalties 50
2.3. Main Findings 53
VI. Proportionality Assessment of the Inclusion of Facial Images 54
1. Provided by Law 54
2. Respect the Essence of Fundamental Rights 56
3. Meet Objectives of General Interest 57
4. Necessity 57
4.1. Detailed Factual Description 58
4.2. Fundamental Rights Affected 58
4.3. Legitimacy of the Objective 59
4.4. Effectiveness and Intrusiveness of the Limitation 60
5. Proportionality 62
5.1. Scope, Extent and Intensity of the Interference 62
5.2. Fair Balance Evaluation 64
5.3. Conclusion on the Proportionality of the Measure 65
Conclusion 67