University of Zagreb

Faculty of Law

Matija Kontak

BIOMETRIC LAW IN MIGRATION AND ASYLUM IN THE EUROPEAN UNION

DOCTORAL THESIS

Mentors:

Prof. dr. sc. Iris Goldner Lang

Assoc. Prof. Dr. Niovi Vavoula

Zagreb, 2025.

Sveučilište u Zagrebu

Pravni fakultet

Matija Kontak

BIOMETRIJSKO PRAVO U MIGRACIJAMA I AZILU U EUROPSKOJ UNIJI

DOKTORSKI RAD

Mentorice:

Prof. dr. sc. Iris Goldner Lang

Assoc. Prof. Dr. Niovi Vavoula

Zagreb, 2025.

Note on Thesis Supervisors

Iris Goldner Lang

Professor Iris Goldner Lang is a Jean Monnet Professor of EU Law, the head of the Department of European Public Law and the vice dean for International and Interinstitutional Affairs and Quality Management at the Faculty of Law, University of Zagreb. She is the holder of the UNESCO Chair on Free Movement of Persons, Migration and Inter-Cultural Dialogue and the academic coordinator of the Jean Monnet Centre of Excellence "EU's Global Leadership in the Rule of Law".

She is also a partner in the interdisciplinary project granted by Volkswagen Foundation "Algorithmic Fairness for Asylum Seekers and Refugees (AFAR)" and in the Horizon 2022 project "Protecting Irregular Migrants in Europe: Institutions, Interests and Policies (PRIME)". She has held visiting positions at University College London and at Harvard Law School, where she was a John Harvey Gregory Visiting Professor of Law and World Organization and a Fulbright Visiting Researcher.

She completed her LLM at the London School of Economics (LSE). She is the president of the Croatian Society for European Law (FIDE affiliate); a member of the Odysseus Network; vice-chair of the Board of Trustees of the Academy of European Law (ERA) and an ERA Forum Advisory board member. Goldner Lang has been the editor-in-chief of the Croatian Yearbook of European Law and Policy, and she is now a member of its Editorial Board. Currently, she is also a member of the Editorial Board of the European Foreign Affairs Review.

She has published her research widely in the form of books, book chapters and articles in international peer reviewed journals, e.g. European Constitutional Law Review, American Journal of International Law, Journal of Human Rights, European Journal of Migration and Law and European Journal of Risk Regulation. She is a co-editor of five books, the most recent being The Changing European Union: A Critical View on the Role of Law and the Courts (co-editor with T. Ćapeta and T. Perišin, Hart Publishing, 2022), one Special Issue on "Migration in the Time of COVID-19: Comparative Law and Policy Responses" in the journal Frontiers (co-editor with J. Ramji-Nogales), a convenor of a Special Section on "Migration and the Rule of Law" in the European Constitutional Law Review (2021) and the author of a monograph From Association to Accession: How Free is the Free Movement of Persons in the EU (Eleven International Publishing, 2011).

Niovi Vavoula

Niovi Vavoula is Associate Professor and Chair in Cyber Policy at the University of Luxembourg, FDEF, Department of Law. Since 2014, she also serves as Associate Editor of the New Journal of European Criminal Law. Her primary field of expertise is on the privacy and data protection challenges stemming from the digitalisation of EU immigration control, with insights into international and national initiatives, publishing a monograph entitled Immigration and Privacy in the Law of the European Union – The Case of Information Systems (Brill Nijhoff, 2022). Niovi Vavoula has also researched on the fundamental rights challenges posed by the establishment of various avenues of processing of personal data for law enforcement purposes. Besides that, she has published extensively on the use of AI in these fields and the fundamental rights challenges coming along with it.

In addition to her monograph, Niovi Vavoula has published more than 80 contributions in her fields of expertise, presenting many articles in peer-reviewed journals (e.g. European Law Journal, European Journal of Migration and Law, European Public Law). She regularly provides expert advice to EU institutions and agencies (e.g. European Parliament, EU Fundamental Rights Agency), and civil society organisations (e.g. CEPS, ECRE). She has been awarded for the project 'EU/UK Digital Regulation and Transatlantic Data Transfers', organized by the Global Policy Institute of the Queen Mary University of London and CEPS (December 2021). Also, she has been awarded, by the Society of Legal Scholars – Research Activities Fund, for a study of AI used for immigration in the US and Canada (April 2021).

Before her appointment in February 2024, she was a Senior Lecturer (2022-2024) in Migration and Security at the School of Law of Queen Mary University of London, where she taught Criminal, AI and Migration Law. Niovi Vavoula has also been a Teacher at the LSE – London School of Economics and Science (part time, 2017-2018) and worked as a legal intern at Eurojust in the Hague (2012), at the Greek Council for Refugees in Athens (2011-2012) and at a private Athenians law firm (2009-2010).

Prof. Vavoula received a Ph.D. (2017) with a thesis on immigration and privacy in the law of the European Union at the Queen Mary University of London. She holds a LLM in European Law (2011) from the same University, and an LLB from the National and Kapodistrian University of Athens. She has been a visiting scholar at ULB – Université Libre de Bruxelles (2014), George Washington University (2022) and EUI – European University Institute (2022) (SLS Grantee).

Summary of the Thesis

This thesis examines legal issues of biometric technologies, focusing on fingerprint and facial recognition in EU migration and asylum. The main research question is whether encryption as a privacy enhancing tool can mitigate biometrics' negative impacts on migrants' and asylum seekers' fundamental rights. Recommendations are made to improve legal terminology for biometrics. EU legal rules concerning biometrics are systematised as 'biometric law' of the EU with critical analysis of CJEU and ECtHR case law. Facts relating to biometrics, such as the length and place of storage of biometric data, are constructed as biometric parameters, allowing a legal assessment of any biometric system. The thesis analyses interoperability of EU information systems arguing that biometric templates represent biometric data. The thesis conducts a fundamental rights analysis, finding that biometrics are primarily framed as a justified limitation of fundamental rights of privacy and data protection. Forced fingerprinting, especially of children for Eurodac, is deemed to infringe human dignity. The fundamental right to non-discrimination is challenging to prove in context of facial recognition due to a lack of transparency, which requires the use state-of-the-art algorithms trained on representative data, though balancing accuracy against fairness remains challenging. Encryption is explored as a legal phenomenon highlighting bloom filters and homomorphic encryption for pseudonymity, anonymity, irreversibility, and revocability. It is stated that there might be an emerging right to encryption of personal data, but that public authorities argue for the ability to decrypt any personal data for the purpose of public security. Finally, it is determined that it is necessary to use encryption in order to mitigate the negative effects of biometrics on fundamental rights, but that encryption, by itself, is not enough to address fundamental rights problems raised by biometrics.

The thesis primarily uses the methods of legal doctrinal research, including textual interpretation, contextual and teleological interpretation of legal texts and case law. The main objective is normative. The research for the thesis also involved semi-structured interviews with experts.

Key Words

Biometrics, privacy, data protection, biometric data, fingerprint and facial recognition, artificial intelligence, biometric identification and verification, encryption, non-discrimination, human dignity.

Sažetak na hrvatskom jeziku

Tema ovog rada su pravna pitanja izazvana korištenjem biometrijskih tehnologija u migracijama u Europskoj uniji (EU). U ovom radu, doktorand Matija Kontak kritički analizira pravne aspekte biometrije u području prava Europske unije. Analizira mogu li se metode enkripcije tj. šifriranja, koje su u biti matematičke metode koje skrivaju sadržaj informacija, koristiti kao pravni alati za uklanjanje negativnih učinaka biometrije na temeljna prava. Doktorand utvrđuje da je enkripcija nužan alat kako bi se ograničili negativni učinci biometrije, ali samo šifriranje nije dovoljno za postizanje odgovarajuće razine zaštite temeljnih prava kada se primjenjuje biometrija.

Glavni dio rada sastoji se od šest poglavlja: 1. Uvod, Metodologija, Istraživačka pitanja i biometrijska terminologija, 2. EU Biometrijski Lex Generalis, 3. Biometrijski podaci u migracijama i azilu: Analiza biometrijskog prava kroz sudsku praksu, informacijske sustave EU i interoperabilnost, 4. Analiza temeljnih prava biometrije primijenjene u migracijama i azilu, 5. Mogu li alati za poboljšanje privatnosti smanjiti ograničenja temeljnih prava uzrokovana korištenjem biometrijskih tehnologija u migracijama i azilu EU? i 6. Zaključci i pogled u budućnost.

Glavno istraživačko pitanje jest može li se šifriranje kao alat za poboljšanje privatnosti koristiti kao pravno rješenje za ublažavanje negativnih učinaka biometrije na temeljna prava migranata i tražitelja azila. Kako bi se odgovorilo na glavno istraživačko pitanje koje se odnosi na šifriranje i biometriju, odgovora se na na niz sporednih istraživačkih pitanja. Prvo se analizira pravni i tehnički vokabular koji se odnosi na biometriju i izrečene su preporuke o tome kako se može poboljšati pravni vokabular za objašnjenje pojmova vezanih uz biometriju i obradu biometrijskih podataka. Zatim su sistematiziraju pravila o korištenju biometrije u pravu EU, posebno u kontekstu migracija i azila. Ta pravila su nazvana u disertaciji ‘biometrijsko pravo’ Europske unije. Nakon utvrđenja najvažnijih pravnih pravila biometrijskog prava, utvrđena je te analizirana je sudska praksa Suda Europske unije i Europskog suda za ljudska prava u vezi s korištenjem biometrije kako bi se utvrdilo kako ti sudovi rješavaju biometrijske slučajeve. Biometrijska praksa sudova se kritički analizira te se savjetuje kako se pristup biometriji od strane tih sudova može poboljšati. Također se utvrđuju najvažniji elementi koje navedeni sudovi razmatraju pri odlučivanju u predmetima koji se tiču korištenja biometrije. Sljedeće se utvrđuje kako biometrija utječe na temeljna prava migranata i tražitelja azila. Zaključuje se da su privatnost i zaštita podataka temeljna prava koja se koriste za oblikovanje pravnih pitanja u vezi

s biometrijom, ali da biometrija može negativno utjecati i na temeljna prava na ljudsko dostojanstvo i nediskriminaciju. Zaključuje se da enkripcija može doprinijeti rješavanju negativnih učinaka uzrokovanih biometrijom, ali da sama enkripcija nije dovoljna za rješavanje problema temeljnih prava koje postavlja biometrija.

Prvo poglavlje objašnjava osnovne pojmove vezane uz biometriju i daje preporuke o tome kako poboljšati pravnu biometrijsku terminologiju. Najvažniji pojmovi biometrijskog prava su biometrijski podaci, biometrijska identifikacija, verifikacija i kategorizacija te biometrijski predložak. Rad predstavlja analizu ovih pojmova u pravnom smislu i određuje kako se trenutno tumače u pravu EU i kako bi ih trebalo tumačiti.

Drugo poglavlje predstavlja analizu elemenata koji čine ono što doktorand naziva biometrijsko pravo Europske unije. Istražuju su elementi koji čine definiciju biometrijskih podataka. Prema analizi, biometrijski podaci, kako ih trenutno tumači zakon, trebali bi se tumačiti kao osjetljivi osobni podaci u smislu članka 9(2) GDPR-a, iako istraživanje kandidata jasno pokazuje da postoje nesigurnosti zakonodavca u načinu na koji su biometrijski podaci trenutno definirani u GDPR-u. Zaključuje se da bi se pojam biometrijske identifikacije trebao koristiti umjesto manje preciznih pojmova omogućavanja i potvrđivanja jedinstvene identifikacije, a karakteristike spomenute u definiciji trebale bi se pojednostaviti kako bi se odnosile na bihevioralne i biološke karakteristike. Ovaj rad objašnjava kako koncept biometrijskih podataka treba tumačiti prema pravu kakvo ono trenutno jest, ali se također daju preporuke o tome kako bi se definicija biometrijskih podataka trebala poboljšati.

Drugo poglavlje sadrži sistematizaciju pravila koja čine biometrijski zakon Europske unije, što uz Opću uredbu o zaštititi osobnih podataka, uključuje odredbe Direktive (EU) 2016/680, EUDPR-a, te odredbe Akta o umjetnoj inteligenciji. Iznose se argumente da bi dio zakona o zaštiti podataka koji se odnosi na korištenje biometrije trebalo prepoznati kao zasebno biometrijsko pravo, s obzirom na specifične karakteristike obrade biometrijskih podataka i njezinu važnost. Posebno je značajna analiza odredbi koji se tiču biometrije u Aktu o umjetnoj inteligenciji Europske unije.

Treće poglavlje disertacije predstavlja kritičku analizu zakonodavstva i sudske prakse koja smješta biometrijsko pravo u specifičniji kontekst migracija i azila. Doktorand dolazi do zaključka da Sud Europske unije koristi pravni okvir privatnosti i zaštite podataka za rješavanje slučajeva koji se odnose na obradu biometrijskih podataka. Međutim, u radu se kritizira pristup Suda kao nedosljedan, pokazujući to na primjeru analizirane biometrijske sudske prakse. U radu

se uspostavljaju činjenice ili biometrijski parametri koji su važni za procjenu bilo koje biometrijske sheme s obzirom na zahtjeve prava EU o privatnosti i zaštiti podataka, a temeljeni na analiziranoj praksi sudova. Model biometrijskih parametara može omogućiti praktičarima ili istraživačima da procijene pridržava li se određeni biometrijski sustav pravnih uvjeta koje mu nameće europsko pravo. U završnom dijelu trećeg poglavlja analizira se interoperabilnost biometrijskih sustava EU i biometrijski predložak kao značajni koncepti biometrijskog prava. Doktorand u radu iznosi argumente da biometrijske predloške treba smatrati biometrijskim podacima.

Četvrto poglavlje predstavlja analizu temeljnih prava pri korištenju biometrije. Ovaj dio bio je nužan kako bi se utvrdili učinci biometrije na temeljna prava. Doktorand zaključuje da su privatnost i zaštita podataka najvažnija temeljna prava za regulaciju upotrebe biometrijskih podataka u EU, analizirajući postojeću sudsku praksu koja se odnosi na obradu biometrijskih podataka. Ovdje se u radu objašnjava zašto su upravo temeljna prava na privatnost i zaštitu podataka najznačajnija temeljna prava u slučajevima koji se odnose na biometriju. Disertacija nastavlja s ispitivanjem drugih temeljnih prava u kontekstu biometrije. U disertaciji se dolazi do zaključka da se ljudsko dostojanstvo, kao temeljno pravo, narušava praksom prisilnog uzimanja otisaka prstiju ranjivih osoba, uključujući djecu, u svrhu biometrijskog sustava Eurodac. Također se iznosi uvid da se zakonska obveza davanja otisaka prstiju može protumačiti kao promjena značenja prava na azil i definicije izbjeglice, jer da bi se ostvario status izbjeglice potrebno je dati otiske prstiju.

Disertacija nadalje, temeljem iznesenog istraživanja, tvrdi da temeljno pravo na nediskriminaciju može biti relevantno posebno u kontekstu biometrijskih algoritama za prepoznavanje lica. Provodi se kritička analiza pravnog okvira za nediskriminaciju i tehničkih aspekata pristranosti (*bias*) koje donosi tehnologija prepoznavanje lica. Zaključuje da je pravni okvir za zaštitu od diskriminacije, za razliku od privatnosti, vrlo zahtjevan za uspješnu primijenu kod upotrebe biometrije zbog strogosti pravnog okvira za diskriminaciju, posebno u slučajevima umjetne inteligencije i algoritama koji mogu biti netransparentni u svom radu. Doktorand navodi niz praktičnih preporuka i uvida. Kako bi se smanjila algoritamska pristranost, moraju se koristiti najbolji dostupni algoritmi te oni koji su najnoviji, te moraju biti „obučeni“ na podacima dovoljne kvalitete i reprezentativnog uzorka, kao zakonski zahtjev pri korištenju tehnologije prepoznavanja lica. Pristranost uzrokovanu alatima za prepoznavanje lica treba staviti u perspektivu uspoređujući je s alatima koje zamjenjuje, a ne strogo očekivati da moderne tehnologije ne smiju iskazivati bilo koju razinu pristranosti, budući da ljudi također

mogu pokazati značajnu pristranost u odlučivanju. Nadalje se obrazlaže da biometrijski algoritmi mogu dovesti do dileme tj. izbora između pravičnosti ili točnosti rezultata. To je stoga što ovi sustavi, kako bi ostvarili preciznost tj. točnost kod biometrijske identifikacije, moraju obrađivati osjetljive osobne podatke, kao što je etničko podrijetlo ili spol, što može utjecati na pravičnost.

Prethodna poglavlja sistematizirala su i kritički analizirala pravila za korištenje biometrije u Europskoj uniji u području migracija i azila te su dala odgovor kako biometrija utječe na temeljna prava pojedinaca na koja se primjenjuje. U petom poglavlju, na tom temelju, odgovara se na glavno istraživačko pitanje i provjerava se glavna hipoteza. U petom poglavlju rada prikazuje se da postoje metode enkripcije tj. šifriranja koje mogu zaštititi biometrijske predloške i time značajno smanjiti negativne učinke biometrije na privatnost i zaštitu podataka. Nadalje, već postoje pravila koja se mogu tumačiti kao pravna osnova za šifriranje biometrijskih podataka, kako u pravu EU tako i u nacionalnom pravu (koristeći prvenstveno hrvatsko pravo u analizi kao primjer nacionalnog prava) koja se mogu koristiti kao temelj za uvođenje enkripcije kao pravne obveze. Metode koje autor ističe kao posebno obećavajuće metode šifriranja su tzv. *bloom* filteri i homomorfno šifriranje.

Objašnjavaju se pravni učinci metoda šifriranja na pseudonimnost i anonimnost osobnih podataka, uz prikaz njihovih pozitivnih prednosti u smislu nepovratnosti i opozivosti biometrijskih predložaka. Navedene pojmove, zaključuje se, treba definirati kao pravne termine u zakonodavstvu koje se odnosi na korištenje biometrije. Rad otvara pitanje kako moderne metode šifriranja dovode do dileme za javna tijela u Europskoj uniji. S jedne strane, prikazuje se kako raste shvaćanje šifriranja tj. enkripcije kao novog prava u kontekstu pravnog okvira zaštite podataka (pravo na enkripciju osobnih podataka), a s druge strane raste potreba da se omogući javnim vlastima da se svi podaci mogu dešifrirati radi sigurnosti društva i države. Na kraju disertacije, obrazlaže se da je enkripcija nužan, ali ne i dovoljan element privatnosti i zaštite podataka u kontekstu onoga što autor utvrđuje kao biometrijsko pravo Europske unije.

U radu se prvenstveno koriste metode pravnog doktrinarnog istraživanja. Istraživačka pitanja su pravne prirode a metode istraživanja su metode pravne znanosti. Glavna metoda je tumačenje pravnih tekstova i sudske prakse. To uključuje metode tekstualnog tumačenja, uključujući kontekstualno i teleološko tumačenje. Istraživački podaci uključuju pretežno pravne izvore poput primarnog i sekundarnog prava Europske unije, uključujući posebno Povelju o temeljnim pravima. Detaljno se analizira sudska praksa Suda Europske unije o biometriji, pri čemu autor

kritički analizira niz povezanih slučajeva pred Sudom Europske unije koje opisuje kao biometrijsku sudsku praksu. U radu se analizira pravo Vijeća Europe, posebno članak 8. Europske konvencije o ljudskim pravima. Kandidat se u svom istraživanju oslanjao na tehnički vokabular koji se odnosi na biometriju, prvenstveno ISO standarde, kako bi popunio praznine u pravnoj terminologiji koja se odnosi na biometriju. Kao sporedna istraživačka metoda, provedeni su i intervjui sa stručnjacima.

Ključni pojmovi

Biometrija, privatnost, zaštita podataka, biometrijski podaci, prepoznavanje otisaka prstiju i lica, umjetna inteligencija, biometrijska identifikacija i verifikacija, enkripcija, zabrana diskriminacije, ljudsko dostojanstvo.

Contents

Note on Thesis Supervisors i
Iris Goldner Lang i
Niovi Vavoula ii
Summary of the Thesis iii
Key Words iii
Sažetak na hrvatskom jeziku iv
Ključni pojmovi viii
Chapter 1: Introduction, Methodology, Research Questions and Biometric Terminology 1
1.1. Introduction: The Importance of Biometrics and the Reasoning Behind the Thesis 1
1.2. Research Questions, Hypothesis and Scientific Contribution. 2
1.3. Outline of the Thesis 5
1.4. Methodology, Data and Values of the Research. 5
1.4.1. Doctrinal Legal Research 5
1.4.2. Interviews as a Subsidiary Method of Research 7
1.4.3. Interdisciplinary Approaches 7
1.5. Theory and Project Background: Algorithmic Fairness for Asylum Seekers and Refugees 9
1.6. Scope of the Thesis 10
1.7. The Name of the Rose: Naming Biometric Law and Biometric Legal Concepts 11
1.7.1. Biometric Law: Justification and Systematisation of the New Concept 11
1.7.2. Biometric Legal Terminology 13
1.7.3. Concluding Remarks Regarding Biometric Terminology 27
Chapter 2: EU Biometric Lex Generalis 28
2.1. Introduction 28
2.2. Tracing the Development of EU Biometric Law 30
2.3. General Aspects of Processing Personal and Biometric Data 34
2.3.1. Principles of the GDPR in View of Biometric Data Processing 34
2.3.2. Individual Rights of the GDPR and Biometric Law 37

2.3.3. Automated Decision-Making and Profiling: Not Very Helpful to Data Subjects .. 38
2.3.4. Data Protection by Design and by Default 41
2.3.5. Data Protection Impact Assessment..... 42
2.4. Biometric Data: The Building Blocks of EU Biometric Law 44
2.4.1. The Element of Personal Data in the Definition of Biometric Data 46
2.4.2. Resulting from Specific Technical Processing 46
2.4.3. On Physical, Physiological or Behavioural Characteristics of Natural Persons 51
2.4.4. Genetic Data and Biometric Data: Different Purposes 54
2.4.5. Allowing or Confirming Unique Identification 57
2.4.6. The Crucial Debate: Are All Biometric Data Sensitive or Only Those of Article 9 GDPR? 60
2.4.7. Concluding Remarks on the Definition of Biometric Data 67
2.5. Processing of Biometric Data: The Rule or the Exception? 68
2.5.1. Explicit Consent for the Processing of Biometric Data 70
2.5.2. Biometric Data Manifestly Made Public as a Basis for Processing..... 72
2.5.3. Substantial Public Interest of Article 9(2)(g) GDPR 73
2.5.4. Article 9(4) GDPR: National Laws May Further Regulate the Processing of Biometric Data. 75
2.6. LED and EUDPR as Parts of EU General Biometric Law 77
2.6.1. The European Data Protection Regulation 77
2.6.2. Law Enforcement Directive and Processing of Biometric Data 78
2.7. The AI Act: Biometric Lex Specialis? 79
2.7.1. The AI System and Biometric Data as in the AI Act: Novelties in EU Biometric Law 80
2.7.2. The Biometric Categorisation System of the AI Act: A True Novelty in EU Biometric Law 83
2.7.3. An Emotion Recognition System: Another Type of Biometric Categorisation 85
2.7.4. Biometric Identification in the AI Act 86
2.7.5. A Real-Time Remote Biometric Identification System 87
2.7.6. The Relation of the AI Act to the GDPR and LED: Blink and You Will Miss It .. 90
2.7.7. How Does the AI Act Work: The Risk Pyramid 92
2.7.8. Prohibited AI Practices in the AI Act and Biometrics 94
2.8. The Council of Europe and Its Influence on EU Biometric Law 96
2.8.1. Convention 108: Influencing EU Biometric Law 96

2.8.2. The European Convention of Human Rights and the Case Law of Its Court: A Vital Inspiration for EU Biometric Law 99
2.9. Clearview AI: Theft in Broad Daylight 104
2.9.1 The Facts Concerning Clearview AI. 105
2.9.2. The Scope of the GDPR and Clearview AI Activities 106
2.9.3. Legitimate Interests and Reasonable Expectations 107
2.9.4. The Lessons of the Clearview AI Case 108
2.10. Worldcoin: Explicit Consent for Biometric Identification 110
Chapter 3: Biometric data in Migration and Asylum: Analysis of Biometric Law Through Case Law, Information Systems of the EU, and Interoperability 112
3.1. The Aim and the Structure of This Chapter 112
3.2. Biometric Case Law: CJEU Justifies the Use of Biometrics 113
3.2.1. Case C-291/12 *Schwarz* 114
3.2.2. Joined Cases C-446/12 to C-449/12 *Willems:* National Biometric Databases Are Allowed. 121
3.2.3. Case C-70/18 *A, B and P* 124
3.2.4. Case C-205/21 *Ministerstvo na vatreshnite raboti:* Processing of Biometric Data for Law Enforcement Purposes 129
3.2.5. Conditions for the Storage of Biometric Data in Police Records: Case C-118/22 *NG v Direktor na Glavna direktsia "Natsionalna politsia" pri Ministerstvo na vatreshnite raboti* 131
3.2.6. Case C-61/22 *RL v Wiesbaden:* Biometrics Reaffirmed as Justified 133
3.3. Biometric Parameters: Case Study of Eurodac as a Biometric System 142
3.3.1. The Methodology for the Analysis of Biometric Parameters 142
3.3.2. Eurodac as a Case Study of a Biometric System 144
3.3.3 Concluding Remarks 172
3.4. Interoperability and Biometric Templates as EU Biometric Law Phenomena 173
3.4.1. The Interoperability of EU Information Systems: The Impact on EU Biometric Law 174
3.4.2. Components of Interoperability 176
3.4.3. Biometric Templates in the sBMS: Storage of Biometric Data in Interoperable Form 182
3.4.4. Concluding Remarks on Interoperability and Biometric Templates 189
Chapter 4: Fundamental Rights Analysis of Biometrics Applied in Migration and Asylum 192
4.1. Aims, Methods, and Structure. 192

4.2. Privacy (and Data Protection) as the Main Arena of EU Biometric Law 193
4.2.1. Introduction 193
4.2.2. Privacy and Data Protection: Theory, Development and the Distinction Between the Two Rights 194
4.2.3. Justifying Limitations of Privacy in Four Steps: A Biometric Checklist That Failed 197
4.2.4. Conclusion on Privacy and Data Protection Analysis of Biometrics 205
4.3. Human Dignity and the Rule of the Thumb 207
4.3.1. The Eugenic History of Fingerprinting 207
4.3.2. The Concept of Human Dignity: A Link Between Morality and Law. 210
4.3.3. Human Dignity in EU Law: A Right and a Value under Threat. 213
4.3.4. Conclusion: Human Dignity is Not Properly Utilised but Remains an Important Check on Biometrics. 228
4.4. The Right to Non-Discrimination in EU Biometric Law: A Viable Route to Challenge Algorithmic Bias? 231
4.4.1. Structure of the Section and the Main Arguments 231
4.4.2. Understanding Algorithmic and Biometric Bias as Legal Phenomena 232
4.4.3. Algorithmic Bias in Legislation and Academic Writing 233
4.4.4. Theoretical Framework for Understanding Algorithmic Bias 236
4.4.5. The Three Arguments Against the Use of Non-Discrimination Legal Framework for Tackling Biometrics 240
4.4.6. Conclusion: How to Counter Algorithmic Bias 248
4.5. Conclusion to Chapter 4. 249
Chapter 5: Can Privacy Enhancing Tools Reduce the Limitations of Fundamental Rights Caused by the Use of Biometric Technologies in EU Migration and Asylum? . 251
5.1. Answering the Main Research Question: The Path Taken and the Light at the End .. 251
5.2. Remarks on the Scope of Investigation of Encryption and Three Examples on Benefits of Encryption 252
5.3. The Legal Framework for the Encryption of Biometric Data and Privacy Enhancing Tools 254
5.4. A Right to Encryption or an Obligation to Decrypt? 256
5.5. Podchasov: The Facts, the Decision, and the Consequences for Encryption. 258
5.6. The Quest for the Holy Grail: Legal Effects and Methods of Encryption. 262
5.6.1. Pseudonymisation and Anonymisation of Biometric Data 262
5.6.2. Irreversibility and Revocability: An Eye for an Eye 264

5.6.3. Two Promising Methods of Encryption of Biometric Data 266
5.7. Conclusion: Kerkhoff's Principle 269
Chapter 6: Conclusions and a Look to the Future. 271
6.1. Conclusions 271
6.2. A Look into the Future of Biometric Law 275
Bibliography and Other Sources Used in the Research 277
Bibliographic Sources 277
Legislation 285
Case Law 290
Other Sources 292
Note on Author and Published Works 303

Chapter 1: Introduction, Methodology, Research Questions and Biometric Terminology

1.1. Introduction: The Importance of Biometrics and the Reasoning Behind the Thesis

People rely on biometrics to unlock their phones, access banking services, or cross borders. The application of biometric technologies is rapidly growing. Biometrics are used by the private and public sector. This thesis focuses on legal issues raised by the use of biometric technologies in migration in the EU. Namely, the government has to provide public security, but on the other hand, there is an obligation to respect migrants' rights to privacy and other fundamental rights. Biometric technologies are at the heart of this conflict of public and private rights and interests.

The use of biometric technologies in migration is a controversial area, especially in the EU. When a migrant approaches an EU external border, they are immediately faced with an array of modern technologies. Drones and thermal cameras inspect the green (and blue) border, while designated border crossings are equipped with fingerprint and facial scanners. Depending on whether they are perceived as legal or as irregular, migrants might be subject to wearing ankle bracelets with GPS, having their phone searched and their phone data extracted and analysed, or at least submitted to different methods of biometric identification and verification. Biometric technology is used to capture unique and permanent human features, which sets biometric data apart from other personal data. For example, if one loses a passport, one can apply for a new one. But, if one's iris scan is stolen, it may not be possible to get a new pair of eyes. These features are part of the reasoning why biometrics justify a special, more stringent legal framework.

In the EU, biometric systems are being set up or upgraded. Eurodac will collect biometric images along with fingerprints of irregular migrants and asylum seekers. The Visa Information System, the Entry-Exit System and other systems collect biometric data of migrants. These systems are linked by what the EU calls "interoperability", meaning that data collected for different purposes, such as migration, asylum, or counter-terrorism purposes, can be cross-referenced and accessed by hundreds of designated national bodies of EU Member States and EU bodies. Of course, public authorities are restricted in their processing of the biometric data of individuals. But where exactly are the limits and how are these limits legally framed?

Biometrics are probably unstoppable because they have proven to be highly useful. The identification of persons has shifted from an evaluation of documents to an automatic evaluation of human physical properties. Because of the importance of biometrics for public authorities, it

is extremely unlikely that an approach to prohibit biometrics in principle (as being contrary to human or fundamental rights) would gain any traction. The cat is out of the bag, said one legal migration expert on this author's proposition to write a doctoral thesis on how to prevent the negative effects of biometrics. The cow is out of the barn, said another prominent academic upon hearing the research proposal that would develop into this thesis. Since one cannot "Stop all the clocks, cut off the telephone,/Prevent the dog from barking with a juicy bone",[1] what can be done to face these changes without biometrics representing a loss of fundamental rights for individuals? The author of this thesis thus early on decided that a realist approach is needed, one that would strive to improve the position of migrants within the sphere of what is possible. That is why the research is framed by the question of how privacy enhancing tools, such as encryption, contribute to the fundamental rights of migrants.

The personal interest in the topic of biometrics in EU migration can be traced back to the attendance of the fifth-year elective course EU Migration and Asylum Law, held by Prof. Iris Goldner Lang (who is now the supervisor of this doctoral thesis). Every student had to make a short presentation on a given topic, and this student chose to present on Eurodac – the European fingerprinting system for asylum seekers, perhaps because it was the last item on the list of prospective topics. The student presentation was, from a subjective perspective, a success. However, fingerprinting millions of migrants seemed a strange practice, and the author had at that time made a mental note that it would be most interesting to understand the rules which regulate this processing of fingerprint data. How are these modern technologies understood as legal phenomena, and how do they interact with fundamental rights which every person is entitled to, including irregular migrants? These would not become the research questions of this thesis but were the questions that inspired interest in the subject. After preliminary research into the topic of modern technologies and artificial intelligence used in EU migration and asylum, it quickly became clear that among the most prominent authors on this topic was Prof. Niovi Vavoula, particularly in relation to EU information systems. The author is thus most grateful to Prof. Vavoula for being the co-supervisor of this thesis.

1.2. Research Questions, Hypothesis and Scientific Contribution.

The main research question is whether encryption as a privacy enhancing tool could be used to mitigate the negative effects of biometric data processing on fundamental rights. The hypothesis associated with this main research question is that there are indeed a number of privacy

[1] "Stop All the Clocks", a poem by WH Auden.

enhancing tools, particularly encryption, developed in the sphere of cryptography and computer sciences, which can be repurposed as legal tools to enhance the fundamental rights of migrants. To repurpose would mean to set into legal rules the requirements to encrypt in view of the effects it can have on biometric data, such as pseudonymisation, anonymisation or revocability.

This hypothesis was reached after the preliminary research, which included conducting a literature review of both academic and scientific writing on the topic of biometrics, the associated legal effects and the technical tools for protecting biometric data. As previously explained, the idea behind this thesis was to adopt a realist approach that could stand a chance of being implemented and actually improve the fundamental rights of migrants. Encryption in particular seemed to represent low-hanging fruit in the sense that it promised to alleviate some of the most serious drawbacks of biometrics in terms of privacy. However, encryption seemed to be significantly unexplored as a legal phenomenon.

In order to test the main hypothesis, it was necessary to answer a number of subsidiary research questions, which correspond to the chapters of the thesis. First among these research questions was to determine the legal framework that applies to the use of biometric technologies in the sphere of EU migration law. The answer to this question led to a systematisation of rules relating to biometric technologies (Chapter 2). The next question was to determine the particular rules for applying biometric technologies in migration and asylum in the EU (Chapter 3). Chapter 4 examined what fundamental rights are affected by the use of biometric technologies, and how these rights are affected. Chapter 5 then provided an answer to the main research question, by determining the legal framework for the encryption of biometric data, the encryption methods that may be particularly useful and their effects on fundamental rights. Finally, a conclusion followed on whether or to what extent encryption can mitigate what was determined as negative effects on the fundamental rights of migrants and asylum seekers in the context of the application of biometric technologies.

The main research objective of the thesis is recommendatory in nature, meaning that the goal is to recommend how the law should be interpreted regarding the main research question. These subsidiary questions also had a descriptive element, in that the task was to systematise existing rules in order to be able to critically examine them. Finally, there is an evaluation element in the thesis, because a subsidiary research objective is to evaluate whether the current legal framework is sufficient for regulating biometric technologies in the sphere of migration.

The scientific contribution of this thesis has several aspects. There is significant value in the systematisation of rules of EU law which are applicable when biometric technologies are applied in the context of migration. The thesis achieves this systematisation, which can be of use for both researchers and practitioners and may be named as EU biometric law in migration and asylum. A further scientific contribution of this work lies in finding that the definition, or definitions, of biometric data as they stand in EU law are unclear and possibly contradictory. Both the legislation and the case law analysed in this thesis show that crucial stakeholders are not aware of the problems and the contradictions of the concept of biometric data. This thesis identifies the problem and proposes a correct interpretation, both in terms as they should be understood as the law stands, and in the ways that the definition of biometric data could be improved. Related to this, a further scientific contribution of this thesis lies in improving and enriching the legal vocabulary relating to biometrics. This is done by introducing certain crucial concepts for regulating biometrics. It should also be noted that the thesis has scientific value for Croatian legal science. Biometric law is studied in this thesis with a view to Croatian legislation concerning the processing of biometric data and migration. Furthermore, the author conducted a number of interviews with Croatian representatives and practitioners of data protection and information systems used for migration control. This gave an insight into the particular position of Croatian authorities both in terms of migration control and in terms of legal understanding of biometrics.

Further, the thesis resolves questions of the imprecise use of biometric terminology by EU legislation by detecting and advising on the use of terminology which is aligned with technical biometric vocabulary. The scientific contribution of the thesis is also evident in the conceptualisation and critical analysis of the case law on biometrics. These cases are recognised as forming an evolution in the understanding of biometrics by both the CJEU and the ECtHR. Nevertheless, the case law is criticised on points where the approach, particularly that of the CJEU, should be more stringent towards the use of biometric in view of fundamental rights. Future legal research may benefit from the presented factors that are crucial for a fundamental rights analysis of biometrics. Finally, a particularly important scientific contribution of this thesis is to interpret technical phenomena, such as the encryption of biometric data, through the legal effects these tools have on fundamental rights. An attempt is made to bridge the gap between the technical and legal understanding of biometrics, and thus to use existing technical tools for the better protection of the fundamental rights of migrants.

1.3. Outline of the Thesis

This thesis is made up of six chapters. Chapter 1 contains the introduction, which explains the importance of the topic and the reasons for choosing this area of legal research, the main and subsidiary research questions and the hypothesis, the outline of the thesis, the methodology, a note on the theoretical framework of the AFAR project, and a comment on the scope of the thesis. The final part of the introductory chapter is devoted to definitions of biometric law, which will be used in the rest of the thesis.

Chapter 2 represents a systematisation of rules which pertain to the use of biometric technologies in the sphere of EU law by creating a new legal concept, namely EU biometric law. This chapter contains a critical analysis of the definition of biometric data, which is a key concept in biometric law. Chapter 3 is a more detailed analysis of biometric law in the particular setting of migration and asylum. It includes an analysis of the EU biometric information system Eurodac, interoperability and the meaning of biometric templates, as well as an analysis of the CJEU's case law which combines issues of biometrics and migration.

Chapter 4 provides a fundamental rights analysis of biometrics in three main parts. First, there is a critical analysis of the fundamental rights to privacy and data protection in view of biometrics, followed by an examination of the issue of human dignity in the study of forced fingerprinting for Eurodac, and ending with a fundamental rights analysis of facial recognition and non-discrimination. Chapter 5 is an analysis of privacy enhancing solutions that could limit the effects of biometrics on the fundamental rights and data protection rights of migrants. Consideration is given to the technical solutions for the protection of biometric templates which could be adopted and enforced as legal standards, with a view to the effects they have on the pseudonymity and anonymity of data. Chapter 6 draws the conclusion of the thesis.

1.4. Methodology, Data and Values of the Research.

1.4.1. Doctrinal Legal Research

This section briefly outlines the methodology used for this thesis, including methodological approaches, research data and research methods. First of all, the thesis primarily uses the method of legal doctrinal research. This can be justified since the research questions are of a legal nature, the main method is the interpretation of texts, and the main objective is normative

in character. This distinguishes legal research from the social or natural sciences.[2] The approach in this thesis to studying the law, and case law in particular, is well described by Olsen and Byrne who hold that doctrinal scholarship is a dynamic relationship between theory and practice that does not recite judicial decisions but examines them drawing on law's own logical and functional criteria.[3]

Since the thesis is predominantly legal doctrinal research, the research methods are those of legal science. The main method is the interpretation of legal texts and case law. This includes textual interpretation, where the literal text is interpreted; contextual interpretation, which examines the relation of the legal text to the system it belongs to as well as the motivations that made the text as it is; and teleological interpretation, which interprets the text by considering its purpose.[4] The case law concerns primarily that of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

Research data includes predominately legal sources such as EU primary and secondary law, including the Charter of Fundamental Rights (which contains relevant fundamental rights provisions of the right to privacy, data protection and non-discrimination), regulations such as the Eurodac regulation;[5] and the GDPR. The case law of the CJEU on biometrics is analysed in detail. The thesis analyses the law of the Council of Europe, particularly Article 8 ECHR. Additionally, in the area of biometrics and law, soft law plays an important role. For example, the research will rely on recommendations, the opinions of the European Data Protection Board and the European Data Protection Supervisor, NGO reports, and communications and reports from the EU Commission and parliament on biometrics. Technical standards (ISO and similar)[6] are also important as they set the vocabulary and technical standards for biometrics. The methods employed for collecting data involve desk research, namely exploring case-law databases (CURIA, HUDOC, the FRA Case Law database, GDPR Hub) the EU law database

[2] Mark Van Hoecke, "Legal Doctrine: Which Method(s) for What Kind of Discipline?" In Mark van Hoecke (ed), *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* (Hart Publishing, 2011) 1–18.
[3] WH Byrne & HP Olsen (2024). "Doctrinal Legal Science: A Science of Its Own? (pp. 1–25). University of Copenhagen. MOBILE Working Paper Series No. 36, 10.
[4] Koen Lenaerts, Jose Gutierrez Fons, "To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice" (EUI AEL 2013/09, Distinguished Lectures of the Academy).
[5] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints [2013] OJ L180/1.
[6] See biometric standards developed by the biometric working group at ISO: ISO/IEC JTC 1/SC 37 https://www.iso.org/committee/313770.html.

EUR-Lex, and also databases containing academic literature, such as ScienceDirect or HeinOnline.

1.4.2. Interviews as a Subsidiary Method of Research

The research for this thesis also involved conducting a number of semi-structured interviews with experts. Interviews were conducted with representatives of the Ministry of Interior of Croatia who are operating various parts of Eurodac or the Schengen Information System, along with an interview with the representative of the Croatian Agency for the Protection of Personal Data (AZOP). The purpose of these interviews was to gain insight into specific questions of how biometric information systems at the level of a Member State operate, and whether migrants and asylum seekers may exercise their rights. In short, the intention was to acquire knowledge which cannot be discerned from reading the specific perspectives of public authorities and practitioners that use the biometric systems or are entrusted with data protection. Interviews were in a semi-structured form, meaning that questions were provided in advance, but the answers did not have to strictly adhere to the questions. Information on the rights of persons being interviewed was provided. The Ethical Committee of the Faculty of Law of Zagreb approved the interviews, in terms of the methods of the interview and the persons being interviewed. The persons in question were experts and the interviews did not engage with migrants, asylum seekers or other vulnerable groups.

1.4.3. Interdisciplinary Approaches

Although the thesis has certain elements of interdisciplinarity, drawing on certain other disciplines, it remains predominantly doctrinal research in the area of law. The methodological framework for the question of the interdisciplinarity of the thesis is provided by a paper by Van Klink and Taekema.[7] Interdisciplinarity stems from the fact that biometrics are a technical as much as a legal phenomenon. Technical developments in the field of biometrics have legal implications. For example, if biometric algorithms used for facial recognition are not accurate, they might distinguish darker faces with less precision than lighter faces and consequently cause legal discrimination. Thus, it is at points necessary to delve into technical aspects of biometrics

[7] Bart van Klink, Hester Sanne Taekema, "On the Border: Limits and Possibilities of Interdisciplinary Research" in Bart van Klink, Hester Sanne Taekema (eds), *Law and Method: Interdisciplinary Research into Law* (Mohr Siebeck, 2011) 7–32.

to answer legal research questions. This dissertation can be considered to involve two levels of interdisciplinary research, as outlined below.

First, heuristic research, as some questions are inspired by texts of other sciences, namely legal philosophy and political science, which are used for policy and philosophical insights into the issue of biometrics in EU migration. In this sense, the philosophical underpinning of biometrics can be understood by association with "biopolitics", conceptually established by Michel Foucault,[8] to explain how authorities implement measures to control the biological aspects of the population. Giorgio Agamben connects biopolitics with the state of exception found in the works of Carl Schmitt.[9] According to Agamben, since the turn of the century and terrorist shocks, the state of exception has grown to a justification for the permanent reduction of individual privacy on account of the imperative of public security. This seems to correspond to the question of why new biometric technologies are being introduced by States and how they are justified. Ultimately, this philosophical framework and the cited literature were used in the thesis only indirectly. Nevertheless, the mentioned works have been influential for the author in his understanding of the material sources of law, that is, the powers that shaped the (biometric) legal system.

Secondly, the thesis involves auxiliary interdisciplinarity, which represents a higher level of research which utilises multiple approaches. This is because the findings of computer science are used to answer legal research questions ("is there algorithmic discrimination with facial biometric recognition, or how does encryption technically achieve the pseudonymisation of biometric data?"). In this regard, associated with the AFAR project, Prof. Kostanjčar of the Faculty of Electrical Engineering and Computing in Zagreb provided interpretations of certain academic papers which required mathematical or computer science knowledge. Finally, the fundamental value that this dissertation is based on is human dignity. The research presented in this thesis should not be used in a manner that would be harmful to the rights of migrants and asylum seekers.

[8] Michel Foucault, *Rođenje biopolitike* (Sandorf i Mizantrop, 2016).
[9] Giorgio Agamben, *Homo sacer: Suverena moć i goli život* (Multimedijalni institut, 2006).

1.5. Theory and Project Background: Algorithmic Fairness for Asylum Seekers and Refugees

This thesis is written as part of the international project AFAR: Algorithmic Fairness for Asylum Seekers and Refugees, a project funded by the Volkswagen Foundation and involving researchers based in Berlin, Copenhagen, Florence, Oxford and Zagreb.[10] The AFAR project focuses on different concepts of fairness and the examination of modern technologies (newtech) in migration and asylum. Within the AFAR project framework, this legal dissertation can be understood as a contribution to the understanding of individual fairness.

The AFAR project understands fairness as a normative legal and empirical concept with three dimensions. First is individual fairness, which concerns migration and asylum subjects. Distributive fairness captures fairness in relation to different States or other communities concerning migration and asylum governance (MAG). Thirdly, perceptions of fairness concern how fairness is viewed amongst the public and MAG subjects themselves. This thesis primarily explores individual fairness, expressed as a human and fundamental rights analysis of the effects of biometrics on individuals. Furthermore, the thesis provides original legal research on points of non-discrimination and facial recognition, where different aspects of fairness are examined, in particular the trade-offs between fairness and accuracy.[11] Biometric technologies raise issues of automated decision making (ADM) by public authorities, as is analysed in this thesis,[12] which further connects it to the main goals of the AFAR project. The main method, as stated, is doctrinal legal research which explores normative (legal) sources.

[10] AFAR project website, https://www.hertie-school.org/en/research/research-directory/afar.
[11] See 4.4.3 and 4.4.5.3 of the thesis.
[12] See 2.3.3 of the thesis.

1.6. Scope of the Thesis

This thesis has a defined, limited scope in terms of the law and technologies. In its legal scope, the thesis examines primarily EU law. The analysis at points expands to include issues of the national law of Member States when this is necessary to understand the applicability of EU law. The law of the Council of Europe, namely the ECHR, is also included in this thesis, because it is influential for the development of EU (biometric) law, as will be further explained.[13] In terms of EU law, the use of biometrics examined in this thesis can be positioned largely within the Area of Freedom, Security and Justice,[14] which includes, in particular, policies on border checks, asylum and immigration, but is also interwoven with the Common Foreign and Security Policy of the EU and Member States. Finally, the fundamental rights that are most important for studying the legal implications of biometric technologies are privacy (along with data protection) and the right to non-discrimination. According to EU primary law, everyone has a right to data protection,[15] and third country nationals have a right to international protection, which includes the right to asylum and the principle of *non-refoulement*,[16] which is particularly relevant to the study conducted in this thesis.

Biometrics have a wide range of applications. However, in this thesis, the focus is on the use of biometrics by public authorities, and not the private sector, even though there are significant similarities and generalisations which can be made concerning the rules applicable to any application of biometrics. This is why, even though the thesis considers rules for the use of biometrics by public authorities on individuals, particularly in the context of asylum and migration, it is unavoidable that certain generalised rules can be deduced, which apply to any application of biometrics in the EU. The technological scope of the study includes biometric technologies, particularly fingerprinting, but also facial recognition, iris recognition, and DNA biometrics.

[13] See in particular 2.8 of the thesis.
[14] Article 3(2) TEU and Title V TFEU.
[15] Article 16 TFEU.
[16] Article 78 TFEU; Articles 18 and 19 CFR.

1.7. The Name of the Rose: Naming Biometric Law and Biometric Legal Concepts

This section comments on the biometrics terminology that will be used throughout the thesis. The concept of biometric law will be explained. This will be followed by an elucidation of how biometrics operate. Thirdly, a basic vocabulary for describing legal biometric concepts will be provided.

1.7.1. Biometric Law: Justification and Systematisation of the New Concept

Biometric law is a novel concept developed in this thesis. It is based on the idea that it is important to systematise EU rules concerning biometrics and recognise this as a new area of law, further providing a critical analysis to recognise legal gaps or ambiguities. The idea originally developed in this thesis is to systematise EU legal norms concerning biometrics into a new area under the name biometric law. There are several good reasons for recognising biometric law as a novel and useful concept. First, the use of biometrics is growing astonishingly. Biometrics are vital for transactions online and for confirming identity when using a mobile phone. Public authorities have also embraced biometrics to verify the identity of travellers, to interact with citizens and to fight crime. Increased use of biometrics in the everyday practice of state authorities can produce a legal vacuum that will be filled either by interpreting existing rules or by creating new ones. Biometric law reflects both these tendencies.

Another reason for "biometric law" is that there are already a number of provisions that deal specifically with biometrics, mostly embedded in broader data protection or law enforcement acts. There is, primarily, the definition of biometric data. The General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) regulate the processing of biometric data. Since the processing of biometric data is a limitation of the fundamental rights of privacy and data protection, the Charter of Fundamental Rights of the European Union (CFR) and the procedure of justifying limitations of fundamental rights are essential elements of biometric law. Further, the Artificial Intelligence Act (hereinafter: AI Act)[17] regulates surveillance, biometric categorisation, identification, and verification. These components

[17] 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 - AI Act) [2024] OJ L2024/1689.

provide the bones of the general part of EU biometric law, which is applicable to most of the application of biometrics.

EU biometric databases, such as Eurodac, have their own specific legislation that regulates biometric data in a narrower context. All these provisions, taken together, make up a distinguishable area of EU law concerning biometrics. There is also EU secondary legislation on specific aspects of applying biometrics – in the passports and IDs of EU citizens, or for the registration of irregular migrants or asylum seekers. EU biometric law is not complete without the provisions of the ECHR and the case law of ECtHR, which has played an influential role in defining the relationship between biometrics and human privacy. The CJEU case law on biometrics is not substantial in terms of numbers of cases, but it is vital for interpretation, and is growing. Finally, one must consider national laws which often interact with EU provisions on biometrics.

Biometric law is to a large extent a specific subset of data protection law. However, it has special characteristics, found, for example, in its distinct legal concept of biometric data, and in other characteristics which delineate biometric law from other areas of data protection law. Biometric law should not be fully equated to the processing of biometric data. Biometric categorisation is one example of a biometric application that does not concern the processing of biometric data, but personal data. There are other borderline examples or ambiguous interpretations of the meaning of biometric data for which biometric law can be considered a broader concept than what is encompassed by the processing of biometric data. Other specifics of biometric law are the importance of technical sciences such as facial recognition, AI, and cryptography.

The first goal of recognising biometric law as a separate legal area or topic is to tie it more closely with fundamental rights, in particular the rights to privacy, data protection and non-discrimination. This raises the question of whether biometric law needs to be changed and how it should be changed. The second goal is to clarify the legal terminology related to biometrics. As biometrics become more prominent, the vocabulary that describes various related aspects is growing. In many instances, the terminology used in EU law is still inadequate. This thesis will track the development of the terminology and try to provide improvements.

1.7.2. Biometric Legal Terminology

Biometrics is derived from the Greek words *bios* (life) and *metron* (measure). More interestingly, the word itself was coined in the 19th century among scientists who wanted to scientifically prove racial differences. Biometrics thus shares uncomfortable origins with the more notorious eugenics.[18] Biometrics is the automated recognition of individuals based on their biological and behavioural characteristics[19] and is synonymous with biometric recognition.[20] Thus, biometrics is an umbrella term for any kind of technology, such as fingerprint or facial recognition, that uses human traits to identify or verify the identity of a person. Besides identification and verification, there is a third mode in which biometrics are used, biometric categorisation.

The question of terminology is among the key issues concerning biometrics and law. To grasp the process, the technical challenges and the legal issues, there must be clarity in the meaning of the basic terms of biometrics. Even the word "biometrics" has been conflated with biometric data[21] and biometrics has sometimes been wrongly understood as the face or the finger that provides the biological source for the operation of biometric systems instead of the name of the process. For example, a 2013 report concerning Council of Europe (CoE) Convention 108 provides the following introductory definition: "Biometric data (or biometrics) are measurable, physiological or behavioural characteristics that can be used to determine or verify identity".[22] This definition manages to conflate biometrics, biometric data and biometric characteristics as one and the same. It is therefore important to clarify the concept of biometrics. However, the sophistication of legal-biometric vocabulary is growing. This might lead to excessive complexity in legal terminology, as seen in the recommendations made by the European Data Protection Board (EDPB) from a report analysing the legal aspects of biometrics:

> Implement safeguards during enrolment phase to ensure bootstrapping enrolment process with a verified identity. For example, to reinforce the assessment of users'

[18] For more on this, see Chapter 4.

[19] ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics.

[20] ibid.

[21] As explained further in the first part of this chapter; C.A. Jasserand, "Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective" (2016) 6(1) International Data Privacy Law, https://doi.org/10.1093/idpl/ipv020, 66-67.

[22] Council of Europe, Consultative Committee of the Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No. 108] (Strasbourg 2013) T-PD(2013)06 https://rm.coe.int/consultative-committe-of-the-convention-for-the-protection-of-individu/16806945c7.

identities multifactor authentication, steps can be implemented, ranging from password protected one-time links to activate the app, to local device unblocking mechanisms.[23]

However, even in this 2024 document, authentication and verification are still being used interchangeably. It nevertheless shows that the need to ensure data protection and privacy in the context of modern technologies such as biometrics requires more sophisticated vocabulary.

1.7.2.1. Biometric Recognition: Identification and Verification

Biometric recognition encompasses biometric verification and biometric identification.[24] This is a crucial division for understanding biometrics. Verification and identification present vastly different legal challenges. Simply put, verification is the process of comparing one-on-one the identity of a certain person. Biometric identification is comparing one set of biometric data against biometric data in a database, a one-against-many comparison.

Biometric recognition works by comparing two sets of data. Biometric comparison (a less formal term is "matching") is an assessment of the similarity between a biometric probe and a biometric reference.[25] A person's identity is verified by using data collected from the person's fingerprint (biometric probe) against the fingerprint data already stored in a document (biometric reference), or in a remote database. There is no practical difference between fingerprint data or facial image data at the point of comparison. Any kind of biometric characteristic is "translated" into a biometric template that is then compared.

An example of biometric verification is when a person at a border crossing presents their passport and where the biometric data in the passport are compared to the photograph of the person taken by the camera at a border crossing. Verification, in plain terms, means comparing a facial image of an individual captured, for example, at an airport with the biometric data stored in the passport of that individual. Verification is thus comparing two sets of biometric data to answer the question whether these are the same (if they are, this leads to the conclusion that

[23] European Data protection Board (EDPB), Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024) https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en.

[24] Note 3, International Organization for Standardization, ISO/IEC 2382-37:2022(en)37.05.07 Information technology — Vocabulary — Part 37: Biometrics, www.iso.org.

[25] ISO/IEC 2382-37:2022(en).

both originate from the same person. Thus, the person presenting the passport is the same as the person shown in the passport).

Biometric identification is another type of biometric recognition. It means searching one-to-many and involves a biometric database. There are many biometric databases (also known as large-scale information systems) at the level of the EU, such as Eurodac, the Schengen Information System and the Visa Information System. Additionally, there are also national databases that contain biometric data for specific categories of persons such as persons convicted of serious crimes. Biometric identification involves a comparison of many, sometimes millions of, biometric templates with data stored outside the control of the individual.

In principle, there are greater security and privacy concerns connected with biometric identification than with biometric verification. Nevertheless, both biometric verification and identification require careful legal and technical consideration since they involve the personal and sensitive data of natural persons. It must be noted that the difference between biometric verification and identification is not definite. As analysed by Sumer, verification can work with a one-to-many comparison, and the lines between identification and verification may be "blurry".[26] The author of this thesis nevertheless understands the distinction as follows: verification checks whether the person is who they claim to be. Identification goes one step further by checking all available biometric templates against the claim.

Biometric identification presumes comparing biometric data (more specifically, a biometric template) of one person against a large amount of other data in a database. When an irregular migrant is apprehended, their fingerprints are recorded and then compared against the fingerprint data in the Eurodac database which contains recorded fingerprint data of millions of individuals. The question posed by biometric identification is thus: is this person's biometric data already recorded in a database?[27] Identification is more intrusive than verification because it requires the storage of biometric data in a database. Verification *can* be done with data being stored only locally on a passport. The GDPR uses the term allowing or confirming unique

[26] B Sumer, "The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?" (2024) 10 European Data Protection Law Review 150 https://doi.org/10.21552/edpl/2024/2/6, 153–154.
[27] Even if this database contains only one biometric template, so effectively may represent a 1:1 comparison, as pedantically pointed out by B Sumer, "The AI Act's Exclusion of Biometric Verification" (cited above) 153.

identification to mean both identification and verification.[28] This includes biometric identification and verification and excludes biometric categorisation. Article 3(35) of the Artificial Intelligence Act defines "biometric identification" as "the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database".

Even if the distinction between verification and identification is not simple, there is a significant difference, in legal terms, between a fingerprint image stored locally, on a passport, and a fingerprint image that is stored remotely from the person, for example in a national database of convicted criminals or of asylum seekers. This storage of biometric data opens up many legal questions that are referred to in regulations, case law and soft law. Whose data can be (remotely) stored, for how long, when can these data be accessed and by whom? These issues are addressed in this thesis.[29] In legal terms, these questions crucially affect the assessment of the impact of the processing of biometric data on data protection, privacy and other rights, particularly in the context of a proportionality analysis, which is a requisite in EU law in the context of processing biometric data, but also in the ECHR. Identification should always be compared to verification.

The mentioned ISO standard defines biometric recognition with greater precision but also adding further complexity. Thus, biometric verification is the "process of confirming a biometric claim through comparison".[30] A biometric claim is a statement that a biometric capture subject is or is not the bodily source of a specified or unspecified biometric reference.[31] In contrast, biometric identification is the "process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual".[32] the AI Act confusingly refers to biometric verification as including authentication in multiples places.[33]

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 General Data Protection Regulation [2016] OJ L119 (GDPR), Article 4(14).
[29] See 3.3 of this thesis.
[30] ISO/IEC 2382-37:2022(en).
[31] ibid.
[32] ibid.
[33] Regulation (EU) 2024/1689, Article 3(36).

1.7.2.2. Biometric Categorisation: Odd Man Out

As this thesis has developed, it has become clear that categorisation is among the key concepts in understanding biometrics, at the same time illustrating the technical and legal limits of such understanding. Biometric categorisation is not defined in ISO/IEC Biometric Vocabulary since it does not involve the automated recognition of individuals. Biometric recognition only includes verification and identification.[34] Nevertheless, biometric categorisation does involve the use of biometric technologies such as facial recognition. Biometric categorisation is the processing of individual human characteristics to categorise these persons in certain groups.

Thus, biometric categorisation can be defined as applying biometric technologies to certain unique human features to sort persons into categories, but without uniquely defining any individual. For example, biometrics can categorise people according to their skin colour, gender, or age. Biometric categorisation can be understood even more broadly, for the categorisation of persons under any criteria – whether they are (regularly) breathing, whether or not they are under the influence of alcohol, and similar examples. Biometric categorisation tools are used in the context of border control. Heartbeat sensors are used to determine whether there are migrants hiding under lorries crossing a border.[35] In these cases, the person is not uniquely identified, nor is their identity verified. But there is a processing of a certain human characteristic to gain information; in other words there is a processing of personal data.

Biometric categorisation features in the AI Act and in EU soft law documents.[36] From a legal perspective, two clear types can be delineated. One involves categorising persons by their race or ethnicity, their health status and other categories which are defined in Article 9 GDPR as concerning sensitive personal data. This kind of biometric categorisation, involving the processing of sensitive data, is regulated in the same way as the processing of biometric data. This is because such categorisation is based on the sensitive data listed in Article 9 GDPR. Other types of biometric categorisation that do not involve the processing of sensitive data would be regulated as the processing of "ordinary" personal data. Examples of this non-sensitive categorisation include the mentioned heartbeat sensors in border control, or biometric

[34] Note 3 ISO/IEC 2382-37:2022(en).

[35] See the company booklet explaining how heartbeat sensors are used to detect persons in lorries or near critical infrastructure: "Science for Humanity: Human Presence, Movement & Heartbeat Detection System (MDS)" https://s4h.be/wp-content/uploads/2020/12/Science-for-Humanity-Frontex-booklet.pdf.

[36] See e.g. A29WP, "Opinion 3/2012 on Developments in Biometric Technologies" (2012) 00720/12/EN WP193; A29WP, "Opinion 2/2012 on facial recognition in online and mobile services" (2012) 00727/12/EN WP 192, Regulation (EU) 2024/1689.

categorisation tools, or the biometric categorisation of persons based on their hair style in the context of camera filters. These examples can be considered biometric categorisation because they rely on certain human properties, but not amounting to identification or verification, and thus would not concern the processing of biometric data. Nevertheless, heartbeat sensors do use human, biological properties (the heart pulse) and concern information about identifiable persons (that they are in a certain place) so they do represent the processing of personal data. This "ordinary" biometric categorisation should be regulated as the processing of ordinary, or non-sensitive, personal data.

The AI Act defines biometric categorisation as assigning natural persons to specific categories based on their biometric data.[37] This is an unusual definition because it means that biometric categorisation is the result of the processing of only specifically biometric data. Biometric data has a specific, narrow meaning in EU law, as mentioned, and as will be further analysed. In an elegant and concise definition, the AI Act then adds that this definition of biometric categorisation does not include biometric categorisation systems which are "purely ancillary" to another commercial service, such as facial filters on online marketplaces.[38] The AI Act also states that biometric data include identification, verification, and categorisation of natural persons, even adding a fourth category of biometric data: emotion recognition systems.[39] As stated later in the thesis, emotion recognition should be understood as a type of biometric categorisation.

Another taxonomy of biometrics that is often mentioned is the difference between soft and hard biometrics. Soft biometrics concern those human characteristics which are not unique and therefore do not result in unique identification.[40] One example of soft biometrics would be emotion recognition. The author of this thesis notes that soft biometrics is the same as biometric categorisation, while hard biometrics would concern identification and verification. The opinion of the author is that the dichotomy of soft and hard biometrics in not necessary if one has in mind the meaning of biometric categorisation.

[37] AI Act, Recital 16 and Article 3(40).
[38] See part 2.9.2.2 of this thesis on biometric categorisation in the AI Act.
[39] See part 2.9.2.3 on emotion recognition.
[40] A Kak, "Introduction" in A Kak (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions* (AI Now Institute, 1 September 2020) 6.

1.7.2.3. Use of ISO/IEC Biometric Vocabulary

This thesis will rely on the definitions of biometrics and related concepts as devised in the ISO/IEC community, in particular, the standard 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics.[41] ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) together form the system for worldwide standardisation. ISO has published tens of thousands of international standards and has hundreds of expert committees developing these standards.[42]

The reason for choosing ISO/IEC standardisation in this thesis as a reference is that ISO is the accepted international standardisation body, covering also biometrics standards. Prominent international scholars devise these standards precisely for the purpose of providing an international biometric "language". ISO/IEC terminology is used by scholars examining the technical aspects of biometrics, but also by legal scholars.[43] ISO/IEC technical standards are at least indirectly embedded in EU law as well. For example, the EU Passport Regulation states that travel documents must comply with International Civil Aviation Organization (ICAO) standards, in particular ICAO 9303,[44] while the said ICAO 9303 states that ISO endorses it.[45]

ISO is referred to as the standard setting body in multiple areas of biometrics. eu-LISA, the organisation responsible for maintaining EU information systems, contributes to the ISO subcommittee on biometrics.[46] EDPB extensively referred to ISO/IEC biometrics vocabulary in its recent opinion on the use of facial recognition at airports.[47] Another important standard-setting body is the National Institute for Standards and Technology (NIST), which, for example, sets the standards for the data format for the interchange of fingerprint data as stipulated in the

[41] International Organization for Standardization, ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics www.iso.org.
[42] International Organisation for Standardization, About ISO, https://www.iso.org/about.
[43] E.g. C Jasserand, "Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective" (2016) 6(1) International Data Privacy Law, https://doi.org/10.1093/idpl/ipv020.
[44] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1, Recital 3 and Annex.
[45] International Civil Aviation Organization (ICAO), Doc 9303, Machine Readable Travel Documents Part 1 — Introduction ISBN 978-92-9265-291-3, https://www.icao.int/publications/Documents/9303_p1_cons_en.pdf.
[46] eu-LISA Single Programming Document 2024–2026, 61.
[47] A3.1. European Data Protection Board (EDPB), Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024) https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en.

Eurodac Regulation.[48] NIST is a US government body which is highly influential thanks to its extensive testing of modern technologies, such as biometric algorithms.[49] ISO/IEC biometric vocabulary provides important definitions that should, in the opinion of this author, be used as a reference when discussing biometrics in the legal community. "Automatic", as in automatic recognition, implies that a machine system is used either fully or with human assistance.[50] Individual means it is applied only to individual humans.[51] However, some biometric categorisation systems may apply to groups of individuals. This is another point by which categorisation differs from identification and verification.

1.7.2.4. Biometric Data

Biometric data are a key concept in biometric law. Paradoxically, the current legal definition is unclear.[52] Biometric data are a biometric sample or aggregation of biometric samples at any stage of processing.[53] A biometric sample is, for example, a photograph of a face or the recorded image of a fingertip.[54] It is important to note that biometric data as defined in ISO as any biometric sample is a much broader definition of biometric data than the one used in EU law. As will be pointed out, this creates problems because the legal concept of biometric data excludes data that from a technical standpoint are biometric data. But there are strong reasons for the definition of biometric data in EU (biometric) law to have a more limited scope than the technical concept of biometric data as found in ISO/IEC. EU soft law instruments recognise biometric samples, characteristics, and templates as separate concepts.[55]

Biometric data are special. This type of data is intimately linked with an individual, from whose characteristics it is derived. In a sense, biometric data are the uniqueness of a human translated into a digital code. Biometric data can be opposed to alphanumeric or biographical data. There is no intrinsic or biological connection between biographic data and a person. Names are often misspelled, changed, or wrongly transcribed. Date of birth and place of residence may be shared

[48] Annex I Regulation (EU) 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" (Eurodac regulation).
[49] NIST (National Institute of Standards and Technology), "Face Technology Evaluations - FRTE/FATE", https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate.
[50] Note 4 37.01.03 ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics.
[51] Note 1 ISO/IEC 2382-37:2022(en).
[52] See 2.2.3.
[53] ISO/IEC 2382-37:2022(en).
[54] ibid.
[55] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (2022) https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en.

among millions. Declared nationality and ethnicity may also be unreliable or subjective. Biometric data are more dependable. Unique whorls and ridges on a finger (biometric characteristics recorded as biometric samples) become a proxy for the identity of a person. This is why it is the fingerprint data that are currently kept in the EU database of asylum seekers and irregular migrants – the Eurodac, and not the name of the person.[56] Biometrics have thus become crucial for public authorities to establish or verify the identity of a person, or to find out their biological properties. If in the current world the most valuable resource is (digital) information, biometric data are the most valuable kind, being unique and sometimes irreplaceable. This means biometric data should also be protected in the most rigorous manner, using technical and legal tools.

1.7.2.5. Biometric Characteristics and the Biometric Template

The biological or behavioural characteristics of individuals such as the topography of a face or the ridges of a finger are biometric characteristics.[57] Another important concept is the biometric template, which is the subject of Chapter 3 given its prominence in EU biometric information systems.[58] ISO defines a biometric template as a set of stored biometric features comparable directly to a biometric probe and gives an example of a record containing a set of finger *minutiae*.[59] Putting these concepts into context, biometric recognition involves recording the biometric characteristic as a biometric sample. This biometric sample is further transformed into a biometric template, which is the digital extract of the biometric characteristic that is stored for comparison.[60] This means that from a finger, a fingerprint is extracted. The finger is a biometric characteristic; the fingerprint is a biometric sample. An algorithm that makes a comparison does not necessarily use all the details of a biometric sample. It may need to record certain key points of the fingerprint or to store a picture of a certain pixel density. Therefore, a simplistic diagram of the process of biometric identification would show: (biometric) characteristic to sample to template.[61] The AI Act still conflates the biometric characteristic

[56] Regulation (EU) 603/2013, Article 11.
[57] ISO/IEC 2382-37:2022(en).
[58] See 3.4.3.
[59] ISO/IEC 2382-37:2022(en).
[60] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes" [Thesis fully internal (DIV), University of Groningen] (2019) University of Groningen, 66.
[61] This template can be vastly reduced and incomprehensible to a human. So, a crucial legal question has emerged: is a biometric template legally speaking personal data (or biometric data)? It is not simply a doctrinal debate, but a question of importance for millions of people whose biometric data will be collected and stored as biometric templates in EU information systems. If biometric templates are not personal data, but simply a meaningless string of zeroes and ones, the data protection framework does not apply. Just to anticipate a more detailed analysis of the

with biometric data, as it mentions that examples of biometric data are the face of a person or a person's fingerprint.[62]

Article 29 Working Party (A29WP) Opinion 3/2012 on biometrics did not properly define biometrics or biometric data, but extensively discussed the legal nature of biometric templates. The Working Paper was faced with the same dilemma that is still relevant today. A biometric template is the reduction of a biometric sample so that it contains only the information needed to conduct a biometric comparison. The biometric template is the information that is stored, often in a database, and therefore the question of the legal nature of the biometric template is crucial for regulating biometrics. If the biometric template is not considered to be biometric data (or personal data) then such information can be stored without invoking the personal data legal framework. But how can a biometric template not be personal data if the purpose of the template is precisely to identify a person, given that personal data are information relating to an identified or at least identifiable individual?[63] The Working Paper states that a biometric template in most cases is indeed personal data.[64] However, it states that templates might not be personal data if "no reasonable means can be used by the controller or by any other person to identify the data subject".[65] The question was thus left open. The biometric template as an EU legal concept will be analysed in a later part of this thesis.

1.7.2.6. Accuracy of a Biometric System

An important aspect of biometrics is accuracy. Biometrics are considered accurate and trustworthy. This perception may be influenced by machine bias – where humans uncritically accept the decisions made by a machine. In practice, it is hard to imagine that a decision-maker would question a deoxyribonucleic acid (DNA) analysis or fingerprint recognition results. However, no technology is absolutely accurate, and this applies to all biometrics as well. EU

question of the nature of biometric template in EU information systems (in the sBMS), a parallel can be drawn with the beginning of DNA analysis when public authorities started to collect and store DNA, claiming that it is not personal data because apparent strings of AGTC that make each person's DNA is unreadable gibberish, without, that is, the use of additional tools, such as computers. With these additional tools, a unique AGTC string can actually tell us quite a lot about a person.

[62] Regulation (EU) 2024/1689, Recital 30.

[63] Regulation (EU) 2016/679, Article 4(1); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Data Protection Directive - DPD), Article 2(a).

[64] A29WP, "Working Document on Biometrics" (2003) WP 80, 5.

[65] ibid, footnote 11.

authorities may overestimate the accuracy of biometrics.[66] One in twenty persons may not be able to be enrolled, for example, because of problems with their fingerprints, while in about one percent of cases a facial recognition system will produce a false negative result, meaning that the person will not be recognised even though he or she should have been.[67] Today, fingerprints and facial images are generally accurate, and mistakes are usually the result of problems at the enrolment phase, for example if the finger was not properly pressed against the scanner or if the facial image was captured in inadequate lighting conditions.[68]

It is important to note the term "enrolment" which can be found in EU soft law,[69] but also in secondary legislation.[70] For the purpose of assessing the performance of the Entry Exit System (EES), the "Failure to Enrol Rate" (FTER) examines the quality of enrolment. FTER means the proportion of registrations that were of insufficient quality for the biometric system to work. Enrolment means the first registration of biometric data. It is when a person's biometric data are enrolled in a system (or stored in a database). These enrolment data are then used for future comparison. EES means that the first time a third country national wants to enter the EU, they must step in front of a camera and hold still for a short time (enrolment of data). These data are then used for future comparison. FTER represents a margin of failure (due, for example, to poor lightning conditions, damaged fingertips, or unsteady movement in front of the camera) that caused errors in recording the biometric data. Naturally, a robust biometric system should have an FTER as low as possible, and a high FTER would signify that there are problems: either with the hardware of the system, the software, or with some aspects of the practicalities of the procedure.

For biometric verification, there is a "false matching rate". This is the "proportion of impostor attempts that are falsely declared to match a template of another object (a person's biometric template)".[71] In the context of biometrics and more broadly cybersecurity, when someone acts

---

[66] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022), 79.

[67] EDPS (European Data Protection Supervisor), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System (VIS) and the Exchange of Data Between Member States on Short Stay-Visas (COM (2004)835 final), 3.4.3.

[68] P Grother, M Ngan and K Hanaoka, "Face Recognition Vendor Test Part 3: Demographic Effects" (19 December 2019) NIST publication, 54 https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[69] European Data Protection Board (EDPB), Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024).

[70] Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES) C/2019/1280 OJ L 57 (EES Implementing Decision 2019/329).

[71] EES Implementing Decision 2019/329.

as an impostor or tries to commit fraud, it is called spoofing. Spoofing methods can range from putting on a fake nose and glasses to trick facial recognition, to more sophisticated kinds of fraud. On the other hand, the false nonmatching rate "is the proportion of genuine attempts that are falsely declared not to match a template of the same object".[72] These are simply other names for false positives and false negatives. False positives are occurrences when a system incorrectly makes a conclusion that biometric data in, for example, a passport match the biometric data taken at the airport of the person holding the passport. The person appearing does not actually match the person in the documents, but the system makes the mistake of showing that they do There can be other situations related to false positives; for example, an honest traveller is mistakenly identified as being on a terrorist watchlist. The other kind of error is false negatives. In this instance, the system mistakenly states that there is no recognition in a comparison, while in fact there should be. A person truthfully presenting documents is not recognised or a migrant is mistakenly taken from the queue for a further check.

The mentioned EES decision prescribes that biometric systems must reach a defined level of accuracy. For example, the maximum value of false nonmatching rates must be lower than 1 percent.[73] This means that an EES biometric system must not make the mistake of not matching a genuine person with a genuine passport more than once in one hundred times. Considering the many millions of people will be using EES, this level of accuracy is far from impressive.

Concepts of accuracy, false positives and negatives are not the only relevant aspects. They can serve to assess discrimination if, for example, a biometric system works less accurately with female or Black faces. If a biometric system is of low accuracy, it could also be argued that the system is a disproportionate and unjustified infringement of rights to privacy and data protection. In this case, the limitation of privacy and data protection caused by the processing of biometric data is not justified because it is not suitable or proportionate in the strict sense of the proportionality test. However, the levels of accuracy or of error rates that are universally unacceptable are not defined.

1.7.2.7. Different Biometric Technologies & the Importance of System Architecture

Biometrics mostly concern either fingerprint recognition or facial recognition. Fingerprint recognition as a biometric technology appeared as early as the 19th century. Fingerprints were

[72] 1.2 EES Implementing Decision 2019/329.
[73] 1.2.2 EES Implementing Decision 2019/329.

manually and visually inspected and compared. This means that before the age of computers, there had to be an archive containing countless fingerprints and these would have to be manually compared against a fingerprint collected from a suspect or obtained from a crime scene (the latter known as a latent fingerprint). The human "quirk" that enabled fingerprint recognition is that the fingerprints of each human are unique. Moreover, not only are they unique but fingerprints can be easily recorded. Even better, these records can now be processed and compared automatically by machines. Machines (or modern computers) simply look at patterns created by an algorithm, so that there is no difference on how facial recognition or fingerprint recognition work. The point is that biometrics enable public authorities to answer the questions "who is this person" or "has this person been here before" or "is this person telling the truth" by supplanting these questions with the mathematical operation of comparing the data derived from a person's fingertips.

Besides fingerprint recognition, especially important is facial recognition. This is an automated recognition of individuals based on their facial features. Facial recognition in the modern sense depends on computers and has grown in use with the development of the latest AI technologies. As with fingerprints, what is compared is simply a code that is derived from a facial image. There are countless facial recognition algorithms which in diverse ways process the facial image into data. One can broadly distinguish two-dimensional from three-dimensional facial recognition. These algorithms differ in their performance (accuracy or in demographic bias).

There are many other, prominent, biometric technologies. Each has its own peculiarities. For example, there is evidence that iris recognition would be more efficient in terms of the storage required than fingerprints.[74] Another prominent biometric technology is DNA profiling. This technology is used particularly in the context of law enforcement.

The number and type of biometric technologies is not a closed list. Every so often a new human characteristic is discovered that may be unique in each individual and thus potentially used for biometric recognition. Whether a biometric technology is adopted depends on a number of factors: how economic and how fast it can perform, how accurate it is, and how it is perceived by the public. Examples of biometric technologies considered by Frontex for the purpose of

[74] C Busch, "Biometric Data Interchange Standards and ICAO 9303 Relevance" presentation, https://www.christoph-busch.de/files/Busch-ICAO-39794-NFIQ2-210419.pdf, Part 6 of presentation: "At only 2,000 bytes, iris images are now much more compact than fingerprints".

border security include eye or hand vein recognition, gait recognition, and many others.[75] Voice biometrics, more precisely accent recognition, is used in the asylum procedure in Germany. The purpose is to assess the veracity of a person's claimed origin by checking their accent (variation of Arabic).[76] If one applies the nomenclature of biometrics developed in this thesis, one can conclude that such voice biometrics are an example of biometric categorisation. This is because such a system can only categorise persons by their accent (with a certain level of accuracy) and not by itself to uniquely identify them from their speech. This may make such a system less legally onerous to apply because biometric categorisation involves not the processing of biometric data, but of personal data.

Understanding an algorithm is not sufficient to assess the legal effects of biometrics. Particularly important are issues of the duration of storage, the security of biometric data, and the general system architecture.[77] For example, the Croatian Automated System for Biometric Identification (ABIS) is an integrated system that connects five collections of biometric data: the National Information System for Border Management (NISUDG), the Penal and Probationary Information System (ZPIS), the Criminal Evidentiary, the Croatian Visa Information System (HVIS), and the National EURODAC System.[78] ABIS is connected to multiple large scale information systems of the EU. Namely, it is connected to the Schengen Information System (SIS), the Visa Information System (VIS), EURODAC, the European Criminal Records Information System for Third Country Nationals (ECRIS-TCN), the EES and European Travel Information and Authorisation System (ETIAS, which does not collect biometric data), as well as the Europol Information System (EIS) and the Interpol Information System (IIS).[79] Therefore, biometrics do not merely raise legal issues concerning how biometric data are collected. Equally important for individual rights are questions on how the data are stored, how, when and with whom they are shared, and how they are protected against abuse. Answers to these questions determine the legality of processing biometric data and thus also make up EU biometric law.

---

[75] Frontex, Technology Foresight on Biometrics for the Future of Travel (European Border and Coast Guard Agency, 2022), www.frontex.europa.eu.

[76] For an overview of modern technologies used in the asylum procedures in the EU, see D Ozkul, "Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe" 2023 University of Oxford, Refugee Studies Centre.

[77] See 3.3.2 of the thesis, on the parameters of a biometric system using the example of Eurodac.

[78] Article 4 Pravilnik o obradi biometrijskih podataka NN 122/2020 (Croatian Ordinance on the processing of biometrics data). Croatian legislation translated into English here is by the author of the thesis.

[79] Article 5, Croatian Ordinance on the processing of biometrics data.

1.7.3. Concluding Remarks Regarding Biometric Terminology

The following recommendations can be made on the use of proper legal terminology for biometrics. ISO/IEC biometric vocabulary should be used to describe legal biometric concepts. As both the implementation of biometrics and the legal understanding of biometrics grow, there should be a conscious effort to keep biometric vocabulary in line with technical understanding. Secondly, authentication should be dropped as a term signifying biometric verification. Even in the recent AI Act, both authentication and verification are used inconsistently to describe the same phenomenon. This should be changed. Most complex issues concern the status of biometric categorisation and the definition of biometric data. Biometric categorisation is not biometric recognition, but it nevertheless collects personal and often sensitive data, in most cases by using highly sophisticated technologies. Categorisation features prominently in the AI Act as well, which shows that the EU legislator is trying to treat these types of biometric practices in a due legal manner. How categorisation should be treated falls to the definition of biometric data. If this definition refers only to verification and identification, then categorisation is excluded. This is a policy choice. This will be discussed in Part 2.4 of thesis where the definition of biometric data is scrutinised in detail.

Chapter 2: EU Biometric Lex Generalis

2.1. Introduction

This chapter offers a systematisation and critical analysis of EU general biometric law. EU biometric law can be divided into the general part, which applies to the processing of biometric data, and special biometric law, which comprises the rules on biometrics concerning migration and asylum applications. Biometric general law is made up of EU law (the GDPR, its law enforcement cousin LED,[80] EUDPR[81], and CFR) and Council of Europe law (Convention 108, ECHR, and the case law of the ECtHR). Biometric migration law consists of biometric-specific secondary legislation (such as the Eurodac regulation), which will be the subject of Chapter 3. National laws of EU Member States can be considered as part of biometric law, general or migration specific, when EU legislation explicitly refers to national legislation.

EU data protection legislation is based on the act of processing certain information, not on the outcome or the technology used. Biometric data are a type of personal data with a few peculiarities. Even though biometrics have become increasingly important, the regulation of biometrics still depends on the interpretation of a small number of norms enacted more than a decade ago and often originate from the understanding of biometrics goes back thirty or more years. Biometric data are the essential legal concept for regulating biometrics in the EU.[82] Depending on the specifics, biometrics may entail the processing of either personal data or more specifically biometric data. At least in theory, it is also possible for biometric data (understood in the technical sense) to be encrypted so that the information is anonymised. Thus, in principle, biometrics may concern the processing of personal data, of biometric data, or may not trigger the data protection legal framework at all. Nevertheless, most biometric applications concern the processing of biometric data.

Biometric law not only concerns the definition of biometric data but also issues of the correct legal basis of processing, and the application of the data protection framework, such as GDPR

[80] 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 [2016] OJ L119/89 (Law Enforcement Directive - LED).

[81] 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 L295/39 (European Data Protection Regulation - EUDPR).

[82] Defined in Article 4(14) Regulation (EU) 2016/679 as well as in Article 3(13) Directive (EU) 2016/680.

principles as well as fundamental rights safeguards contained in the CFR. The LED and EUDPD mostly mirror the provisions of the GDPR in respect of biometric data, so these will not be scrutinised at the same level of detail to avoid repetition. However, several important cases resolved before the CJEU in recent years have concerned biometrics and law enforcement, thus the LED and its case law are significant in biometric law. Finally, the AI Act has introduced a completely new dynamic to the topic of regulating biometrics.[83] Even though it does not have the same scope or purpose as the GDPR, it deals with biometrics extensively, mentioning "biometric" more than a hundred times in its text. It also devotes many pages to explicitly defining biometric categorisation, identification and verification.

Chapter 2 is a significant part of this thesis because it explains some of the crucial concepts of applicable EU biometric law, not limited to the application of biometrics in EU migration and asylum law. The chapter is structured as follows. First, there is a short overview of the development of biometric legal concepts in EU law which predates the GDPR, but which in parts is still relevant. Second, the chapter examines general aspects of the data protection legal framework in view of biometrics, namely the principles of the GDPR, individual rights, the concept of automated decision-making and biometrics, the principles of data protection by design, and finally the requirement of the data protection impact assessment, also in relation to biometrics. The following section offers a detailed critical analysis of the concept of biometric data. Every element of the definition is examined. This includes exploring the meaning of "specific technical processing", biometric characteristics, the difference between genetic and biometric data, and the difference between allowing or confirming identification. This is followed by a presentation of the arguments of the crucial debate on how many definitions of biometric data exist in the GDPR, which determines the requirements for the processing of biometric data. The conditions for processing are then scrutinised, particularly the conditions of explicit consent for processing and the substantial public interest therein. Next, the Law Enforcement Directive and the European Data Protection Regulation are examined in view of their differences when compared to the GDPR. After this, the AI Act is analysed in view of its abundant definitions relating to biometrics, including the concept of biometric categorisation, and how the unusual concept of biometric data in the AI Act interacts with the same concept in the GDPR. This is followed by a short overview of the effects of the Council of Europe on the development of EU biometric law, through Convention 108, the ECHR, and the particularly

[83] Regulation (EU) 2024/1689.

influential case law of the ECtHR. Finally, two real-world examples of biometric applications are examined. The case of Clearview AI shows how the rules of the GDPR prevent the practice of data scraping to create facial recognition (biometric) databases. The unusual case of Worldcoin shows how even explicit consent for biometric data processing might not be enough to make such processing conform to EU (biometric) law.

2.2. Tracing the Development of EU Biometric Law

This section gives a concise overview of the development of the regulation of biometrics in the EU. Certain key legislative choices have facilitated the proliferation of biometric technologies. The approach to biometric data which prevailed has also compelling arguments in its favour as well as negative sides. However, the view that allowed the less restrictive processing of biometric data prevailed. This permissive approach to biometric data, or more broadly to biometrics, started to form well before the GDPR came into existence. Historically, two general trends can be seen. The first is a permissive approach which favours the extensive application of biometrics. The second is the growing use and understanding of biometrics and of biometric terminology in EU law.

The first EU legal interpretative documents concerning biometrics did not precisely define biometric data.[84] Other concepts related to biometrics were similarly misunderstood or not defined. At the beginning of the legal framing of biometrics (the first decade of the 21st century) there was a low level of understanding of biometrics in EU legislation. Later development was characterised by defining the concept of biometric data until the coming into force of the GDPR. Biometric data as a legal term was understood quite differently (more narrowly) from the meaning of biometric data in the technical sense. The GDPR and LED made these understandings of biometrics in interpretative documents binding law. The situation in practice has markedly changed since the GDPR came into force. New biometric technologies have proliferated. Border control has become unimaginable without biometrics. AI has transformed biometrics and facial recognition. New EU information systems are being set up which will use fingerprint and facial recognition. These biometric systems will relate to a shared biometric infrastructure, making them interoperable. Upcoming new legislation will transform "biometric law" in the EU and thus will mark a new phase in the development of legislation on biometrics.

[84] For example, A29WP, "Working Document on Biometrics" (2003) WP 80 states: "It appears that biometric data can always be considered as 'information relating to a natural person'(...)" 5.

Directive 95/46/EC (Data Protection Directive, DPD)[85] was the predecessor of Regulation (EU) 2016/679 (further in text: GDPR). The DPD did not contain any specific reference to biometrics. However, its enduring significance for the regulation of biometrics lay in Article 29 DPD. The Article established the Working Party on the Protection of Individuals regarding the Processing of Personal Data (Article 29 Working Party - A29WP). This advisory body produced many documents in the form of opinions and recommendations. Some of these documents addressed the question of biometric regulation. Many of the conclusions are still relevant.[86]

In 2003, A29WP issued a Working Document on Biometrics. It discussed the application of the then existing data protection rules on biometrics.[87] This report is among the first documents by EU bodies to discuss the regulation of biometrics, but it did not provide clear criteria to relate biometric data to personal data.[88] Neither were the terms "biometrics" nor "biometric data" defined in this Working Document on Biometrics, even though both terms were used throughout. There was no differentiation between biometric data and biometric characteristics. Further, "biometrics" was used synonymously with "biometric data".[89] Biometric data were confused with biometric samples ("image of the fingerprint, picture of the iris or of the retina, recording of the voice").[90] This Working Document wavered between authentication and verification, using the expression "authentication/verification" throughout. Using the term "authentication" in place of "verification" has prevailed in subsequent documents and has continued even up to the present provisions of the GDPR.[91] ISO vocabulary on biometrics considers the term authentication to be a deprecated expression for biometric recognition.[92] The A29WP paper concludes that authentication/verification, in which biometric data are not centrally stored, raises fewer risks for the protection of fundamental rights and freedoms of the individual.[93] This position is still widely accepted, which has led to the legal distinction between

[85] Directive 95/46/EC.

[86] With the coming into force of GDPR, A29WP was replaced by the European Data Protection Board (EDPB). See Article 68 Regulation (EU) 2016/679.

[87] A29WP, "Working Document on Biometrics' (2003) WP 80".

[88] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes (Thesis fully internal (DIV), University of Groningen) (2019) University of Groningen, 63.

[89] See also C Jasserand, "Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective" (2016) 6(1) International Data Privacy Law, 66, https://doi.org/10.1093/idpl/ipv020.

[90] A29WP, "Working Document on Biometrics" (2003) WP 80, 4.

[91] Regulation (EU) 2016/679, Recital 51.

[92] 37.01.03 note 6 ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics.

[93] A29WP, "Working Document on Biometrics" (2003) WP 80, 6.

biometric verification and identification, reflected in Articles 4(14) and 9(1) GDPR. The subsequent 2007 A29WP Opinion defines biometric data as:

> biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.[94]

This is a much broader definition than the one that will take shape in GDPR. The term biometric data is still not differentiated from biometric characteristics, as "Typical examples of such biometric data are provided by fingerprints, retinal patterns, facial structure, voices(...)".[95] Nevertheless, Opinion 4/2007 in a different place attempts to specify the difference between the terms by stating that "human tissue samples (like a blood sample) are themselves sources out of which biometric data are extracted, but they are not biometric data themselves (as for instance a pattern for fingerprints is biometric data, but the finger itself is not)".[96] This shows a movement towards a more precise understanding of biometric data that was fuelled by practical developments in forensics. In this 2007 definition of biometric data, there is no reference to the way the information must be processed ("specific technical processing") or the purpose of processing ("which allow or confirm the unique identification") later found in the GDPR.

The Commission's GDPR Proposal of 2012 is revealingly different in comparison to the GDPR that was finally adopted, in terms of how it defines biometric data. The 2012 GDPR Proposal defines biometric data as any data relating to the physical, physiological, or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopy data.[97] This definition is also markedly different from and more accurate than the previous attempts at defining biometric data in the A29WP documents. It refers to the data gathered from biometric characteristics, instead of mixing up biometric characteristics and biometric data, as was the case in A29WP documents. On the other hand, this definition of biometric data in the GDPR 2012 Proposal is also simpler than the one that was finally adopted in the GDPR. It does not include the requirement of "specific technical processing" nor the

[94] A29WP, "Opinion 4/2007 on the concept of personal data" (2007) 01248/07/EN WP 136, 8.

[95] ibid.

[96] ibid.

[97] Article 4(11) European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final 2012/0011 (COD) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52012PC0011.

purpose of "authentication or identification". The GDPR 2012 Proposal included a definition of biometric data, but unlike the final text, did not include biometric data (for the purpose of unique identification) among special categories of personal data.

These final elements were proposed during the negotiations in the adoption of the GDPR.[98] In essence, the Council succeeded in adding elements so that there is a distinction between the general definition of biometric data and biometric data as sensitive data. This transplant from the Convention 108 modernisation reports was not successful because it led to a lack of clarity of the different definitions of biometric data in the GDPR.

However, the GDPR 2012 Proposal specified that personal data in large-scale filing systems on children, genetic data or biometric data trigger data protection impact assessment.[99] In the final text of the GDPR, however, the provision on the data protection impact assessment was reorganised and any mention of biometric data was removed.[100] This shows that even at the stage of the 2012 GDPR Proposal, there was awareness that biometric data are associated with a specific, higher risk for natural persons. In the adopted GDPR text, biometric data were added to special categories of personal data at the behest of the European Parliament. The requirement of "specific technical processing" of the Article 4 definition of biometric data was laid down by the Council.[101]

After this brief historical overview of the development of biometric data in EU law, what follows is the current legal framework concerning biometric data processing.

[98] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) Interinstitutional File: 2012/0011(COD) 2014 https://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf.

[99] Article 33(2)(d) Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) Interinstitutional File: 2012/0011(COD) 2014

[100] Article 33 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) Interinstitutional File: 2012/0011(COD) 2014; Article 35 Regulation (EU) 2016/679.

[101] C Kuner et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 209, ISBN 978–0–19–882649–1.

2.3. General Aspects of Processing Personal and Biometric Data

What follows is an overview of how the GDPR applies to the processing of biometric data, notwithstanding the issues of the definition of biometric data and the legal basis for processing, which will be analysed in the subsequent sections.

2.3.1. Principles of the GDPR in View of Biometric Data Processing

The principles of the GDPR constitute an important part of the EU data protection framework.[102] By extension, the GDPR principles are a constituent part of EU biometric law. Any processing of personal data must comply with these principles, primarily the principles of lawfulness, fairness, and transparency. The principle of lawfulness is expounded in Article 6 GDPR which enumerates the legal grounds for the lawfulness of processing personal data. For processing to be lawful, it must rely on a legal ground in Article 6 GDPR. In the case of processing biometric data, Article 9 provides exceptional legal bases which must be adhered to in order to satisfy the principle of lawfulness. Fairness of processing means that data subjects understand the extent of their personal data which is being processed.[103] Transparency is also reflected in the duty to inform data subjects (Articles 12 to 15 GDPR).[104] The principles of fairness and transparency also require that data subjects are informed of the existence of processing and its purpose.[105] It is difficult for a natural person to comprehend the manner and the extent to which their biometric data are processed in the context of modern technologies. The lack of awareness about the existence of processing and its purpose might thus be used as an argument against the processing of biometric data by AI tools that process biometric data in novel, unexpected ways. This point will be examined using the example of the Clearview AI case.

Second, the purpose limitation principle means that data must be processed for specified, explicit and legitimate purposes but should not be used further than that.[106] There is a certain overlap between this principle and the lawfulness of processing biometric data. For example, a

[102] Directive (EU) 2016/680 contains principles relating to processing of personal data within its scope in Article 4, and Regulation (EU) 2018/1725 likewise in its Article 4.
[103] Regulation (EU) 2016/679, Recital 39.
[104] See 2.9 of the thesis.
[105] Regulation (EU) 2016/679, Recital 60.
[106] A29WP, "Opinion 03/2013 on purpose limitation" (2013) 00569/13/EN WP 203, 11-12.

purpose contrary to the law goes against the purpose limitation principle.[107] Article 6(3) specifies the purposes of processing and how these may be changed subsequently. The LED allows the repurposing of personal data for law enforcement even if those data were initially collected for another purpose.[108] The GDPR contains stricter conditions for such a change of the purpose of processing personal data.[109] The principle of purpose limitation is also reflected in Article 4(1)(b) of LED. It is also expressed in Article 8(2) CFR, which prescribes that personal data must be processed for a specified purpose.

Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed, according to the data minimisation principle.[110] In relation to biometrics, the importance of this principle is clear. Data minimisation requires that only the minimum (biometric) data needed for establishing or verifying identity are processed. The developers of biometric technologies should have this legal obligation in mind when designing biometric recognition systems, because it may be difficult to adjust them after deployment. The data minimisation principle may be particularly relevant in the context of the interoperability of EU large-scale biometric systems where it may pose a limitation to how much data can be stored to achieve the prescribed purpose of the information systems.

The principle of accuracy requires that personal data is kept up to date and that every reasonable step is taken to rectify or erase inaccurate personal data.[111] This principle can be connected to the rights of data subjects to rectification and erasure.[112] Accuracy in the context of biometrics, particularly for facial recognition, should require that training datasets are large and representative of the population to which biometric recognition will be applied.[113] The principle of accuracy should also be understood to mean the requirement of good technical conditions, in particular lighting, which determines the accuracy of biometric recognition more than demographic factors.

---

[107] C Kuner et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 315.
[108] Directive (EU) 2016/680, Article 4(2).
[109] Regulation (EU) 2016/679, Article 6(3).
[110] ibid, Article 5(1)(c).
[111] ibid, Article 6(1)(d).
[112] ibid, Articles 16 and 17.
[113] Fundamental Rights Agency (FRA), "Facial recognition technology: fundamental rights considerations in the context of law enforcement" (2019), 10, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf .

The principle of storage limitation is vital for assessing the effects of biometrics on natural persons. The storage of biometric data is linked to biometric identification. The principle of storage limitation in particular means that there need to be clear time limits for storing personal data,[114] which includes fingerprint or facial image data. The integrity and confidentiality principles refer to using appropriate safeguards for personal data, as well as organisational and technical measures. This principle provides a strong basis for stipulating security features in biometrics, including encryption, which will be the focus of the final chapter of this thesis.

The accountability principle is the final principle stipulated in Article 5 GDPR. It refers to the responsibility of the controller to demonstrate compliance with the data protection framework. The principle of accountability is developed in Article 24 and 25 GDPR, concerning the controller's responsibilities and data protection by design and by default, respectively.[115] A good example of the application of the principles in the context of biometric data is the decision of the Greek DPA in the case of Clearview AI, which is analysed further in this chapter. Here it can be stressed that concerning their approach to Clearview AI practices, the French DPA focused on specific rights in the GDPR, while the Greek DPA additionally raised the matter that Clearview AI infringed the GDPR principles by, for example, not informing natural persons of their rights or by not respecting the reasonable expectations that natural persons may have in relation to the processing of their biometric data.[116] The GDPR principles are broad and are open to interpretation, which may make them flexible to implement but may also create uncertainty for controllers. For example, it is hard to predict in advance the satisfactory level of explanation that should be extended to a data subject about how exactly their biometric data are processed. It may thus be challenging for data controller to fully honour the principle of lawfulness, fairness, and transparency at the point of boarding a plane, when facial recognition may be applied, without causing traffic paralysis. Nevertheless, biometric law could well be approached from the perspective of the GDPR principles. In this sense, some of the most important legal issues raised by biometrics are framed among the principles. For example, the legal basis for the use of biometrics is enshrined in the principle of lawfulness. The purpose limitation and the accuracy and security of personal data nevertheless reflect some of the pressing issues of biometrics.

---

[114] C Kuner et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 318.
[115] ibid, 311.
[116] See 2.9 of the thesis.

2.3.2. Individual Rights of the GDPR and Biometric Law

The EU data protection legal framework specifies individual rights for data subjects (which can be viewed as natural persons and migrants in the context of this thesis). These rights include: the right to information;[117] the right to access one's own data;[118] the right to rectification of inaccurate data;[119] the right to the erasure of one's personal data;[120] the right to restrict the processing of personal data;[121] the right to data portability;[122] the right to object to the processing of personal data in certain circumstances.[123] For example, data subjects have the right to be informed of the identity and contact details of the controller, as well as about the retention of their personal data, the right to access and to rectification. However, the LED contains exceptions for these obligations of controllers in the context of law enforcement. Article 13(3) LED provides that data subjects do not have the right to be informed if this would result in obstructing or prejudicing ongoing investigations or if it would be detrimental to public security and national security.

Among the most relevant in the context of biometrics is the right not to be subject to a decision based solely on automated processing, including profiling, but this right is severely limited by the remainder of Article 22 and further by Article 23 GDPR. Furthermore, restrictions to the rights of data subjects are numerous, not only under the LED but also under the GDPR (Article 23). Rights can thus be curtailed if this restriction is based on law, respects the essence of fundamental rights, is a necessary and proportionate measure in a democratic society and is used to safeguard many of the listed grounds in Article 23 GDPR, including national security, public security, defence or crime investigation. These numerous restrictions to rights of data subjects are problematic, particularly in the context of biometric data.[124] Finally, also important are the right to lodge a complaint with a supervisory authority (Article 77 GDPR), the right to an effective judicial remedy (Article 78 GDPR) and the right to compensation from the controller (Article 82 GDPR).

---

[117] Regulation (EU) 2016/679, Articles 13 and 14; Directive (EU) 2016/680, Article 13
[118] Regulation (EU) 2016/679, Article 15; Directive (EU) 2016/680, Articles 14 and 15.
[119] Regulation (EU) 2016/679, Article 16; Directive (EU) 2016/680, Article 16.
[120] Regulation (EU) 2016/679, Article 17; Directive (EU) 2016/680, Article 16.
[121] Regulation (EU) 2016/679, Article 18; Directive (EU) 2016/680, Article 16.
[122] Regulation (EU) 2016/679, Article 20.
[123] ibid, Article 21.
[124] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020) 66.

2.3.3. Automated Decision-Making and Profiling: Not Very Helpful to Data Subjects

Data subjects have the right to object to automated decision-making (ADM), including profiling, and the right not to be subject to an automated decision or to profiling.[125] A data protection impact assessment is necessary in the case of ADM and profiling.[126] Biometric identification and biometric verification systems are included in automated decision-making systems.[127]

Article 22 GDPR and Article 11 LED prohibit decisions based solely on the automated processing of personal data. This concept of ADM includes profiling. There is an important exception to this prohibition in Article 22(2)(b). When it is authorised by Union or Member State law, with appropriate safeguards for the rights and freedoms of the data subject, then the prohibition concerning automated decision-making is not applicable. Additionally, the controller has to implement measures to safeguard the data subject's rights, freedoms and legitimate interests, "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision".[128] Generally put, human intervention is envisaged in EU large-scale biometric systems. A positive biometric comparison will result in human intervention, usually by a qualified police officer who would examine the results manually.[129]

In simple terms, ADM is allowed if based on a law that does not infringe human rights, which is a very general condition to impose on a law. Article 22 GDPR continues with a complex structure: 22(1) prohibits ADM, while 22(2) contains exceptions to this prohibition (making ADM allowed in those circumstances). There are stipulated rights for data subjects even if ADM is allowed (Article 22(3) GDPR), namely the right to human intervention, to express his or her point of view regarding ADM and to contest such a decision. Article 22(4) states that automated decision-making based on *special categories of personal data* is not allowed, despite the exceptions of Article 22(2). Article 22(4) finally allows ADM even if based on such sensitive data if it concerns the processing of biometric data on legal bases under Article 9(2)(a)

[125] Regulation (EU) 2016/679, Article 21(1); Regulation (EU) 2016/679, Article 22.
[126] Regulation (EU) 2016/679, Article 35(3)(a).
[127] Y Yang and others, "Automated Decision-Making and Artificial Intelligence at European Borders and Their Risks for Human Rights" (*arXiv.org*, 8 October 2024) https://arxiv.org/abs/2410.17278.
[128] Regulation (EU) 2016/679, Article 22(3).
[129] Zakon o obradi biometrijskih podataka NN 127/19 (the Croatian Act on the Processing of Biometric Data) stipulates that biometric data are compared in an automatic process with biometric data in relevant databases. Article 19 states that in certain cases, the results are verified by a person trained for assessing biometric data.

to (g) (themselves exceptions to the prohibitions of processing of biometric data), which covers the most important applications of biometrics. As with Article 9 GDPR, when the exceptions and prohibitions are neatly cancelled out, ADM based on the processing of biometric data is permitted for most applications of biometrics.

The AI Act is unfortunately structured in an equivalent manner. It stipulates that when so-called high-risk AI systems are used for identification, no decision or action should be taken "unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority".[130] But the article then continues that the two-person requirement does not apply to AI systems "used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate".[131]

The A29WP Guidelines on Automated Individual Decision-making and Profiling provide guidance on the meaning of a decision having legal effects. This implies that the automated decision affects the legal rights, legal status, or contractual obligations of data subjects.[132] An example of such a decision would be that a natural person is denied the right to board a plane because of the result of biometric identification. Similar examples of biometric ADM could include starting a criminal investigation based on the results of biometric identification, or of being denied international protection due to the results of biometric recognition. What is more, even if there are no legal effects, in the case of "significant" effects, the decision should be considered based solely on automated processing.[133] "Solely" means without meaningful human intervention. This does not provide much concrete guidance. In explaining the meaning of automated decision-making, the judgment of the CJEU in *Schufa* is relevant.[134] The case concerned a German company that provided a creditworthiness score using an automatic algorithm that had a pronounced effect on the ability of a person to, for example, rent an apartment. In its judgment, the Court settled on a "highly context-dependent approach in interpreting 'solely automated decision'."[135] Schufa was using ADM, the Court established,

[130] Regulation (EU) 2024/1689, Article 14(5).
[131] ibid, Article 14(5).
[132] A29WP, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (2018) 17/EN WP251rev.01.
[133] A29WP, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" (2018) 17/EN WP251rev.01, 21.
[134] Case C-634/21 *Schufa Holding* ECLI:EU:C:2023:957.
[135] F Palmiotto, "When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis" (2024) 25(2) German Law Journal, 210-236, doi:10.1017/glj.2023.112.

because automated scoring played a determining role in Schufa. But what makes a role a determining role is, of course, "highly" context dependent. In other words, there are no precise criteria to decide when a decision-making process is ADM. Biometric recognition is doubtless an automatic process. Whether it results in automated decision-making depends on the circumstances, such as whether there are persons checking the results of biometric recognition and how often these persons effectively question the decision of the machines. But given the extensive carve-outs for the use of biometrics in both the GDPR and AI Act, particularly concerning the application of biometrics by public authorities, the fact that biometric recognition may qualify as ADM has little overall effect.

Profiling is a subcategory of automated decision-making by which personal data is used to evaluate personal aspects concerning a natural person, particularly that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[136] At first glance, biometric recognition is not about "evaluating" certain aspects of a person, but making precise determinations. On the other hand, if one considers biometric categorisation, it is precisely about evaluating (more precisely sorting) human characteristics. Therefore, biometrics more broadly may represent profiling.

Profiling and ADM require disclosing "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".[137] As will be shown, Clearview AI practised the collection and analysis of facial images (from photographs), but also additional data such as where the image was taken (so-called geolocation data). Both the French CNIL and the Greek DPA considered that this practice of Clearview AI constituted profiling in the sense of the GDPR.[138] Therefore, the practice of the DPAs shows that biometric identification should be considered as profiling.

Could the legislator use the concept of automated processing, instead of specific technical processing, as the latter is used in the definition of biometric data? In that case, coupled with the insight from analysing the concept of personal data, the definition of biometric data could be that it is personal data whereby persons are identified (not merely identifiable) by automated means. This definition would be more succinct and would not need to rely on concepts that are

[136] Regulation 2016/679, Article 4(4).

[137] ibid, Article 13(2)(f); 14(2)(g); 15(1)(h).

[138] Hellenic Data Protection Authority (HDPA), Decision 35/2022 Ref. No. 1809, 12; Commission nationale de l'Informatique et des Libertés (CNIL) Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI, point 34.

otherwise unknown in the GDPR, such as specific technical processing. Nevertheless, it is not clear whether other elements of the definition of biometric data, besides specific technical processing, could be removed. The definition of biometric data is analysed in greater detail later in this Chapter.

2.3.4. Data Protection by Design and by Default

The concept of privacy by design that influenced the GDPR legislators can be pinpointed to a 1995 paper by a team formed around Ann Cavoukian who was for a while an official in Canada dealing with privacy matters.[139] Privacy by Design (PbD) is founded on seven principles. The most interesting ones from the perspective of biometrics are privacy as the default setting, which means that the individual does not have to make any choices to increase the privacy setting, because maximum privacy is already the default position. The end-to-end security principle implies that privacy must be extended through the whole cycle of a process, meaning that not only processing, but also storage and deletion should be considered together.

The critique of PbD is obvious. It may appear too vague for developers to practically implement as it effectively asks for a legal mindset to interpret a principle in the context of technical development.[140] This may feel burdensome and unclear to IT experts developing a system. But it should not be unclear to controllers, and especially to public authorities which must adhere to the data protection legal framework. Public authorities have abundant technical and personnel resources which allow them to take into consideration PbD and to demand PbD in the procurement of biometric systems. One of the main characteristics of PbD is to embed privacy-enhancing solutions in the design stage of modern technologies. In this way, technical and legal aspects go hand in hand, and both must be considered from the drafting of a product that will affect the privacy of individuals.

PbD can be the backstory of Article 25 GDPR named "Data protection by design and by default". It is the controller's obligation to implement technical measures (such as pseudonymisation) to meet the requirements of the GDPR.[141] Data protection by default means that only personal data necessary for a specific purpose are processed. This obligation applies

[139] N Marnau and C Sorge, "From Law to Engineering: A Computer Science Perspective on Privacy and Data Protection' in G González, R Van Brakel, and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (Elgar, 2022) 198.
[140] Therefore, this principle can be interpreted as the duty to have access to legal (ethical) consultants for biometric implementation.
[141] Regulation (EU) 2016/679, Article 25(1).

to the quantity of personal data, to the extent of processing, as well as to the period of storage and accessibility.[142] The problem with the obligations of Article 25 is their vagueness. It is hard to determine how long a storage period would need to be to be contrary to data protection by default. A further problem is that PbD requires technical solutions, while at the same time, the legal implementation of PbD depends on policy choices and an interpretation of the principles it contains. Yet another problem with Article 25 GDPR is that it already envisages many reasons why privacy by design and default may be limited, as it starts with "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (...)."[143] Article 25 does not oblige the controller to implement any concrete technical solutions or organisational measures.[144]

2.3.5. Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) is required from the controller when the processing would result in a high risk for the rights and freedoms of natural persons.[145]

DPIA is required in the case of automated processing, including profiling, the processing on a large scale of sensitive personal data (which includes biometric data) or of personal data relating to criminal convictions and offences referred to in Article 10, or in the case of the large-scale systematic monitoring of a publicly accessible area (meaning surveillance).[146] This neatly corresponds to the use of biometric technologies. Thus, it can be said that the processing of biometric data (mostly) requires a DPIA, and that the use of biometrics as a rule does require one.[147] By extension, this could be interpreted that in the case of biometric verification, DPIA is not mandatory in all cases. There is no exhaustive list of the kinds of activities associated with the processing of personal data that require DPIA.[148] As an exception to the duty to conduct

[142] Regulation (EU) 2016/679, Article 25(2).
[143] ibid, Article 25(1).
[144] EDPB, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" Version 2.0 (2020), point 14.
[145] The terminology of "high risk" may bring to mind the way the AI Act is structured.
[146] Regulation (EU) 2016/679, Article 35(3).
[147] See M Kontak, "Biometric Borders Envisaged by Frontex: Fundamental Rights in the Backseat" (2024) 9(2) European Papers, 621-640, where the author argues that Frontex should conduct a DPIA when it considers the future application of biometric technologies.
[148] A29WP, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the purposes of Regulation 2016/679" 17/EN WP 248 (2017).

DPIA, the supervisory authority may create a list of processing activities which do not require DPIA.[149]

The use of facial recognition requires a prior DPIA.[150] A prior consultation with data protection authorities (DPAs) may also be required from the controller.[151] The use of new technologies is a factor that signals the obligation for a DPIA.[152] DPIA consists of a systematic description of the processing and legitimate interests, a proportionality assessment in relation to purposes, an assessment of the risks to the rights and freedoms of data subjects, as well as the measures to address these challenges.[153] If the DPIA indicates that the processing "in the absence of measures" would result in a high risk, the controller has to consult the supervisory authority prior to processing (the A29WP Guidelines call this occurrence "residual high risk").[154] In *RL v Wiesbaden*, the CJEU was asked by the referring Court whether there was an obligation to conduct DPIA prior to legislation which mandated the processing of biometric data for the purpose of storing fingerprints and facial images locally on the identity document.[155] The Court reasoned that DPIA is generally needed in the context of using new technologies and concerning the processing of biometric data used for identification but ruled that DPIA was not needed in this case since the regulation in question preceded the application of the GDPR and there was therefore no obligation to conduct DPIA according to the rules of the GDPR.[156]

DPIA has the purpose of assessing the likelihood and severity of risk and considers the nature, scope, the purpose of processing and the sources of risk.[157] It should particularly include measures for mitigating risk which demonstrate compliance with EU data protection law.[158] Concerning the LED, DPIA is prescribed in less detail. Importantly, DPIA in the LED context is conducted on the basis of national law.[159] An example of high risk is when there are

[149] Regulation (EU) 2016/679, Article 35(3).
[150] FRA, "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement" (2019) 26; EDPB, Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024).
[151] Regulation (EU) 2016/679, Recital 84 and Articles 35-36; Directive (EU) 2016/680 Articles 27-28; GDPR.
[152] Regulation (EU) 2016/679, Recital 89.
[153] ibid, Article 35(7).
[154] A29WP, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely To Result In A High Risk' for the Purposes of Regulation 2016/679" 17/EN WP 248 (2017), 5.
[155] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251.
[156] ibid, paras 64-69.
[157] It shares a common idea which is also behind the precautionary principle, namely that harm or risk should be considered and minimised even before practical application.
[158] Regulation (EU) 2016/679, Recital 90.
[159] Directive (EU) 2016/680, Article 27.

significant or irreversible consequences and when the risk seems obvious.[160] Kindt comments that such a case would be if a data subject could not change their biometric credentials in the case of theft.[161] One could add other examples in the context of biometrics such as in the case of biometric identification for the purpose of boarding a plane, where a previous DPIA for such a procedure should be viewed as mandatory. There are many factors why DPIA is required in such cases: it concerns the processing of sensitive personal data, it is done on a large scale, it applies a new technology (for example, a new way of registering people boarding a plane). Ultimately, the consequences for the rights and freedoms of natural persons in the case of false negative or positive results are not trivial. The DPIA obligation surely likewise applies to scraping photographs from the internet for creating biometric databases (which may also be considered a banned practice in the EU), to biometric surveillance and to biometric identification in the context of large-scale systems.

2.4. Biometric Data: The Building Blocks of EU Biometric Law

The GDPR was introduced to replace the DPD.[162] Article 16 TFEU gave the EU the competence to regulate data protection across sectors.[163] This novel competence was used for enacting the GDPR. The current legal framework for biometric data seems simple enough to understand. There is a general definition of biometric data in Article 4(14). In addition, there is mention of biometric data among sensitive personal data in Article 9(1). However, the relationship between the definitions of biometric data in Article 4(14) and Article 9(1) is unclear. Moreover, not only is there debate on how biometric data should be reformed (to protect the fundamental rights of individuals or to achieve other goals) but there is no definitive answer to how biometric data is to be understood as the law currently stands.

Here is how biometric data is defined in GDPR, Article 4(14):

> "Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person,

[160] A29WP, "Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is 'Likely to Result in a High Risk' for the purposes of Regulation 2016/679" 17/EN WP 248 (2017) 18.
[161] E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3) Computer Law & Security Review, footnote 49, doi: 10.1016/j.clsr.2017.11.004.
[162] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity, 193–217, 195 https://doi.org/10.3233/IP-211525.
[163] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) [2012] OJ C326/1, Article 16.

> which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data (...).

A number of conclusions follow from this definition. First, the GDPR does have an explicit definition of biometric data, specified from the general concept of personal data. It follows that the legislator wanted to achieve a certain purpose by having a separate concept of biometric data as opposed to the general concept of personal data. This argument speaks against differentiating between the definitions of biometric data in Article 4(14) and Article 9(1), since the Article 4(14) definition would in no way be treated differently from ordinary personal data and thus would have no useful effect. Second, biometric data are a subcategory of personal data, which means that biometrics are framed as the processing of personal data. Third, facial images and dactyloscopy data are given as examples of biometric data, but the list is open to other examples.

The Article 4(14) definition of biometric data can be broken down into the following components: personal data, specific technical processing, and the physical physiological or behavioural characteristics of a natural person to allow or confirm the unique identification of that natural person. The two key components that "narrow" the definition are the requirement of "specific technical processing" and the requirement to "allow or confirm the unique identification". That the definition of biometric data is narrow or indeed strict means that not all data that are in the technical sense understood as biometric data are also biometric data in the sense of EU law and the GDPR. Some authors view biometric data as containing three cumulative conditions: to be based on technology (the "specific technical" part), to relate to physical, physiological, or behavioural characteristics, and to allow or confirm the unique identification of an individual.[164] Thus, one could understand biometric data as information that has the closest link to an individual, because it is derived from the characteristics of that individual and because it reveals more about the individual than "mere" personal data. Biometric data deserve stricter protection than other personal data because of the potential infringement of the privacy of an individual. What follows is a detailed analysis of the elements that make up the definition of biometric data in Article 4(14). Finally, there will be a reflection on how EU biometric law should be changed.

[164] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity 193–21, 198; E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3) Computer Law & Security Review, 5 doi: 10.1016/j.clsr.2017.11.004.

2.4.1. The Element of Personal Data in the Definition of Biometric Data

Personal data is defined as any information relating to an identified or identifiable natural person.[165] The full definition of personal data is contained in Article 4(1) GDPR:

> "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The meaning and scope of personal data are essentially the same in the GDPR as they were in the DPD.[166] It is important to note that being identified means being distinguished from a group, not necessarily determining the identity of that individual.[167] Personal data are the information that relate to a person. Biometric data or biometric information in the technical sense may be understood as any information related to the process of biometric identification or verification. Being identifiable is a lower threshold than being identified and means the possibility of being identified with additional information. Recital 26 GDPR contains a list of factors to assess identifiability, which follow from A29WP Opinion 4/2007.[168]

2.4.2. Resulting from Specific Technical Processing

In addition to the existence of personal data, there must be the "processing" of such data. This is true for any personal data. Processing is any operation performed on personal data, whether or not by automated means.[169] This is the general concept of processing. It very broadly encompasses any operation performed on personal data. However, biometric data must be specifically technically processed. The meaning of *specific technical* processing is not explained in the GDPR, except by means of the proviso that photographs are biometric data

---

[165] GDPR, Article 4(1).

[166] C Kuner et al. (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 106 ISBN 978–0–19–882649–1.

[167] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes" [Thesis fully internal (DIV), University of Groningen] (2019) University of Groningen, 65; A29WP, "Opinion 4/2007 on the Concept of Personal Data" (2007) 01248/07/EN WP 136, 12.

[168] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes" [Thesis fully internal (DIV), University of Groningen] (2019) University of Groningen, 65-66.

[169] See also Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, para 28.

only when processed by specific technical means.[170] Nevertheless, it is clear that the legislator wanted to stress an additional element that needs to apply when it comes to the processing of biometric data to distinguish biometric data from personal data. The requirement that this be "specific technical processing", as in the Article 4(14) definition of biometric data, drastically narrows this concept of processing.

Even if the legislator wanted to curtail an expansive notion of biometric data, it is doubtful that this turn of phrase was the way to go about it. The legislator wanted to narrow down biometric data only to those data derived from biometric processes, such as fingerprint recognition or facial recognition. In other words, operations in which a human characteristic is processed by a biometric system which includes a scanner, computer, or an algorithm for making the comparison. Specific technical processing seems to mean "technology based",[171] but using technology that contributes to the identification of the individual.[172] Otherwise, large swathes of personal data, such as a video or photograph of a person, would fall under the ambit of biometric data. Consequently, the GDPR is much less restrictive when it comes to the processing of video and photographs than would be the case if these were considered biometric data. Some commentators are critical of the way the GDPR (and the LED) regulate the taking and storing of photographs and videos as well as the soft law guidance on the same matter:

> Overall, the treatment of technologies capturing images in EU data protection law is sloppy, unsystematic, and kept vague to avoid legal controversies. The soft law guidance offered by data protection authorities in Member States and by the European Data Protection Board (EDPB) is hardly any better. The result is a permissive system of rules and principles that in practice hardly impedes the out roll of these visual surveillance technologies.[173]

The main complaint of these authors is that video surveillance is not considered the processing of special categories of personal data, even though such surveillance can reveal sensitive data on the person, such as special categories of personal data defined in Article 9(1) GDPR, which

[170] Regulation (EU) 2016/679, Recital 51.
[171] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity 193–217, 198 https://doi.org/10.3233/IP-211525.
[172] EDPB, "Guidelines 3/2019 on processing of personal data through video devices" Version 2.0 (2020), point 74. See also C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes (Thesis fully internal (DIV), University of Groningen) (2019) University of Groningen. 67-68.
[173] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity 193–217, 197, https://doi.org/10.3233/IP-211525.

include, among other things, the racial or ethnic origin, political or religious positions, health status or sexual orientation of a person.

Indeed, the EDPB published Guidelines 3/2019 on the processing of personal data through video devices, which are careful not to provide any definitive or clear answers. For example, they state that a video of a person in a wheelchair is not *per se* considered a special category of personal data. This is despite the fact that a special category of personal data includes data on health, of which identifying disability is a prime example. This EDPB guidance does not explain why a video by which a person in a wheelchair may be identified is not a special category of data ("*per se*"). The exclusion of most photographs and videos from being considered sensitive data relies on the fiction that one cannot identify that there is a person in a wheelchair, or that the video (or photograph) reveals the racial or ethnic origin of a person. What is more, such videos or photographs could be used for biometric recognition, but since they are (nominally) not used, they are considered merely personal data, not biometric data.

It can be discerned that the EDPB in Guidelines 3/2019 attempts to make a distinction between personal and biometric data in that biometric data require two additional elements: a specific technical means (using special tools) and a specific purpose (be it identification or verification).[174] But this test is not developed further. How does one determine, or declare, a purpose for which one records people entering a church? Is it just a video of a church *per se* or a video which is used for the more sinister purpose of creating a database of people who go to church? Revealing religious belief means the processing of sensitive personal data. It is on firmer grounds that this EDPB Guideline states that the GDPR is not applicable at all if the individual cannot be identified, for example if a dummy camera is used, or as in the case of a car parking assistance camera which cannot clearly show either people or licence plates.[175] There is clearly no processing involved. It could be said that there is an objective reason for such examples to lie outside the GDPR: there is no (specific technical) processing of personal data. But in cases where persons are being filmed or photographed, and those data are often stored, whether these are biometric data or merely personal data is not clearly delineated.

Kindt states that the notion of specific technical processing has the (desired) effect of excluding so-called raw data that may be contained in certain databases as opposed to (specifically

[174] EDPB, "Guidelines 3/2019 on processing of personal data through video devices" Version 2.0 (2020) 17.
[175]EDPB, "Guidelines 3/2019 on processing of personal data through video devices" Version 2.0 (2020) 7.

technically) processed biometric data.[176] For example, a video surveillance system can capture the faces of persons or record their voices, but provided that these biometric characteristics are not stored for the specific purpose of biometric recognition, this would not represent data processed for specific technical purposes. In other words, such audio-video recordings are personal data, not biometric data. Kindt traced the requirement of specific technical processing, "the most striking element in the new definition" to a document adopted by the Council in 2015, which in turn can be traced back to the opinion of the Committee on Bioethics from 2012 for the revision of Convention 108.[177]

The GDPR Proposal of 2012, as explain above, contained a remarkably simple definition of biometric data as any data relating to the physical, physiological, or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopy data. This proposed definition would mean that any facial image or a video recording which can be used for identification is biometric data. The addition of "resulting from specific technical processing" drastically narrowed the scope of biometric data. This addition to the concept of biometric data was prompted by the same Committee on Bioethics that reviewed the concept of biometric data (and of genetic data) in the GDPR 2012 proposal. The Committee stressed the divide between ordinary personal data which undergo ordinary processing (such as when private persons exchange photographs) against personal data that are used in a certain way (such as for biometric identification).[178] Kindt raises the point that the Committee on Bioethics might not have sufficiently understood the capabilities of biometrics.[179] Biometric identification can be made from photographs scraped from publicly available Facebook, Instagram or WhatsApp profiles, or from security camera videos. This will be explained in the example of Clearview AI.

It is even more important, in the view of the author of this thesis, to raise the issue of distinguishing the element of "specific technical processing" from the last part of the definition "which allows or confirms unique identification", which neither Kindt nor the cited sources do clearly enough. The Committee on Bioethics, according to Kindt, wanted to stress the different

[176] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020), 64.
[177] E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3) Computer Law & Security Review, 12-13, doi: 10.1016/j.clsr.2017.11.004.
[178] ibid.
[179] ibid.

purpose of a photograph between ordinary (everyday) and sensitive use (for identification),[180] but an even greater problem is that the element of specific technical processing and the element of the purpose of identification or verification are conflated, since both seem to mean some kind of technical, automatic or machine-like process. This raises the question of what the added value is of having both elements in the definition of biometric data. Could the definition be simplified (and made more precise) by removing one of these two elements? If the purpose of allowing or confirming unique identification is removed, there would still be the requirement of specific (biometric) processing, which would ensure that non-biometric uses of photographs or video are not captured by the definition of biometric data. Another idea would be to remove the element of specific technical processing and focus on the element of biometric recognition. Any personal data processed for the purpose of biometric recognition (which includes identification and verification) would be biometric data. The biometric purpose in that case would best be left to the common sense of the decision-makers in a particular case.

To illustrate the oddness of the definition of biometric data which stems from elements of specific technical processing and the purpose of biometric recognition, one can bear in mind the example of a photograph of a person. A photograph contains information about the person and so it is personal data. If this photograph is observed by a human that happens to recognise the person in the photograph (Hey, this is Alice!), the photograph would still only be personal data because there are no technical means involved in the recognition. If an AI system deduces that this is Alice, then the same photograph would be biometric data, because this AI system represents specific technical processing. One would have to further know the exact purpose of why the AI system was processing the photograph. If the image of Alice were processed without the purpose of either verification or identification, it may be considered only personal data. The photograph does not physically change, but the legal qualification of the photograph changes depending on the way it is processed. It is difficult to determine whether there was an intention to biometrically process this photograph or use it for other reasons. All this argues for a uniform interpretation that all biometric data should be considered sensitive.

However, there is also a significant problem in approaching biometric data without inquiring about whether the purpose of processing is biometric recognition. As technologies develop, it is becoming possible to identify persons from photographs or video that used to be of insufficient quality. If processing for the purpose of biometric recognition is not an element of

[180] ibid.

biometric data, then the legal qualification of a photograph or a video changes as the technologies improve. A photograph that used to be of too low resolution to determine identity becomes biometric data when it becomes possible to use it for biometric recognition. Therefore, both solutions produce unusual results. In the first case, which is the current state of the law, a photograph changes its legal nature from personal data to biometric depending on whether it is processed by technical means and for biometric purposes or not. If the purpose of biometric recognition is removed from the definition of biometric data, then a photograph would become biometric data from the moment a technology becomes available for biometric identification to be made with the photograph. Both approaches to the definition of biometric data have a philosophical air: the (legal) nature of the object changes even if the object remains the same.

2.4.3. On Physical, Physiological or Behavioural Characteristics of Natural Persons

This element of the definition of biometric data leads to a discussion of several important points: first, what is the relation between biometric and genetic data; second, what is the relation between biometric data and biometric characteristics; and third, how to differentiate between physical, physiological, and behavioural characteristics?[181]

2.4.3.1. Biometric Data vs Biometric Characteristics

Biometric data, as explained in the chapter on definitions, are different from biometric characteristics. Likewise, the GDPR distinguishes between biological material (e.g. saliva or the finger), which is not personal data, and the personal (including biometric) data derived from it.[182] A simple (and reductionist) way of putting this is to say that parts of a person or biological samples taken from a person are not personal data themselves. The distinction between biological material and the data processed from it has long been recognised by A29WP[183] as well as by scholars.[184] It is useful that the GDPR already includes the concept of characteristics, since this is important to properly define biometric data. In order not to conflate the finger from

[181] Concerning the relation between genetic and biometric data, see 2.4.4 of the thesis.

[182] Regulation (EU) 2016/679, Recital 35.

[183] "Human tissue samples (like a blood sample) are themselves sources out of which biometric data are extracted, but they are not biometric data themselves". A29WP, "Opinion 4/2007 on the concept of personal data" (2007) 01248/07/EN WP 136, 9; See also A29WP, "Opinion 3/2012 on Developments in Biometric Technologies" (2012) 00720/12/EN WP193, 4.

[184] LA Bygrave and L Tosoni, "Article 4(15). Data Concerning Health" in C Kuner et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 223, ISBN 978–0–19–882649–1.

fingerprint data, there is a need for vocabulary to distinguish between the biometric characteristic and the biometric data.

However, in the view of the author, this distinction can become problematic. For example, cellular samples are not considered biometric (or personal) data but merely the material from which such data are processed. So, could cellular samples be stored by public authorities without triggering the application of the data protection framework? The ECtHR's *Marper* case concerned exactly the storage of cellular samples. It would be problematic to claim that data protection and the privacy framework do not apply to cellular samples because the cellular samples are not personal data themselves.[185] Nevertheless, there is a distinction between the cellular sample and the data that can be extracted from it. Clearly, certain flexibility is needed in defining biometric or personal data.

2.4.3.2. Unique Characteristics Compared to Unique Identification

The definition in Article 4(14) does not speak of characteristics being unique, but it is important to consider whether human characteristics must be unique to be used for biometric recognition. This is especially pertinent in delineating biometric recognition (identification and verification) from biometric categorisation since categorisation does not rely on unique human characteristics. Uniqueness is used to describe certain biometric characteristics. For example, it is considered that the ridges and whorls of the fingers of each person are unique. Unique characteristics are thus the prerequisite for unique identification, which is mentioned in the GDPR's definition of biometric data. However, it can be debated whether the fingerprints of each human individual really are unique.[186] Were there ever two identical snowflakes? Perhaps. But uniqueness is not required. What is decisive is that features such as fingerprints or iris scans or facial images (of sufficient quality) are distinct enough to be used for unique identification, even if it is possible that there may be two persons on the planet whose fingerprints or whose faces the biometric algorithm would recognise as the same (and thus create an identical biometric template). This possibility of an identical fingerprint is theoretical and minuscule. Otherwise using biometrics would not be practical and widely used.

---

[185] *S and Marper v UK,* App. no. 30562/04 and 30566/04 (ECtHR, 4 December 2008) para 68.

[186] C Jasserand, "Avoiding Terminological Confusion Between the Notions of 'Biometrics' and 'Biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective" (2016) 6(1) International Data Privacy Law, 74, https://doi.org/10.1093/idpl/ipv020.

2.4.3.3. Differentiating Between Physical, Physiological and Behavioural Characteristics

The GDPR definition of biometric data in Article 4(14) mentions all three types of characteristics. A more elegant solution would have been to use only one expression, such as physical (or instead biological) characteristics. This approach would soon run into trouble because there are biometric technologies that rely on the unique way a person behaves – for example, the gait (the way one walks). Regarding a signature, this could hardly be qualified as a physical or biological characteristic, even though a signature can serve to identify a person. Nevertheless, there is obviously improvement to be made to this segment of the definition. Physical and physiological should be considered to have the same meaning as biological. This would also be in line with ISO biometrics vocabulary which defines biometric characteristics as either biological or behavioural. What is more, ISO vocabulary provides as follows:

> Behavioural and biological characteristics cannot be completely separated which is why the definition uses "and" instead of "and/or". For example, a fingerprint image results from the biological characteristics of the finger ridge patterns and the behavioural act of presenting the finger.[187]

In other words, "behavioural and biological" should always be used together, as a single expression, without attempting to delineate the two. Most biometric technologies concern (primarily) biological characteristics, such as facial recognition, fingerprint recognition or DNA profiling. Signature, gait, or the way a person types at a keyboard can be considered behavioural characteristics.[188] To make matter unnecessarily more complicated, some commentators talk also of physiographic or biochemical characteristics.[189] The distinction between physical and physiological on one hand and behavioural on the other is clear, as noted by scholars as well as other interpretative sources.[190] However, the difference between physiological and physical characteristics is unclear, as noted also by Jasserand.[191]

---

[187] Note 5 ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics.

[188] See also P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity, 193–217, https://doi.org/10.3233/IP-211525.

[189] LA Bygrave and L Tosoni, "Article 4(15). Data Concerning Health" (2020) in C Kuner et al. (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 212, ISBN 978–0–19–882649–1.

[190] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes (Thesis fully internal (DIV), University of Groningen) (2019) University of Groningen, 68; A29WP, "Working Document on Biometrics" (2003) WP 80, 3.

[191] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes (Thesis fully internal (DIV), University of Groningen) (2019) University of Groningen, 68.

One may assume that the physical and psychological refer to the same category of characteristics, but that the legislator wanted to play safe by covering it in two terms, in the event that there are further development in biometrics. But this terminological imprecision shows that the legal understanding of biometrics is still in flux and is developing.

In conclusion, the difference between physical, physiological, and behavioural characteristics should not be viewed strictly. Some characteristics may straddle the line between more than one characteristic, while other characteristics may be difficult to define due to a novel biometric technology. The key aspect of characteristics is that they are *human* characteristics and that they represent what is used from a human person in the process of biometric recognition.

2.4.4. Genetic Data and Biometric Data: Different Purposes

Related to the debate on characteristics is the important issue of how to distinguish between biometric and genetic data. Both are defined in the GDPR and mentioned in Article 9 as well.

Genetic data is defined in the GDPR Article 4(13) as follows:

"'Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result from an analysis of a biological sample from the natural person in question.[192]

This GDPR definition mentions "characteristics" and "sample". Unfortunately, these are not understood in the sense of ISO biometrics vocabulary, so it is best not to equate these to biometric characteristics, as the definition currently stands.

In the Working Document of Biometrics of 2003, A29WP stated that biometrics mostly concerned "areas of DNA and fingerprint testing".[193] Opinion 4/2007 considered that DNA has a "dual character" as it can be used both for information on the human body and for unique identification.[194] The subsequent Opinion 3/2012 noted that DNA profiling has become much faster and cheaper. Therefore, DNA profiling can be much more extensively used for

[192] Recital 34 of Regulation (EU) 2016/679 also mentions that genetic data include data resulting from not only deoxyribonucleic acid (DNA) but also chromosomal, or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained. in the same sense it is understood here, as encompassing other venues of determination alongside DNA.
[193] A29WP, "Working Document on Biometrics" (2003) WP 8, 2.
[194] A29WP, "Opinion 4/2007 on the concept of personal data" (2007) 01248/07/EN WP 136, 25.

identification, but considering the nature of the information contained in DNA and the sensitive data it contains, such use would create serious consequences.[195] This Opinion noted the creation of the Prüm Treaty which allows cross-border access to national DNA databases for the prosecution of crime.[196]

DNA can be viewed both as biometric and as genetic data. DNA sequencing is used to establish the identity of persons, particularly in criminal law. In this sense, DNA profiling is a biometric technology which is very reliable and secure, but also most taxing on the privacy of an individual. Due to its accuracy, DNA profiling is extensively used in the law enforcement context. In addition, databases for particularly serious crime, such as terrorism or sex offences, exist in many EU Member States. DNA profiling is also used to establish the identities of missing persons or of unaccompanied children.[197] However, besides law enforcement and use by public authorities, DNA sequencing is also widely employed in medicine to determine the right treatment or the propensity to a certain medical condition. In this medical context, DNA sequencing is used as genetic, not biometric data. Genetic data shares similarities with biometric data, as both are counted as special types of personal data in Article 9(1) GDPR and both biometric and genetic data are subject to special additional national legislation, a possibility provided by Article 9(4) GDPR.

DNA profiling can be used as a method for the identification of a person or for the verification of identity. As a biometric method, it has strengths and weaknesses. DNA profiling infringes the privacy (and human dignity) of an individual in the strongest sense, especially when a DNA profile is stored, often for an exceedingly long period.[198] DNA profiling is thus from a human rights and legal standpoint a very contentious biometric technology. DNA profiling is more expensive and takes significantly longer than fingerprint or facial recognition.

The strengths of DNA profiling are that it is precise and, more importantly, hard to fool. So-called spoofing methods are a risk when it comes to biometrics such as faking fingerprints for

---

[195] A29WP, "Opinion 3/2012 on Developments in Biometric Technologies" (2012) 00720/12/EN WP193, 9.

[196] 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 210/1.

[197] Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L 312/56, Article 42(3).

[198] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, 4 December 2008); *Gaughran v UK*, App. no. 45245/15 (ECtHR, 13 June 2020).

fingerprint recognition or using masks, stolen images or deepfake methods to trick facial recognition. DNA profiling is the least susceptible to fraud of this kind.[199] Besides, fingerprints (or other biometric samples) may not be available, but cellular samples, for example from a crime scene, may be, thus making DNA profiling the obvious choice for determining identity in the law enforcement context. Another aspect of DNA profiling is that it requires an actual physical sample as opposed to a fingerprint or a facial image. More intriguingly, some commentators raise the point that "DNA matching is not done in real time and, for the most part, is not automated".[200] This point is dubious, as it is hard to claim that DNA profiling is not automated since it necessarily involves sophisticated technical tools.

On the other hand, the costs of DNA profiling are falling exponentially. The results can be obtained very quickly. This has nudged Frontex to consider using DNA profiling for border control and migration purposes, in the way fingerprint recognition is used now. A Frontex report on the future of biometric technologies for border control examined DNA profiling among twenty biometric technologies and concluded that DNA profiling is especially good from a security standpoint, but there may be problems with public acceptance and costs.[201]

Genetic data are mentioned among the special categories of personal data in Article 9(1). There is a significant similarity between genetic and biometric data. Both biometric and genetic data pertain to an individual natural person. Genetic data may be understood as the most extreme, or intimate, personal data. It is not "merely" fingerprints, or a facial image, but a blueprint of an individual. Genetic data have been at the forefront of many ECtHR cases. The *Marper* case concerned the collection and unlimited period of storage of DNA profiles of persons who were suspected but not convicted of crimes, where the ECtHR deemed that such practice was contrary to the right to respect for private and family life (Article 8 ECHR).[202] Another of CJEU's seminal judgments concerning the processing of biometric data in which it was viewed as a justified infringement of privacy is *Schwarz*, which referred to *Marper*.[203]

---

[199] Frontex, Technology Foresight on Biometrics for the Future of Travel (European Border and Coast Guard Agency, 2022) www.frontex.europa.eu.

[200] LA Bygrave and L Tosoni, "Article 4(14) Biometric Data" in C Kuner et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), ISBN 978–0–19–882649–1, 213.

[201] Frontex, Technology Foresight on Biometrics for the Future of Travel (European Border and Coast Guard Agency, 2022) www.frontex.europa.eu.

[202] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, 4 December 2008).

[203] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, para. 27, stating that fingerprints constitute personal data and paragraph 55 which concerns the proportionality test.

In short, DNA and biometric data share many common features from the perspective of legal analysis. The more recent ECtHR judgment in *Gaughran* closely follows *Marper*, but it explicitly refers to DNA as biometric data.[204] A 2024 CJEU judgment concerning biometric data and law enforcement confirmed that it is contrary to the LED and the CFR to store indefinitely biometric and genetic data, mentioning *Gaughran*.[205] These connections show that the legal treatment of genetic and biometric data under the ECHR and EU legal framework is closely connected.

In conclusion, there is a significant overlap between genetic data and biometric data. DNA profiling can be used as a biometric technology, along with facial, fingerprint or iris recognition. The difference thus lies in the purpose. If the purpose of DNA profiling is to determine certain health or biological properties of a person, it is genetic data processing. If the purpose of DNA profiling is to determine the identity of a person, it is biometric data processing. There is no closed list of possible biometric characteristics that can be used for biometric recognition, especially since new ways of determining the unique identity of a person are being developed. Thus, one should consider that DNA profiling can be interpreted either as the processing of genetic data or of biometric data, depending on the purpose and national laws of EU Member States. GDPR Article 9(4) states that "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health".[206]

2.4.5. Allowing or Confirming Unique Identification

In defining biometric data, Article 4(14) uses the expression to "allow or confirm unique identification". Allowing unique identification should be understood as biometric identification (also known as one-to-many identification), while to confirm unique identification should be understood as biometric verification (also known as one-to-one identification). The GDPR may confuse the reader by using the noun "identification" both to describe biometric identification (to allow identification) and to describe biometric verification (to confirm identification). This part of the definition precludes categorisation from being included as biometric data. Biometric

[204] *Gaughran v UK* App. no. 45245/15 (ECtHR, 13 June 2020).
[205] Case C-118/ 22 *NG v Ministerstvo na vatreshnite raboti* ECLI:EU:C:2024:97.
[206] See 2.5.4 of the thesis.

categorisation does not result in unique identification, but in sorting persons into categories. Whether categorisation should escape the definition of biometric data depends on a policy choice. If one opts for a stricter regime for biometric categorisation, then changing this part of the definition by removing "unique" would make sense.

This element of "allowing or confirming unique identification" suggests that the meaning of biometric data depends on why these data are processed. This element can thus be seen as an external and a subjective element in the definition of biometric data. External, because the purpose of processing cannot be determined by the data themselves, since the purpose of processing is determined by the data controller. The external element in the definition is a particularly legal feature of the definition of biometric data. It would be absurd if the ISO/IEC biometric vocabulary tied biometric data to how or why biometric data are processed, as is done in the GDPR's understanding. However, a closer look reveals that the ISO definition of biometric recognition implicitly includes the purpose of biometric identification or verification, since biometric recognition only happens when the *intention* is to make a biometric comparison, and not accidentally.

"Unique identification" means the highest degree of identification, not merely to be identified or to be identifiable.[207] The biometric data themselves do not have to be unique, but they must lead to the identification of a single individual.[208] Biometrics operate within probability. In other words, there is always a chance that a person was wrongly identified. Therefore, biometric data are not a unique identifier of a person, as a unique citizen number is. Biometric data lead to the singling out of a natural person with high probability.[209]

The term "unique identification" from the GDPR should be understood to mean the representation of a higher threshold of identification for biometric data than for personal data.[210] For example, the address of an individual is personal data, because the person is identifiable from this information. Fingerprint data are biometric data because they lead to a unique identification, a singling out of that natural person. It should be kept in mind that personal data are understood as information concerning either identified or identifiable individuals. Thus,

[207] C Jasserand, "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data' (2016) European Data Protection Law, 13-14
[208] ibid.
[209] See analysis in C Jasserand, "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data' (2016) European Data Protection Law, 13-14.
[210] C Jasserand-Breeman, "Reprocessing of Biometric Data for Law Enforcement Purposes (Thesis fully internal (DIV), University of Groningen) (2019) University of Groningen, 70.

personal data that lead to unique identification should be understood as the highest form of identification, not merely the possibility of identifying, or even singling out from a group, but specified in its identity.

This element of "allowing or confirming unique identification" is also subjective. Determining the purpose requires answering what one wanted to achieve, which is subjective by nature. As mentioned previously, it is questionable whether a video of a church is a video processed for the purpose of keeping an eye on churchgoers or for the purpose of protecting church property. This depends on determining the mental processes of the controller and the processor. Naturally, this opens the question whether controllers can be trusted when they state the purpose of processing. How is it possible to determine their true intention and to prove something that is exceedingly hard to establish: intention? This subjectiveness of the definition of biometric data is like defining pink as a colour that is of a certain wavelength and is also observed for the specific purpose of the determination of colour, so something would not be legally pink if it were merely observed for another purpose.[211]

On the other hand, this definition of biometric data in the GDPR was based on clear practical considerations. An outside, subjective element in the definition was needed (for the purpose of specific technical processing). As already stated, without this element, any photograph or video recording would potentially be a source of biometric data. This would be too cumbersome, and it would endanger the whole *économie générale* of the GDPR, because anything that could be used for the identification of a person could be deemed to be biometric data. Another consequence would be that, as biometric technologies improve, the meaning of biometric data would shift with the changes, also as explained above.[212]

But with the subjective element of purpose added to the definition in Article 4(14), it does not matter that a video *could* be used for the identification of persons as recent technology becomes available. For the video to be biometric data it must specifically be used for that purpose. A hundred years ago, a blood stain did not reveal any personal information. Fifty years ago, the blood type could be determined from such a blood stain. For decades now, the whole DNA of a person can be determined from a blood stain. A blood stain thus shifted from being a source of no personal data, to personal data, to biometric (and genetic) data. The nature of the data

[211] What is more, to be pink would also require to be observed by a specific (technical) process, not by the naked eye.
[212] See 2.4.2 of the thesis.

from that blood stain however remains constant if the purpose is not to determine identity (with the use of specific technical means). So the conundrum at the heart of the GDPR approach to biometrics (a conundrum that was sensed long before the GDPR in the A29WP documents): how to carve out biometric data and give them heightened protection without bringing down the whole system of personal data?[213] First, one needs to define the object of this extensive protection. This requires defining biometric data. If one opts for an "objective" definition, the definition is simple. Biometric data are personal data used for biometric recognition (adding the distinction of categorisation). But this definition would encompass too much. The GDPR opted for a "subjective" definition of biometric data, which is as narrow as possible. And this would have been workable had it not been for the unclear, muddled approach to biometric data taken in Article 9.

2.4.6. The Crucial Debate: Are All Biometric Data Sensitive or Only Those of Article 9 GDPR?

Article 9(1) GDPR defines special categories of personal data. This are personal data of a particularly sensitive nature. Recital 10 of the GDPR refers to special categories of personal data also as "sensitive data". Therefore, the processing of such special personal data is prohibited. Unless, of course, any of the ten broadly defined exceptions to the prohibition of processing of special categories of personal data are applicable. Special categories of personal data are so defined:

> (...) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (...)

One can firstly notice the mention of biometric data among the special categories of personal data. The problem is that what is mentioned is not simply "biometric data", which would clearly mean that biometric data as defined in Article 4(14) are among special categories of personal data. Article 9(1) mentions biometric data *for the purpose of uniquely identifying a natural*

[213] In a sense, the same problem now occurs with the AI Act: how to define AI so that it does not encompass everything while including biometrics as an AI technology? Legal science has thus succeeded in bending issues of innovative technology to a theoretical debate: what is the nature of "x", is "x" separate or the same as "y"?

person. This opens the question of whether there are at least two types of biometric data in the GDPR, or even more.

What is certain is that it is extremely important to properly interpret the relationship between biometric data mentioned in Article 4(14) and Article 9(1) GDPR. If all biometric data are a special type of personal data, then they can be processed only exceptionally, under the stricter conditions of Article 9(2). If there are biometric data that do not concern Article 9(1), then those biometric data can be processed under the less restrictive legal basis of Article 6 GDPR. In the following pages, this debate will be analysed and relevant arguments will be put forward. Along with the components making up the Article 4(14) definition of biometric data, Article 9 is the key provision in EU biometric law.

As was already explained, the European Parliament first proposed adding biometric data to the list of sensitive data in the GDPR.[214] The Council of the EU stated that biometric data can be added to Article 9, but that they should be qualified by the addition of "uniquely identifying a person", reflecting the ambit of the draft of the modernised 108 Convention of the Council of Europe.[215] Meanwhile, the Council of Europe warned that biometric data should be sensitive data, in the context of the modernisation of Convention 108. This was based on the notion that biometric data contain information about health and race, have the ability to identify people and can make it easier to link records and are furthermore irrevocable.[216] In terms of risk to privacy and data protection, it was argued that verification is less risky than using databases, especially in public spaces.[217] The use of databases represents identification, and thus verification and

[214] Sensitive is the term used to refer to special categories of personal data in recital 10 Regulation (EU) 2016/679. See also recital 51 Regulation (EU) 2016/679 .

[215] Point 6, Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Written debriefing of trilogue on 24 November ST 14461 2015 INIT https://www.consilium.europa.eu/en/documents/public-register/public-register-search/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentLanguage=EN&ImmcIdentifier=ST%2014461%202015%20INIT.

[216] Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81

[217] Strangely from the perspective of the worries shown previously, Regulation (EU) 2024/1689 explicitly allows the most intrusive form of biometrics – remote real time biometric *identification* in Article 5. It does so in a similar convoluted way that Regulation (EU) 2016/679 treats special categories of personal data: a general prohibition followed by detailed exception(s). Finally, remote real time biometric identification is allowed in Regulation (EU) 2024/1689 as much as the processing of sensitive data is allowed in Regulation (EU) 2016/679.

identification should be legally treated differently – verification as general biometric data, while identification as the processing of sensitive personal data.[218]

The question is whether there are two fundamentally different conceptions of biometric data, one in Article 4(14) and the other in Article 9(1). Opinions are divided, one camp arguing that there is only one kind of biometric data, read jointly in these two provisions and that thus fingerprint data or facial images used for biometric recognition must all be processed only exceptionally when so allowed by Article 9(2). The other stance is that there are two notions of biometric data, and that only if biometric data are used for the purpose of identification (such as in databases e.g. Eurodac) the conditions of Article 9(2) must be adhered to. The second stance continues that if, however, biometric data are used only for purposes of verification, such as in the case of facial images and fingerprint data stored locally on a passport, then this type of biometric data can be processed under the more lenient conditions of Article 6, which regulates the legal bases for processing personal data generally. Below are the arguments for both sides, starting with the latter position that there is more than one kind biometric data regulated in the GDPR.[219]

2.4.6.1. Arguments for Claiming that Article 4(14) and Article 9(1) Refer to Different Concepts of Biometric Data.

The main point for arguing that the Article 4(14) definition of biometric data is different from the Article 9(1) definition is that Article 9 stresses biometric data *for the purpose of unique identification*, leaving out the verification part. Georgieva and Kuner state that Article 4(14) covers both identification and verification, but Article 9 does not, because Article 9(1) applies only when biometric data are processed for the purpose of unique identification.[220] This textual interpretation is supported by further argumentation: the legislator apparently deemed identification as a greater threat to data subjects' fundamental rights, and, furthermore, objectively, verification does not require a centralised database and it usually involves a smaller number of affected individuals.[221] One problem with this argumentation, spotted also by the commentators themselves, is that Article 4(14) "covers both goals" of identification and

[218] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020), footnote 32.
[219] And hence, also in Directive (EU) 2016/680 and Regulation (EU) 2018/1725 on the processing of personal data by EU institutions, bodies, offices and agencies.
[220] L Bygrave and L Tosoni, "Article 4(14) Biometric Data" in C Kuner et al. (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), ISBN 978–0–19–882649–1, 213-214.
[221] ibid, 214.

verification, so it is difficult to explain why identification is covered only by Article 9(1). In other words, Article 4(14) should refer only to verification, but it refers to both identification and verification. They also rightly notice that Recital 51 GDPR considers the definition from Article 4 and 9 interchangeably by the way it refers to photographs, a point which will further be made in the end of the analysis in this section of the thesis.[222]

Kindt has claimed that there is a distinction between Article 4 and 9 biometric data,[223] but this line of reasoning has led to extreme results. Namely, Kindt argues that there are four types of data relating to the physical, physiological, or behavioural characteristics of a natural person in the GDPR. The first are ordinary personal data derived from such characteristics, which do not satisfy all the requirements of Article 4(14). The second are the biometric data of Article 4(14) but which legally are not distinguished from "ordinary" personal data. The third type are the sensitive biometric data of Article 9. The last are sensitive biometric data that additionally must satisfy the requirements for the large-scale processing of personal data, which must submit to a data protection impact assessment (DPIA), stipulated in Articles 35 and 36 GDPR. But, in the opinion of this author, this goes too far in inferring from the wording of the GDPR categories that were not intended. It makes no sense to claim that there are two definitions related to biometric data which are under the same legal regime as ordinary personal data. In other aspects, the observations of Kindt are sound. Biometric categorisation could be understood as biometrics to which the 'ordinary' regime of the processing of personal data is applied. For example, a heartbeat sensor for detecting irregular migrants hiding under a lorry does process personal data, and these personal data are related to a certain physiological characteristic of a natural person, but the purpose is not verification or identification.[224]

The EDPB has argued for the position that only when the purpose is biometric identification does the Article 9 concept of biometric data arise. The example it gives, however, is problematic: a shop owner who uses a video surveillance system to adjust marketing based on the gender and age of the customer.[225] The idea is that since such a system does not have the purpose of unique identification, it does not fall under the Article 9 concept of biometric data.

---

[222] ibid, 214.

[223] E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3)Computer Law and Security Review, 17.

[224] There are biometric methods to identify persons by their unique electrocardiogram, but this is not the case with the sensor here that can simply infer if there is a heartbeat or not.

[225] EDPB, "Guidelines 3/2019 on processing of personal data through video devices" Version 2.0 (2020), point 21.

But the reasoning of the EDPB on why Article 9 is not applicable is unusual. The EDPB states that in such an example the processing of personal data does not fall under Article 9 because there are no biometric templates stored, instead of claiming that it is so because this is not biometric identification.[226] It is quite extraordinary to introduce the concept of a biometric template, which is not defined in any way in GDPR, as the deciding element. The biometric template is, one might recall, the information that is used for biometric recognition.[227] In other words, there are many original approaches to understanding the definition(s) of biometric data. But in the EDPB view, it suffices to say that the biometric template is not the distinguishing element in the Article 4 and Article 9 GDPR dichotomy, simply because it is not defined there. What is more, the biometric template may also be used for verification stored locally (as mentioned in 1.7.2 of the thesis). More than twenty years ago, A29WP tried to make the distinction between verification (calling it authentication/verification) and identification on the grounds that it is not necessary to store "reference data" (meaning a biometric template) in a database to conduct verification.[228]

Criticising the position taken by the EDPB in the above-mentioned Opinion 3/2019, De Hert and Bouchagiar state that it is unsustainable not to consider photographs (or video) sensitive data, simply because "all kinds of sensitive data can be implied from one simple photograph".[229] Thereby, these authors criticise the even broader distinction that Recital 51 tries to make between photographs as personal data and other sensitive (or) biometric data. The authors, however, hold the position that, while it may be possible to make a distinction between Article 4 and 9, in most cases biometric data are and should be treated as sensitive data, on account of what they can say about an individual.[230]

A better element to distinguish between sensitive and ordinary biometric data might be to ask whether the biometric data are stored in a database. If they are, this is more harmful to privacy. If biometric data are not stored but immediately discarded after processing (and one must take a shop owner's or the police's word on this) then this is less intrusive for privacy unless other points of sensitive personal data arise. But that is merely an observation on how the definition

[226] ibid, points 79-89.
[227] Biometric templates were defined in 1.7.2. Biometric templates in the context of EU information systems are analysed in 3.4.3 of the thesis.
[228] A29WP, "Working Document on Biometrics" (2003) WP 80, 4.
[229] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity, 193–217, footnote 11 https://doi.org/10.3233/IP-211525.
[230] ibid.

of biometric data could be altered (*de lege ferenda*) not on how it should be interpreted as it stands (*de lege lata*). Overall, this reflection should also point towards the view that the distinction between Article 4(14) and Article 9(1) GDPR is unsustainable.

2.4.6.2. Arguments for Claiming that Articles 4 and 9 Should Mean One Unified Concept of Biometric Data

Even in 2006, the European Data Protection Supervisor (EDPS) stated that "biometric data are sensitive by definition".[231] Advocate General Mengozzi picked that up in his opinion in *Schwarz* and also stated that there is a general understanding that biometric data are inherently sensitive.[232] This case, it must be noted, precedes the GDPR, and concerns Regulation 2252/2004 on security features in passports. The judgment of the Court in *Schwarz* did not take up on this point expressed in the opinion on the sensitive nature of biometric data in passports.[233] A recent Grand Chamber judgment of the CJEU is clearer: "Fingerprints, as biometric data, are by their nature particularly sensitive and, as is apparent in particular from recital 51 of the GDPR, enjoy specific protection under EU law".[234]

In another paper, Kindt exposes the view that the Article 4 and 9 concepts of biometric data may be one and the same: "Because the GDPR and DP LED do not differentiate between the two functionalities [of identification and verification], there is legal uncertainty for companies that want to invest in biometric verification technologies and privacy-enhancing methods".[235] Are decision-makers, that is controllers, capable of distinguishing identification from verification, and is this technical difference always clear-cut? Kindt raises a similar worry, and also stresses that the storage place of biometric data is important, yet less understood (legally).[236]

---

[231] EDPS, "Opinion on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions" (2006/C 313/13), point 9 https://www.edps.europa.eu/sites/default/files/publication/06-10-13_lpc_en.pdf.

[232] Case C-291/12 *Schwarz* ECLI:EU:C:2013:401, Opinion of AG Mengozzi, para 52.

[233] Case C-291/12 Case C-291/12 *Schwarz* ECLI:EU:C:2013:670.

[234] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C:2024:251, para 107.

[235] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020), 67 (text in brackets added for clarification by the author of this thesis).

[236] E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3) Computer Law & Security Review, 6, doi: 10.1016/j.clsr.2017.11.004.

The author of this thesis is of the opinion that the key to understanding biometric data lies in the careful reading of Recital 51, particularly how it implicitly refers to biometric data. In this regard, the crucial sentence of Recital 51 GDPR states:

> The processing of photographs should not systematically be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

In other words, photographs are among sensitive personal data only when they are also biometric data used for either identification or verification. Therefore, Recital 51 implies that there is one definition of biometric data, and that this one concept of biometric data is sensitive personal data and covers both identification and verification. In other words, Articles 4 and 9 must be read jointly as referring to one single concept of biometric data, as is understood in Recital 51.

The arguments of a substantial number of legal scholars as well as authoritative bodies have been analysed above. These arguments investigate the legislative history of the GDPR to uncover the intentions of the stakeholders and use methods of textual interpretation to reveal the meaning of relevant GDPR provisions. Both positions, that Article 4 and 9 either represent different or the same concept of biometric data, can be well substantiated. To show the confusion of the legislator in approaching biometric data, it is sufficient to point out that whatever stance one takes, it leads to a paradox. If one considers that the biometric data of Article 9 are a separate definition, then the Article 4(14) definition has no effect. This would deprive meaning to biometric verification, as such processing of personal data would not be distinguished from any other processing of "ordinary" personal data. This goes against the intention of the legislators, who wanted to raise biometric data from personal data by giving them a different definition and goes against the interpreting provisions so that they have a legal effect, since the general definition of biometric data would be wholly redundant. However, if one takes the approach that Articles 4 and 9 should be understood together, then the addition in Article 9 of biometric data for the purpose of (unique) identification does not add up to anything. However, one can understand "unique identification" as an umbrella term that covers both the confirming of unique identification (biometric verification) and allowing unique identification (biometric identification). With that understanding, the Article 9 definition of biometric data can be understood as having equal scope to the Article 4(14) definition of biometric data. This

author considers that biometric data under Articles 4 and 9 is the same and that consequently, all biometric data must be processed on the legal bases provided in Article 9(2). All biometric data are sensitive personal data, whether used for verification or identification.

The AI Act has only added to the confusion. It states explicitly that biometric data "constitutes a special category of personal data".[237] Unfortunately, the following is added: "Biometric data can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons".[238] This addition is contrary to the GDPR's concept of biometric data, which does not include categorisation. It seems that in the drafting of both the AI Act and the GDPR what was missing was a view that would consider all provisions concerning biometrics together. Instead, here and there a certain reference is made to biometrics according to a particular interest, which creates an incoherent whole. The legislator and the Court (as will be seen in the recent case of *RL v Wiesbaden*) do not clearly comprehend the confusion created by the potential of having two different concepts of biometric data regulated by different rules. In the same legislative act and judgment, reference to biometric data is given in one place where a distinction is made, and in another place where all biometric data are considered as sensitive, without the contradiction being grasped.

2.4.7. Concluding Remarks on the Definition of Biometric Data

For information to be biometric data in the sense of the GDPR, four elements are needed: it needs to be personal data (usually unproblematic); it needs to be processed in a specific technical manner; it needs to concern certain human characteristics; and it needs to be done for the purpose of biometric recognition.

The above analysis of the elements making up the definition of biometric data demonstrates that the definition can be better understood but also improved. The purpose of allowing and confirming identification should be replaced with the more precise term of the purpose of biometric recognition. This would have the same meaning but would avoid confusion as to whether the current definition relates to both identification and verification. The improved definition, without changing its current meaning, could be that biometric data are personal data resulting from biometric recognition (verification and identification) relating to the behavioural and biological characteristics of a natural person. A question remains about whether biometric

[237] Regulation (EU) 2024/1689, Recital 54
[238] ibid, Recital 14.

data should also include photographs and videos even if they are nominally not used for that purpose. But this is a *lege ferenda* question that depends on a policy choice.

Then there are changes that could be made to improve the definition of biometric data in the sense that the definition changes its scope. Biometric categorisation could be included in the concept of biometric data, but this would require a significant overhaul of the current definition. It would have to go beyond the meaning of biometric recognition. It must be said that the reasons for the narrow definition of biometric data are sound. If biometric data are given higher standards of protection than ordinary personal data and if most photographs or video recordings are considered biometric data, this would turn the GDPR on its head. On the other hand, there are good reasons to argue that indeed any photograph of a person from which we could identify a person (especially by using readily available AI tools) should be biometric data, whatever the purpose might have been when the photograph was taken and stored. It is nevertheless hard to envisage the consequences if this strict approach to videos and photographs were adopted. These questions are outside the legal sphere.

To summarise, the position taken in this thesis is that both biometric identification and verification should be considered as operations of the processing of biometric data and have the legal basis for processing in Article 9(2) GDPR.[239] Biometric categorisation is regulated as the processing of ordinary personal data, unless it processes special categories of personal data, for example a biometric system which categorises persons based on their ethnicity or religious beliefs.

2.5. Processing of Biometric Data: The Rule or the Exception?

Article 9(1) defines special categories of personal data and prohibits their processing. Article 9(2) GDPR contains ten "sweeping"[240] exceptions to this prohibition of processing biometric and other sensitive data. Thus, Article 9(2) effectively enables the use of biometrics in the context of EU biometric law. These exceptions are not only numerous, but some of them are also broad, meaning that many uses of biometrics could be justified under one of these "exceptional" legal grounds for processing special categories of personal data. The effect of

[239] See corresponding Directive (EU) 2016/680 provision of Article 10 in the case of processing for law enforcement purposes. See also Article 10 of Regulation (EU) 2018/1725, which applies for the processing of personal data by EU bodies.

[240] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020) 66.

Article 9(2) is to allow the processing of biometric data. It could thus be argued that the exceptions listed in Article 9(2) are the rule here, meaning that EU biometric law permits rather than prohibits the use of biometrics.

Both the GDPR and its predecessor, the Data Protection Directive (DPD), included a provision defining special categories of personal data and the exceptional legal bases for the processing of such sensitive data. The GDPR defined biometric data for the first time, but it also added two completely new legal bases allowing the processing of special categories of personal data. One is processing for reasons of public health and the other for scientific research, archiving in the public interest and for scientific or historical research. In comparison to the DPD, the GDPR also refined several other legal bases for sensitive data processing.[241] Broadly put, the GDPR did not dramatically change the scope of processing sensitive data, but neither did it make the processing of sensitive data more restrictive.

It is important to stress that to process biometric data, the data controller must also satisfy the legal basis for the (general) processing of personal data. These legal bases are enumerated in Article 6 GDPR. Article 6 provides the legal bases for processing personal data (in general) while Article 9 provides for exceptional legal bases, allowing for the processing of sensitive personal data. This is important because, as will be shown in the example of the case concerning Clearview AI, the data controller may fail even to cross the first hurdle of Article 6 to (legally) process biometric data. Article 6 and Article 9(2) must be cumulatively satisfied for the processing of sensitive data.[242]

Article 6 GDPR provides six legal bases for the processing of personal data. The first is the consent of the data subject. Then there are five bases when "processing is necessary": for the performance of a contract; for compliance with a legal obligation of the controller; to protect the vital interest of the data subject or other natural person. The sixth, final legal basis for processing of personal data of Article 6 GDPR, like the first, is particularly important. It allows for the processing of personal data for the purposes of legitimate interests pursued by the controller or by a third party. The provision adds the following rider: unless those legitimate

[241] See Figure 9.1. L Georgieva and C Kuner, "Article 9. Processing of Special Categories of Personal Data' in C Kuner et al. (eds.) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 376, ISBN 978–0–19–882649–1.

[242] Georgieva and C Kuner, "Article 9. Processing of Special Categories of Personal Data' in C Kuner et al. (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 376, ISBN 978–0–19–882649–1.

interests override the interests or fundamental rights and freedoms of the data subject which require the protection of personal data if the data subject is a child. This legal basis for the processing of personal data concerning legitimate interests (Article 6(1)(f) GDPR) is particularly important for the use of biometrics in the private sector, because it allows use if this is in the legitimate (economic) interest of a company. But this must be balanced with the fundamental rights of the data subject under Article 6, and then, with regard to biometric data, a further legal basis under Article 9(2) must be satisfied. This will be illustrated in the example of the DPA's decisions concerning Clearview AI.[243]

The GDPR's legal bases for the processing of special categories of personal data include the following cases: if there is a legal obligation of the data controller in the context of employment and social security obligations; if it concerns the vital interests of the data subject or another natural person; if the processing of sensitive data is conducted by certain non-for-profit organisations related to their members or connected persons and is not disclosed outside these organisations; if the processing of sensitive data is necessary in connection to legal claims and the judicial process; and if the processing of sensitive data is done for the purposes of preventive or occupational medicine. These are the less pertinent legal bases for the processing of biometric data given that the focus of this thesis is on biometrics applied in migration and asylum. The analysis now turns to a number of legal bases that the author considers most important in the context of biometrics.

2.5.1. Explicit Consent for the Processing of Biometric Data

Article 9(2)(a) allows the processing of biometric data[244] in the case of explicit consent given by the data subject. The key word here is "explicit", not mere consent of the data subject. Explicit consent has the effect that the data subject cannot be taken to have implicitly consented to the processing of personal data, as can be construed from the consent legal basis for the processing of "ordinary" personal data found in Article 6(1)(a) GDPR. This legal ground is particularly relevant for the processing of biometric data by the private sector. Member States may prohibit explicit consent as a legal basis.[245]

[243] See 2.9 and 2.10 of this thesis.
[244] Along with other special categories of personal data.
[245] Regulation (EU) 2016/679, Article 9(2)(a).

The EDPB recently issued an opinion on the use of facial recognition used by airport operators to ease passenger flows.[246] The Opinion states that the relevant data controllers would need to obtain explicit consent from passengers, thus reflecting the condition in Article 9(2)(a) GDPR. The opinion does not concern the processing of personal data controlled by public authorities. If airport operators and airline companies want to use biometrics to streamline passenger flows (to enable more efficient boarding) the legal basis must be the explicit consent of the passengers. It must be possible to withdraw this consent easily, without detriment to accessing certain services, ensuring that passengers who refuse do not have their faces scanned (by allowing for specific lanes with and without facial recognition). The principles of necessity and proportionality, for example, in the GDPR still apply even if passengers provide explicit consent.[247]

The legal basis for the processing of biometric data also depends on national laws. If the laws of Member States do not oblige airport operators and passenger airlines to verify the identity of passengers against their boarding passes, then any verification by biometrics should not be performed as it would be excessive and thus in breach of the data minimisation principle of Article 5(1)(c) GDPR.[248] But, in the opinion of the author of the thesis, this interpretation of the data minimisation principle is too broad. If any processing of biometrics that is not required by law is considered illegal (as being contrary to the data minimisation principle) then it would eliminate explicit consent as a possible legal basis at all – the only legal basis for processing biometric data would practically be if it is so required by law. Thus, this interpretation of the data minimisation principle in this point of the Opinion should be disregarded as it is not consistent with the rest of the GDPR. Indeed, the GDPR does allow many legal bases for the processing of biometric data other than that they are legally required. This Opinion can be regarded as relevant for any application of biometrics by data controllers from the private sector, who thus do not have the benefit of using the "substantial public interest" legal basis for the processing of biometric data as public authorities have. The problematic nature of the

[246] EDPB, Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024).

[247] ibid, point 15; EDBP, Guidelines 5/2020 on consent under Regulation 2016/679 Version 1.1 (2020) para 5.

[248] EDPB, "Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024)", point 17. Scandinavian countries are cited as an example in the Opinion as not having the obligation to verify identity when travelling between them.

explicit consent basis for the processing of biometric data is explained in this chapter using the example of the Worldcoin case.[249]

2.5.2. Biometric Data Manifestly Made Public as a Basis for Processing

This exception contained in Article 9(2)(e) GDPR is quite problematic. It allows the processing of biometric data if the data subject has made their biometric data manifestly public. It is difficult to draw the line between what is made manifestly public and what is not, particularly in the new circumstances of social networks and all the data that can be harvested (scraped) from the internet by recent AI advances. In relation to photographs, the EDPB has opined that the exception of "manifestly made public" cannot be construed from the default settings of a service by which templates are made public, or by the absence of choice.[250] This opinion was made in the context of the manifest public exception of Article 10 LED, thus in the context of law enforcement.

It is unclear exactly what the boundaries are of making one's sensitive data manifestly public. Kindt, a prolific author on the subject of biometric data, has called this exception "intriguing" without providing much further explanation.[251] In a more recent paper, Kindt was of the opinion (relegated to a footnote) that law enforcement authorities can use the manifest public exception for the processing of biometric data that data subjects publish on social media.[252] This interpretation is highly problematic. This would mean that public authorities can create biometric databases, even when there is no specific authorising law, but on the basis that natural persons have published their photographs on social media, thus making them manifestly public. This is remarkably like what Clearview AI was doing, with the only difference being that Clearview AI was selling its services to law enforcement, and thus Clearview AI could not rely on this exception since it was processing biometric data in the interest of profit, not law enforcement.

"Biometric data manifestly made public" is a problematic exception because it depends on the interpretation of the term which can create loopholes for the use of biometrics in unlikely situations, such as in the case with law enforcement biometric databases which are expanded

[249] See 2.10 of this thesis.
[250] EDPB, "Guidelines 3/2019 on processing of personal data through video devices Version 2.0" (2020), point 70.
[251] E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3) Computer Law & Security Review, 5. doi: 10.1016/j.clsr.2017.11.004.
[252] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020), footnote 19.

from the data that private persons publish on the internet without knowing that these data could be used in such a manner.[253] This exception should thus be deleted, at least as far as biometric data are concerned. This is particularly true since there is already an exception allowing the processing of biometric data in the case of the explicit consent of the data subject.

2.5.3. Substantial Public Interest of Article 9(2)(g) GDPR

This legal basis allows the processing of biometric data when it "is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".[254] This ground is of fundamental importance for the use of biometric identification by public authorities.

In the context of this thesis, Article 9(2)(g) should be seen as a crucial component of EU biometric law. The importance of this exception is recognised by the new Eurodac regulation as well.[255] The LED contains a different legal basis for the processing of special categories of personal data, by allowing it when authorised by Union or Member State law, which corresponds to the substantial public interest of Article 9(2)(g). When public authorities use biometrics (when they process biometric data), they rely primarily on Article 9(2)(g) which allows for the processing of biometric data and other special categories of personal data based on legitimate interest and substantial public interest, as the most important legal grounds for the application of biometrics concerning public authorities. The legitimate interest exception of Article 6(1)(f) and Article 9(2)(g) both contain an explicit reference to fundamental rights.

The Article 9(2)(g) conditions for the processing of sensitive personal data are that such processing is necessary for reasons of substantial public interest, that it is based on law, that it is proportionate to the aim pursued, that it respects the essence of the right to data protection, and that it provides specific measures to safeguard the fundamental rights and interests of data subjects. This is remarkably like the conditions for justifying the limitations of fundamental rights (such as privacy and data protection) which are applied in cases concerning the effects of

[253] See also a discussion on this point at 2.6.2 as well as concerning Clearview AI at 2.9 and the analysis of Regulation (EU) 2024/1689 at 2.7 which prohibits the scraping of biometric data from the web.
[254] Regulation (EU) 2016/679, Article 9(2)(g).
[255] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of "Eurodac" for the comparison of biometric data [2024] OJ L2024/1358 (Eurodac 2024 Regulation), Recital 9.

biometrics on fundamental rights, such as in *Schwarz* or *RL v Wiesbaden*. According to Article 52(1) CFR, the conditions for justifying the limitations to fundamental rights and freedoms are that such limitation is provided by law, that it respects the essence of those rights and freedoms, and that such limitation is subjected to the principle of proportionality. In this way, the data protection laws of the GDPR and the fundamental rights legal framework are intertwined in the application of biometrics. EU biometric law thus inescapably requires respect simultaneously for the data protection and the fundamental rights legal frameworks. Concerning special categories of personal data, exceptions to the general prohibition of the processing of special categories must be interpreted restrictively.[256]

Article 9(2)(g) GDPR also shows similarities with Article 8 ECHR, which justifies interference with privacy by public authority if it is in accordance with the law, necessary in a democratic society and in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The CFR states that the meaning and the scope of the Charter corresponds to the ECHR when concerning the same rights,[257] which means that privacy (and data protection) as fundamental rights correspond to the notion of privacy in Article 8 ECHR. The right to privacy contained in Article 8 ECHR states that interference by public authorities must be based upon law, "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Both the GDPR and ECHR see biometrics as an infringement of privacy (and data protection) that can be justified only by a proportionality test. It is not surprising then that some of the crucial CJEU judgments concerning biometrics, such as *Schwarz*, refer to the most important ECtHR judgment on the matter of biometrics, the *Marper* judgment.[258] The proportionality tests which examine the effects on human or fundamental rights of privacy look remarkably similar.

---

[256] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251 para 35; Georgieva and C Kuner "Article 9. Processing of Special Categories of Personal Data" in C Kuner et al. (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020) 375, ISBN 978–0–19–882649–1.

[257] Charter of Fundamental Rights of the European Union [2012] OJ C326/393 (CFR), Recital 9.

[258] See 3.2 of this thesis.

Border control, migration purposes and asylum applications are areas where the legal basis of "substantial public interest" for the processing of biometric data is applied.[259] In the context of law enforcement, it is enough that the processing of biometric data is authorised by law, is strictly necessary, and is subject to appropriate safeguards for the rights and freedoms of data subjects.[260] The AI Act stipulates that the use of real time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement should only be used in narrowly defined situations, where the use is strictly necessary to achieve a "substantial public interest".[261]

In conclusion, Article 9(2)(g) connects the GDPR data protection framework and the human and fundamental rights frameworks concerning the use of biometrics by public authorities. These "double legal frameworks and the double necessity and proportionality test"[262] can thus also be considered a key feature of EU biometric law.

2.5.4. Article 9(4) GDPR: National Laws May Further Regulate the Processing of Biometric Data.

National legislation may set additional conditions and limitations for the processing of biometric data. This possibility is provided by Article 9(4) GDPR, which states that Member States may have further limitations on the processing of biometric data, genetic data or data relating to health. Article 9(4) is thus a strong indicator of the EU legislator recognising the sensitivity of biometric (and genetic) data. Certain authors advocate that Member States should introduce more restrictive laws on biometrics than provided by the GDPR.[263]

One example is the Croatian biometric legislation based on Article 9(4). Croatian legislation stipulates that public authorities may process biometric data if it is so stipulated by law and if it is necessary for the protection of persons, property, classified data or business secrets and if the interests of data subjects which may be contrary to the processing of biometric data do not

[259] E Kindt, "Biometric Data Processing: Is the Legislator Keeping Up or Just Keeping Up Appearances" in G González, R Van Brakel, and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (Elgar, 2022) 395.
[260] Directive (EU) 2016/680, Article 10.
[261] Regulation (EU) 2024/1689, Recital 33.
[262] E Kindt, "Biometric Data Processing: Is the Legislator Keeping Up or Just Keeping Up Appearances" in G González, R Van Brakel, and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (Elgar, 2022) 389.
[263] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity, 193–217, https://doi.org/10.3233/IP-211525.

prevail.[264] It is assumed that the processing of biometric data is stipulated by law if it is necessary for the fulfilment of obligations from international agreements in connection with the identification of an individual when crossing the state border.[265]

The processing of biometric data in the private sector is allowed only if it is prescribed by Croatian law or if it is necessary for the protection of persons, property, classified data, business secrets or for the individual and secure identification of consumers of services if the interests of those consumers not to have their biometric data processed do not prevail.[266] The legal basis for the processing of biometric data for the secure identification of users of services is the explicit consent of data subjects in accordance with the GDPR.[267] In Croatia, it is further permitted to process biometric data for the purpose of recording working hours and for recording the entering and exiting of official premises if it is prescribed by law or if the employee has given explicit consent in accordance with the GDPR.[268] The obligation to carry out a Data Protection Impact Assessment (DPIA) is not affected by the provisions of Croatian legislation on the processing of biometric data.[269] The Croatian Act on the Application of the GDPR excludes its application in areas of defence, national security and the security-intelligence apparatus.[270]

Interestingly, Croatian legislation limits the scope of its national provisions on the processing of biometric data concerning the private sector to data subjects in Croatia if processing is conducted by the data controller established in Croatia or a body of public authority.[271] This could mean that if an international company processes the biometric data of Croatian citizens, but is neither established in Croatia nor provides its services in Croatia, specific provisions concerning biometric data processing in Croatia would not apply. This would be the case with businesses such as Clearview AI, as they are not established in Croatia nor do they offer services to Croatian companies, but they do process publicly available photographs and other personal data of Croatian citizens (and everyone else). Nevertheless, the provisions of the GDPR would apply in such a case of the non-application of Croatian biometric legislation. In addition to the

[264] Zakon o provedbi Opće uredbe o zaštiti podataka NN 42/2018 (Croatian Act on the Implementation of the GDPR), Article 21(1).
[265] ibid, Article 21(2).
[266] ibid, Article 22.
[267] ibid, Article 22(2).
[268] ibid, Article 23.
[269] ibid, Article 24(2).
[270] ibid, Article 24(3).
[271] ibid, Article 24.

provisions of the Croatian Act on the Application of the GDPR, provisions concerning the processing of biometric data are contained in the Croatian Act on the Processing of Biometric Data[272] and the Ordinance on the Processing of Biometric Data.[273]

2.6. LED and EUDPR as Parts of EU General Biometric Law

The GDPR is the most important legislative act which concerns data protection in the EU and, particularly, which regulates the processing of biometric data as well. Nevertheless, there are a few other pieces of EU legislation which also define biometric data and set conditions for processing in their respective areas. The European Data Protection Regulation (EUDPR)[274] is applied for the processing of biometric data by the Union institutions, bodies, offices, and agencies, while the Law Enforcement Directive (LED) is applied for the processing of biometric data for the purposes of law enforcement. The analysis of the definition of biometric data and other considerations are applicable here as well. This is why only a short overview of the specifics of the EUDPR and LED will be provided here.

2.6.1. The European Data Protection Regulation

The EUDPR applies to the processing of personal data by all Union institutions, bodies, offices, and agencies. In that regard, the EUDPR takes precedence over the GDPR concerning the processing of biometric data within its scope. The purpose of the EUDPR is to protect the personal data of natural persons and to ensure free movement of personal data within the Union in the fields of judicial cooperation in criminal matters and police cooperation.[275]

The EUDPR greatly resembles the GDPR in its layout, defining the legal bases for the processing, rights, and principles of data protection in a comparable manner. The EUDPR does not apply to the processing of personal data concerning TFEU-defined areas of judicial cooperation in criminal matters and police cooperation (this concerns so-called operational personal data).[276] The EUDPR should be interpreted homogenously with the GDPR.[277] When

[272] Zakon o obradi biometrijskih podataka NN 127/19 (Croatian Act on the Processing of Biometric Data).
[273] Pravilnik o obradi biometrijskih podataka NN 122/2020 (Croatian Ordinance on the Processing of Biometrics Data).
[274] Regulation (EU) 2018/1725.
[275] ibid, Recital 3.
[276] ibid, Articles 2 and 3.
[277] ibid, Recital 5.

it concerns operational personal data, the EUDPR should be interpreted consistently with the LED.[278] The EUDPR defines biometric data in the same way as the GDPR (and the LED).

2.6.2. Law Enforcement Directive and Processing of Biometric Data

The GDPR excludes from its scope the processing of personal data by "competent authorities for the purposes related to criminal offences or criminal penalties, including threats to public security".[279] As the name suggests, the LED is a directive. It needs to be transposed by national legislation, unlike either the GDPR or the EUDPR. This makes sense especially if one has in mind that the scope of the LED is related to law enforcement, an area of law which is closely tied to national sovereignty and national security. A significant difference from the GDPR is that the LED does not contain a general prohibition of processing of biometric data (and other sensitive personal data) as is specified in Article 9(2) GDPR. The LED allows the processing of sensitive data only if it is strictly necessary and if there are appropriate safeguards for the rights and freedoms of the data subject. In addition, one of three conditions must be true. First, that the processing of sensitive data (for the purpose of law enforcement) is prescribed by national legislation. Second, the processing is done to protect the vital interests of the data subject or another natural person. Or, thirdly, the (biometric) data have been made manifestly public by the data subject. It was rightly noted that in the last two exceptions no specific national law is necessary,[280] thus, for example, biometric identification under the LED could be conducted without a specific national law.

This last legal basis concerning biometric data made manifestly public by the data subject in the LED context is particularly problematic, as was already pointed out concerning "manifestly made public" in the application of the GDPR.[281] It could allow law enforcement authorities to create biometric databases containing sensitive data of millions of natural persons if those persons have published photographs online. Police may be allowed to conduct web scraping even if private entities such as Clearview AI are not (as well be explained below). The EDPB believed this exception should not apply to photographs published on social media in the

[278] ibid, Recital 10.
[279] Regulation (EU) 2016/679, Article 2(2)(d).
[280] E Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020), footnote 19.
[281] See 2.5.2 of the thesis.

context of facial recognition and law enforcement.[282] As explained in the analysis of biometric aspects of the AI Act, the AI Act prohibits web scraping.[283]

Nevertheless, this exception opens the question of what kind of circumstances could be taken as meaning that the data subject has made their personal data manifestly public. The EDPB suggests that this would be the case if the data subject made public not only the facial image, but the biometric template.[284] This is unconvincing for three reasons. First, it would require technical knowledge of a natural person to be aware of the distinction between a photograph and a biometric template of a photograph and then intentionally make the biometric template public. This cannot be expected. Second, there is no imaginable motivation why a person would manifestly make their biometric template public to law enforcement (would a person be aware of the consequences?). Thirdly, on what basis can a biometric template be made manifestly public while a photograph cannot? The exception that allows the processing of publicly available biometric data for law enforcement should be deleted. It produces uncomfortable results for fundamental rights by allowing public authorities to scrape the internet and create biometric databases. Cases C-205/21 and C-118/22, which concern the LED and the processing of biometric data, are analysed in sections 3.2.5 and 3.2.6 of this thesis.

2.7. The AI Act: Biometric Lex Specialis?

The AI Act is a regulation of the European Union for the harmonisation of rules on artificial intelligence.[285] In this part of the thesis, the author provides a critical analysis of the AI Act's relation to biometrics, and more specifically the place of the AI Act in relation to EU biometric law. This part provides an overview of the biometric terminology used in the AI Act and how it could be improved. There is an analysis of how the most prominent biometric technologies are regulated and the relationship between the AI Act and other general biometric legislations, namely the GDPR and the LED.

The AI Act devotes significant space to defining biometric concepts. Some of these concepts are already defined in other pieces of legislation, such as in the GDPR. However, the AI Act introduces concepts that were not defined in other EU legal provisions, such as biometric

[282] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (2022), point 76.
[283] See 5(1)(e) Regulation (EU) 2024/1689.
[284] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (2022), point 75.
[285] Regulation (EU) 2024/1689.

categorisation. The AI Act is often surprising in the way it approaches biometric concepts, in its interesting relationship with the GDPR in relation to biometric data, but also in the number of times it refers to different biometric concepts.

2.7.1. The AI System and Biometric Data as in the AI Act: Novelties in EU Biometric Law

The basic concept that the AI Act uses is the AI system. This is defined as a:

> machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[286]

In the opinion of this author, the definition of an AI (system) is the weakest point of the whole of the AI Act. To regulate AI, it is first necessary to define it. However, defining AI usefully is a difficult task.[287] This is because what artificial intelligence and what intelligence are is not universally established. These are philosophical questions on how to distinguish between humans and machines, what it means to be human, and how to measure intelligence. The definition in the AI Act is vague, even with these insights in mind. The AI Act defines an AI system as something that is machine-based and that infers.[288] Recital 12 explains the notion of inferring as "the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data". Outputs, predictions, recommendations, or decisions, which influence either physical or virtual environments, is a very open-ended definition. It is clear that the legislator fears that any

[286] Regulation (EU) 2024/1689, Article 3(1).

[287] For a recent view on the notion of AI in Regulation (EU) 2024/1689, see European Law Institute Guidelines on the Application of the Definition of an AI System in the AI Act: ELI Proposal for a Three-Factor Approach Response of the ELI to the EU Commission's Consultation (2024). In the opinion of this author, the proposed three factor approach in the paper still does not manage to remedy the lack of precision in the definition of AI in Regulation (EU) 2024/1689. For example, it is not clear whether an Excel sheet with certain operations defined on it would be considered an AI system or not, considering the definition of AI in this legislation. On the one hand, the legislator did not have Excel sheets or the Word virtual assistant Clippy (the paperclip) as AI. On the other hand, an Excel sheet which contains an algorithm and executes results according to inputs may well be considered AI, as there is nothing in Recital 12 or Article 3(1) of the AI Act that would exclude computer programmes from being considered AI, even if these programmes or similar algorithms may not be what anyone had in mind when contemplating the regulation of AI.

[288] Regulation (EU) 2024/1689, Article 3(1) and Recital 12.

precision in the definition would lead to the AI Act being a source of ridicule as soon as the latest innovation from Silicon Valley, or even from China, appears. After all, the AI Act was derailed by the appearance of ChatGPT,[289] and would have designated ChatGPT as a harmless chatbot according to earlier drafts of the AI Act. The remainder of the definition of AI says that an AI system may (and thus, may not) exhibit adaptiveness after deployment, and that likewise it has varying levels of autonomy, all of which excludes nothing, as it includes adaptive and nonadaptive systems which have or may not have autonomy. The machine-based part of the definition of an AI system is straightforward enough because it excludes biological life from being considered AI. The key concept, as the AI Act pronounces, is the ability of the AI system to infer.[290] The AI Act explains that that to infer "transcends" basic data processing by enabling learning, reasoning, or modelling.[291] But what is "basic" data processing, and what, in a legal sense, is "learning, reasoning or modelling?" It is clear that this verbosity (to infer means three other concepts which all have vague and broad meanings themselves) is due to the lack of a simple idea to define artificial intelligence. There are many scientific understandings of what AI is – it may be defined as something that imitates human performance, or otherwise something that acts rationally (it makes the right choices). AI can be approached as a thought process or as the external characterisation of a behaviour.[292] It is questionable whether there was a need for an act to regulate AI in all its diverse applications, especially since AI is a broad and developing concept.

The problems of defining an AI system can be seen in the AI Act when it comes to biometrics. For example, fingerprint recognition may not be considered an AI system, especially since its roots go back to the 19th century. If AI is understood as the capacity to resolve human tasks or to emulate human intelligence,[293] then a fingerprint machine is not AI, because humans cannot identify persons by their fingerprints. In the sense of the AI Act however, a fingerprint identification system is AI, because biometric identification and verification systems are counted among AI systems. It is easiest to disregard the discussion on the general notion of AI

[289] "Initially proposed in 2021, the legislative process faced a notable disruption when OpenAI's ChatGPT was launched on 30 November 2022. This required a change to the draft text, creating specific regulations for generative AI. In its final version, the AI Act also imposes transparency obligations and certain restrictions on the use of general-purpose AI models such as GenAI" https://gchumanrights.org/gc-preparedness/preparedness-economic-social-and-cultural-rights/article-detail/how-is-chatgpt-regulated-by-the-eu-ai-act-reflections-on-higher-education.html.

[290] Regulation (EU) 2024/1689, Recital 12.

[291] Transcendence is likewise an expression that is rarely used in legal documents.

[292] S Russell and P Norvig, A*rtificial Intelligence: A Modern Approach* (4th Edition, Global Edition, Pearson, 2022) 19.

[293] This is what a chatbot such as ChatGPT answers when prompted by the question what is AI?

and take it for granted that biometric identification, verification and categorisation systems are AI systems, because they are in the AI Act in one of the risk categories. In this way, the AI Act redefines long-existing technologies or systems as AI systems.

The AI Act defines biometric data by repeating the first part of the definition from Article 4(14) GDPR, but leaving out the part that states that biometric data allow or confirm unique identification.[294] The AI Act adds in its recitals that biometric data should be interpreted in light of the meaning of this concept in the GDPR, LED[295] and EUDPR, but it goes on to add that biometric data can allow for the authentication, identification or categorisation of natural persons and for recognition of the emotions of natural persons.[296] This second statement is actually contrary to the GDPR definition of biometric data, which in the GDPR is narrow and does not include biometric categorisation. This is because categorisation does not allow or confirm unique identification (biometric verification confirms identification, while biometric identification allows unique identification). In other words, the AI Act has a broader definition of biometric data, which also includes biometric categorisation, even though the AI Act is not primarily concerned with the processing of biometric data. This may indicate that there is growing understanding of biometrics from the side of EU legislation. This may indicate that the data protection framework will be enriched with more sophisticated biometric concepts in its future evolution.

The AI Act has more to say on the matter of biometric data. It adds that biometric data is a special category of personal data.[297] The GDPR, as explained earlier, states that biometric data used for the purpose of identification is among the special categories of personal data. This manoeuvre in the AI Act is unusual. First, it may signal that the legislator wants to affirm that any sort of biometric data, whether used for identification, verification or even categorisation, is sensitive personal data, thereby influencing the interpretation of biometric data in the GDPR. The position that any sort of biometric data is sensitive is shared by this author, as explained above.[298] However, this definition of biometric data in the AI Act which diverges from the same concept in the GDPR may also indicate the confusion of the legislator, who still does not recognise that there are conflicting interpretations of biometric data. The AI Act on multiple

[294] Regulation (EU) 2024/1689, Article 3(34).
[295] ibid, Recital 94 states that the processing of biometric data for biometric identification in law enforcement needs to comply with Article 10 LED and the LED principles of Article 4(1).
[296] Regulation (EU) 2024/1689, Recital 14.
[297] ibid, Recital 54.
[298] See 2.4.7 for the position of the author of the thesis on this subject.

occasions stresses that biometric verification is not high risk,[299] or that it has only a minor impact on fundamental rights,[300] which is contrary to the statement in the AI Act, mentioned above, that all biometric data are sensitive data. Furthermore, the AI Act also continues to mix up the terms verification and authentication, which is a traditional feature of EU biometric law which fails to consistently use only the term verification.[301]

2.7.2. The Biometric Categorisation System of the AI Act: A True Novelty in EU Biometric Law

The AI Act cuts through the Gordian knot of how to deal with biometric categorisation by explicitly including it in its definition of biometric data. The inclusion has created a rift in EU biometric law, because now there are differing concepts of what biometric data are in two major EU legislative acts – the AI Act and the GDPR.

The AI Act also defines a biometric categorisation *system* as an AI system which assigns natural persons to specific categories, importantly adding that it does so based on their biometric data.[302] This addition is significant because categorisation does not need to be conducted based on biometric data.[303] Persons can be categorised based on their skin colour deduced from a photograph. A photograph, according to Recital 50 GDPR (as already analysed in detail) is not biometric data, unless it is processed in a specific manner for a specific purpose. Similarly, people can be categorised based on whether they wear a head cover or not, or other personal data retrieved from visual, audio, or written sources. This information is not biometric data in the sense of GDPR. Thus, one can conclude that the AI Act considers all types of biometric categorisation to necessarily involve the processing of biometric data. The other interpretation is that the AI Act regulates only a narrow subset of biometric categorisation – only that which involves the processing of biometric data. In either case, it is a different and novel approach when compared to any other EU legislation which regulates biometrics, such as the GDPR or LED. This is because the AI Act is the only one that defines biometric categorisation, while the

[299] Regulation (EU) 2024/1689, Recital 54.
[300] ibid, Recital 17.
[301] See ibid, Recitals 14, 54 and 17 and Article 3(34), on how these refer to authentication as a subset of verification, while the proper understanding would be to stop using the deprecated term authentication and use only verification, as was explained in 1.7.2.
[302] Regulation (EU) 2024/1689, Article 3(40).
[303] Biometric categorisation was explained in Chapter 1 concerning Biometric Terminology as well as when the definition of biometric data from the GDPR has been considered here in Chapter 2.

GDPR and LED consider biometric categorisation nothing more than the processing of personal data (unless it concerns the processing of special categories of personal data).

Biometric categorisation systems that categorise persons according to sensitive personal data are either high-risk or prohibited by the AI Act.[304] Biometric categorisation systems that categorise persons based on their biometric data in order to deduce race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation are prohibited, except for law enforcement.[305] Because of the unnecessarily complicated addition of biometric data in the definition of biometric categorisation systems, it is not clear to this author whether the prohibition of categorisation on the basis of special categories of personal data applies if it is not conducted on the basis of biometric data, but on the basis of personal data. For example, it is possible for persons to be categorised based on their clothes, hairstyles, the way they walk or talk – these data are not biometric data in the sense of the GDPR but are only personal data. Recital 30 of the AI Act is there to make it clearer, but it only reveals the lack of knowledge of the legislator since it confuses biometric data with biometric characteristics, by referring to a person's face as an example of biometric data. The face of a person is not biometric data but a biometric characteristic, as explained in this thesis concerning biometric terminology.[306]

There is an additional element in the definition of a biometric categorisation system in the AI Act, which excludes systems which are "purely ancillary to another commercial service and strictly necessary for objective technical reasons".[307] It is clear that the legislator wanted to exclude services that help consumers make purchase decisions,[308] such as virtually trying on sunglasses based on one's (categorisation of) head shape. One can also imagine that social networks and mobile applications may offer facial filters or similar tools that may be counted as biometric (categorisation), and that the legislator sought to exclude such biometric categorisation systems from the scope of the AI Act. This was not a good decision. First, the criterion of "purely ancillary" is vague, which makes the application of these provisions more complicated. Besides, an AI system which uses biometrics for purely ancillary or trivial purposes should not be excluded from the obligations that the AI Act imposes. Instead, the

[304] Regulation (EU) 2024/1689, Recital 54.
[305] ibid, Article 5(1)(g) and Recital 30.
[306] See 1.7.2 of the thesis.
[307] Regulation (EU) 2024/1689, Recital 16 and Article 3(40).
[308] ibid, Recital 16.

triviality (the commercial interests of social networks) should be all the more reason to submit it to regulation, as those systems infringe privacy for trifling purposes. It would be better to prohibit trivial biometric categorisation than to deregulate it.

2.7.3. An Emotion Recognition System: Another Type of Biometric Categorisation

The AI Act introduces the concept of an emotion recognition system, which serves to identify the emotions of a person on the basis of their biometric data.[309] The AI Act prohibits their use in the context of workplace or education, except for medical purposes,[310] otherwise emotion recognition systems are deemed as high risk.[311] In the opinion of this author, this concept was from a legal standpoint wholly unnecessary. Emotion recognition should be regarded as a subset of biometric categorisation, since emotion recognition entails a categorisation of persons based on their facial expression. Such systems do not in fact recognise emotions (setting aside whether emotions exist and how are they expressed in our minds or brains) but instead estimate facial expressions. Certain facial expressions are associated with certain emotions. From that the system deduces whether a person is being truthful. The number of implied assumptions obviously makes for an unusable system in terms of accuracy.

The purpose of having emotion recognition defined and then restricted in the AI Act seems to be more political than motivated by concern for fundamental rights. Namely, emotion recognition is of little use since different individuals and diverse cultures express emotions differently.[312] People may also be reluctant to display their emotions before an "emotion detector" on the border in the same manner as they express their emotions in other circumstances. The EU has spent millions of euros on a project called iBorderCtrl although the project shows that an AI machine can guess the emotions of a person with accuracy only somewhat better than a coin flip, making the technology unreliable.[313] Thus, the prohibition of emotion recognition in the AI Act has no practical effect since emotion recognition is practically useless, but it may achieve the political purpose of sending a message of European values which the AI Act bravely defends by prohibiting emotion recognition.

---

[309] ibid, Article 3(39).
[310] ibid, Article 5(1)(f).
[311] ibid, Annex III(1)(c).
[312] ibid, Recital 44.
[313] The supposed accuracy of this system is about 75%: European Parliament, Parliamentary question, 005624/2018 https://www.europarl.europa.eu/doceo/document/E-8-2018-005624_EN.html.
But even this metric can be easily called into question as too high: "Why Most Published iBorderCtrl Research Findings Are Likely to Be False" https://iborderctrl.no/blog:ioannides.

2.7.4. Biometric Identification in the AI Act

The AI Act devotes many of its pages to biometric identification, biometric identification systems and different subtypes, such as real time remote biometric identification. The AI Act defines biometric identification as:

> automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database.[314]

A key distinction of biometric identification according to the definition in the AI Act is the use of a database.[315] Biometric identification presumes the identification of one person from many persons in a database.[316] The GDPR does not include a definition of biometric identification, even though its definition of biometric data refers to allowing unique identification, which is to be understood as biometric identification. Automated recognition, used to define biometric identification in the AI Act, is indeed a better term than specific technical processing, which is mentioned in the GDPR's definition of biometric data. This is because automated recognition is more aligned with the similar and related concept of automated decision-making in the GDPR (and the AI Act) and thus keeps the terminology simpler. Further, the trinity of "physical, physiological or behavioural" characteristics mentioned in the GDPR for biometric data has increased to four in the definition of biometric identification in the AI Act with the addition of "psychological" human features. As explained in the discussion of characteristics in the definition of biometric data,[317] a better solution would be to refer to only two characteristics or human features: behavioural and biological, to align with the ISO biometric vocabulary.

---

[314] Art 3(35) Regulation (EU) 2024/1689. The definition in Recital 15 is even more detailed: "The notion of 'biometric identification' referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises".

[315] Article 3(35) Regulation (EU) 2024/1689.

[316] For a more nuanced view according to which the difference between verification and identification is not absolutely clear, see 1.7.2 of the thesis.

[317] See the analysis of the concept of biometric data in 2.4 of this thesis.

All biometric systems, including those for identification, categorisation and emotion recognition, are deemed high-risk, except biometric verification systems.[318] Biometric identification systems are deemed by the AI Act to have significant consequences in the event of an incorrect match,[319] and thus are additionally burdened by the requirement that no action or decision is taken on the basis of biometric identification until it is confirmed by at least two natural persons with necessary competences.[320]

2.7.5. A Real-Time Remote Biometric Identification System

One of the most contentious points of AI Act was the issue of live surveillance of public areas with cameras that can instantly identify the faces of persons. The AI Act defines this as real-time remote biometric identification. This technology is obviously egregious for human rights, in particular privacy, human dignity, and non-discrimination. Such biometric surveillance of public areas was deemed contrary to the right to private life under Article 8 ECHR in the case *R (Bridges) v the Chief Constable of South Wales Police*, decided before the ECtHR.[321] The CJEU decided in *Quadrature du Net* that the real-time collection of sensitive data is more problematic than non-real time access to the same data.[322]

The AI Act defines the real-time remote biometric identification system as an AI system that is intended for the identification of natural persons without their active involvement, typically at a distance, by comparing biometric data captured with the biometric data stored in a database.[323] Multiple persons are simultaneously identified without their active involvement.[324] Real-time means that live material is used, such as live video footage.[325] This is opposed, for example, to a biometric identification system that uses fingerprints stored previously on an identity card to conduct biometric recognition.

Real-time remote biometric identification presents a new, exceptionally high threat for human rights. Unlike at a border crossing, a person here may not be aware that they are the target of biometric identification in a public space. Further, this type of surveillance is applied to the

[318] Regulation (EU) 2024/1689, Annex III, point 1. As mentioned, certain purely ancillary biometric categorisation systems are not high risk.
[319] Regulation (EU) 2024/1689, Recital 73.
[320] ibid, Article 14(5).
[321] *R (Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
[322] Joined Cases C-511/18 *Quadrature du Net* ECLI:EU:C:2020:791, paras 187-189.
[323] Regulation (EU) 2024/1689, Article 3(41)-(42).
[324] ibid, Recital 17.
[325] ibid, Recital 17.

general population (anybody walking on a certain street) instead of targeted at persons who are apprehended in an irregular border crossing or suspected of a crime. Thus, it is questionable whether any application of such an AI system could be justified in a fundamental and human rights analysis. The AI Act attempts to remove the doubt by providing detailed conditions for its use.

The AI Act recognises the problems that real-time remote biometric identification poses and considers it as being particularly intrusive on a person's rights and freedoms because these systems evoke a sense of constant surveillance[326] and indirectly discourage the exercise of the freedom of assembly and other fundamental rights.[327] To dissuade persons from exercising their fundamental rights is known as the chilling effect, whereby persons are reluctant to engage in free speech, protest or even appear in certain public spots even if the persons do not plan to engage in elicit behaviour. This was the conclusion of the ECtHR in *Glukhin v Russia*[328] in a case which concerned a facial recognition system used by the police at a metro station where biometric identification was used to suppress a protester in a public space. Further, the AI Act concedes that technical inaccuracies concerning this type of AI system can lead to bias and discrimination, in relation to age, ethnicity, race, sex or disabilities.[329] The higher risk of these systems is caused by the immediacy of their impact and the limited opportunities for correction.[330]

Despite these observations, the AI Act lists the conditions for the use of real-time remote biometric identification. These conditions make up most of Article 5 of the AI Act under the title Prohibited Practices. First, real-time remote biometric identification is allowed only for the purpose of law enforcement. Its use must be strictly necessary and should meet one of three objectives: to search for victims of certain serious crimes; to prevent an imminent threat or terrorist attack; to search for persons suspected of certain serious crimes.[331]

There are several further conditions for the deployment of real-time remote biometric identification systems. Such a system may be used "only to confirm the identity of the *specifically targeted* individual". This aim seems reasonable, but it is formulated as if it

[326] A phrase used in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238, para 37.
[327] Regulation (EU) 2024/1689, Recital 32.
[328] *Glukhin v Russia*, App. no. 11519/20 (ECtHR, 4 July 2023).
[329] ibid, para 107.
[330] ibid, para 104.
[331] Regulation (EU) 2024/1689, Article 5(1)(h).

concerns biometric verification, not identification. What the legislator most likely wanted to express is the idea that there has to be a certain limited list of individuals that are sought with this technology, perhaps a particular fugitive, a missing person or the like, and not merely that the system should compare the face of every passerby with a wanted persons database in a kind of fishing expedition.

Further elements for allowing real-time remote biometric identification are that there must be an assessment of the nature of the situation, as well as the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.[332] This can be likened to a proportionality assessment. Furthermore, such systems can only be deployed in accordance with national law. There must also be a fundamental rights impact assessment conducted prior to deployment, and the system must be registered in an EU database set up according to Article 49 of AI Act, except in cases of urgency, where the registration can be conducted post fact.

Two additional conditions for the use of real-time remote biometric identification systems are that there must be a prior authorisation of judicial or administrative authority, except in cases of "urgency".[333] The possibility to gain authorisation not only from judicial but also administrative authorities has weakened the protection against this technology. Finally, there must be notification to market surveillance authorities and national data protection authorities.[334] The EDPB and EDPS advocated a ban on the automated recognition of human features in publicly accessible spaces, but their view did not prevail in the final version.[335]

One can imagine great divergence in the application of real-time remote biometric identification between Member States. Some may prohibit such use outright, while others may have such systems put in place to be used at a moment's notice. This divergence makes it difficult to make categorical pronouncements on the impact of real-time remote biometrics on human and fundamental rights. However, once such systems become commonplace, both citizens and migrants will undoubtedly feel a certain level of unease, with a chilling effect on their fundamental rights. Carving a distinction between real-time and other types of biometric

[332] Regulation (EU) 2024/1689, Article 5(2).
[333] ibid, Article 5(3) and Recital 35.
[334] ibid, Article 5(6).
[335] 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)" (2021), 2.

surveillance has been criticised as harmful to fundamental rights by EDRi[336] and by the EDPB and EDPS in a Joint Opinion,[337] as essentially facilitating the use of these oppressive technologies.

2.7.6. The Relation of the AI Act to the GDPR and LED: Blink and You Will Miss It

The AI Act proclaims that it does not seek to change the application of existing data protection rules, primarily the GDPR.[338] It does not regulate the processing of personal data and can be viewed as product safety legislation, with the product being AI systems.[339] However, concerning the most contentious AI technology in the AI Act, namely real-time remote biometric identification, the situation is different. It should be noted that the AI Act is an incredibly long piece of legislation (twice as long as the GDPR). The provisions concerning biometrics are very prominent, with the term "biometric" being mentioned over a hundred times in different guises. Especially convoluted is Article 5 on so-called Prohibited Practices, which mostly concerns laying out the conditions for deploying real-time remote biometric identification, not prohibiting it, as the title of the Article suggests. This complexity can be attributed to many stakeholders, from the EU Parliament to the Council, with others in the background, contributing a provision or two to the AI Act without having in mind the whole of this legislation. The stitching of this legal patchwork is particularly seen when it comes to biometrics which, as has been noted, are still not understood properly by the legislator(s).

It takes more than one reading of the provisions to understand the AI Act's relation to the GDPR in view of biometrics. For example, the AI Act states that it does not act as *lex specialis* in relation to the GDPR or LED. But Recital 38 of the AI Act explains that rules that *prohibit* real-time remote biometric identification do act as *lex specialis* in relation to the LED (since this technology is only allowed for law enforcement purposes anyway). The same Recital adds that the LED cannot provide scope for the use of this technology outside the provisions of the AI

[336] European Digital Rights "European Commission adoption consultation: Artificial Intelligence Act Brussels" (2021) https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf.
[337] 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)" (2021), point 31.
[338] Recital 10 Regulation (EU) 2024/1689.
[339] See e.g. M Veale and F Zuiderveen Borgesius, "Demystifying the Draft EU Artificial Intelligence Act" arXiv:2107.03721 https://doi.org/10.48550/arXiv.2107.03721; M Almada and N Petit, "The EU AI Act: A Medley of Product Safety and Fundamental Rights?" Robert Schuman Centre for Advanced Studies, Research Paper No. 2023/59.

Act. This would mean that the AI Act narrows the scope of the use of real-time remote biometric identification, by prohibiting the LED from being interpreted in any way that would allow it, outside the conditions of the AI Act. But there is another point of view. Namely, the rules that prohibit real-time remote biometric identification in the AI Act are the rules of Article 5 (Prohibited Practices). These rules in their substance allow, and do not prohibit, real-time remote biometric identification. Therefore, one interpretation is that the AI Act precludes the LED from prohibiting real-time biometric identification because the AI Act, in its article on Prohibited Practices, allows it. If this technology were considered contrary to the LED provisions, but would satisfy the conditions of the AI Act, then the AI Act would prevail.[340]

The AI Act allows special categories of personal data (Article 9(1) GDPR) to be processed for the purpose of bias detection and correction.[341] Bias is a broader term than discrimination, the latter having a more precise legal meaning. Bias is a recognised phenomenon associated with modern technologies, algorithms, and AI. It means that certain groups of persons are not treated equally. For example, an AI system for the machine reading of job application CVs may favour male over female applicants. Bias creates a legal, ethical, and practical conundrum.[342] One solution is to hide the protected characteristics from the AI system (or, from the algorithm) so that, for example, all references to gender in a job application documentation are hidden. In terms of the provision of the AI Act above, this would mean that the AI system is precluded from processing sensitive personal data, such as race, to prevent the system from showing bias towards one group. The good side of this approach is that it limits the processing of sensitive personal data and thus protects privacy. The downside of hiding protected characteristics from the AI system is that the system can still commit bias (for example, by disfavouring CV applications that mention hobbies and achievements associated with the female gender, thus reconstructing the female bias by proxy).

The other general approach to bias is to allow the AI system to use sensitive (personal) data precisely so that the results can be adjusted to account for the bias. One example of such (affirmative) action is giving extra points to persons with disabilities in university entrance examinations. The system must be allowed to recognise and sort persons by this criterion to

[340] Other interpretations are possible, as suggested by a reading of Recital 94 and other provisions in Regulation (EU) 2024/1689. But it is clear that the legislator wanted to make an explicit point about Regulation (EU) 2024/1689 being a *lex specialis* to Directive (EU) 2016/680 in that one regard, for example be expressly using the term *lex specialis* in Recital 38.

[341] Regulation (EU) 2024/1689, Article 10(5).

[342] Bias, discrimination, and biometric algorithms are analysed in 4.4 of the thesis.

give them advantage. To correct historical bias, or bias caused by unrepresentative training data, the AI system must be aware of the sensitive data. This approach was adopted in the AI Act, which allows the processing of sensitive personal data for purposes of the correction and detection of bias, and in this regard even takes precedence over the GDPR, which generally prohibits the processing of special categories of personal data.[343] Similarly, the AI Act allows the re-use of personal data for testing, and developing AI systems in the context of so-called regulatory sandboxes.[344] In other respects, the AI Act applies in parallel with the GDPR or LED, and on multiple occasions the AI Act expresses that it is without prejudice to the GDPR or that it is additional to it.[345] This is most relevant for biometric AI systems. Facial recognition systems may be trained on data that should reflect the racial makeup of the persons on which it will be used, so that it performs equally well with female or Black faces.

Concerning the application of the AI Act and the GDPR to different AI systems, there are four combinations: that neither legislation applies (in the case of a benevolent AI system that causes minimal risk and does not process personal data); that both regulations apply (such as in the case of, for example, biometric identification or biometric categorisation systems) or that only one of those regulations applies (the French data protection authority CNIL offers an example of a power plant AI system which is high-risk, and thus the AI Act applies, but it does not process personal data, and so the GDPR does not apply).[346]

2.7.7. How Does the AI Act Work: The Risk Pyramid

The AI Act defines AI systems and then creates risk categories of these systems, or what could be seen as a risk pyramid. There are four categories: minimal risk, low risk, high risk, and unacceptable risk. Most relevant for biometrics and regulated in most detail in the AI Act are high risk AI systems and prohibited AI systems (the latter also called systems with unacceptable risk.)

High risk AI systems are listed in Annex III of the AI Act and include biometric AI systems (except biometric verification systems), emotion recognition systems, systems used in law

[343] It also applies in respect of Directive (EU) 2016/680 and Regulation (EU) 2018/1725. See Recital 70 Regulation (EU) 2024/1689.
[344] Regulation (EU) 2024/1689, Article 59.
[345] For example, Article 5(1)(h) last sentence AI Act; Article 10(5) Regulation (EU) 2024/1689; Recital 54 Regulation (EU) 2024/1689; Recital 39 Regulation (EU) 2024/1689.
[346] CNIL, Entry into force of the European AI Regulation: the first questions and answers from the CNIL (2024), https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil.

enforcement (such as polygraphs, AI systems that assess reliability of evidence, AI systems that calculate risk for committing offences). AI systems used in migration, asylum and border control management are also considered high risk,[347] and some of the mentioned systems could also be characterised (at least in part) as biometric systems (e.g. polygraphs, AI systems that assess applications for asylum, visa or residence permits, or AI tools that assess the "security" risk of an immigrant). However, AI systems which only serve to verify travel documents are not considered high risk.[348] The AI Act itself states that AI systems may exhibit bias, errors and opacity in the way they operate, which also cause risks for natural persons.[349] AI systems which are high risk according to the classification of the AI Act may nevertheless be prohibited by EU or national legislation.[350] The Commission can expand the list of high risk systems.[351] AI systems are exempted from the obligations of high risk systems if any of these conditions is true: if they perform a narrow procedural task, improve the result of a previously completed human activity, or perform a task which does not replace human assessment. However, profiling is always considered high risk.[352]

Post-remote biometric identification (used only for law enforcement and in a targeted way) additionally requires a link to a criminal offence or a search for a specific person or a genuine and present threat and is further subject to the requirements of the GDPR and LED.[353] Post-biometric identification systems are, according to the AI Act, all other biometric identification systems which are not real time.[354] Concerning scope, AI systems intended for military, defence or national security are excluded, as are AI systems and models for the sole purpose of scientific research and development.[355]

High risk AI systems, including many biometric systems, have a number of obligations tied to this status. These obligations are primarily targeted at providers and deployers of AI systems.[356] That an AI system presents a risk should be understood as a risk for the values of the EU such

[347] See the reasoning in Recital 60 Regulation (EU) 2024/1689, which mentions non-discrimination and protection of private life and personal data.
[348] Regulation (EU) 2024/1689, Annex III.
[349] ibid, Recital 61.
[350] ibid, Recital 63.
[351] ibid, Article 7.
[352] Regulation (EU) 2024/1689, Article 6(3).
[353] ibid, Article 26(10); Recital 95.
[354] ibid, Article 3(43).
[355] ibid, Article 2(3) and 2(6).
[356] ibid, Section 3.

as human dignity as well as for fundamental rights such as the right to non-discrimination, to data protection and to privacy and the rights of the child.[357] High risk may also signify a risk for the health or safety of a person.[358] High risk AI systems must establish a risk management system throughout the AI system's lifecycle. Such systems must conduct data governance, ensure training, validation, and testing, keep records, allow human oversight, and ensure accuracy, robustness, and cybersecurity.[359] Natural persons should be notified when AI systems which infer their emotions or categorise them process their biometric data.[360]

The AI Act carves out a special position for large-scale IT systems in the area of Freedom, Security and Justice.[361] These are the Schengen Information System, the Visa Information System, Eurodac, the Entry/Exit System, the European Criminal Records Information System on third-country nationals and stateless persons. The European Travel Information and Authorisation System is one among these systems that does not process biometric data. Also listed in the AI Act is the interoperability of these systems, namely the way they are connected.[362] They must comply with the AI Act after 31 December 2030, which gives them more than two years extra.[363] Otherwise, the obligations concerning high-risk AI systems apply to these systems. The risk pyramid of the AI Act is not set in stone. The Act contains mechanisms which allow the EU to change or expand the list of prohibited AI practices and certain other aspects of the Act.[364]

2.7.8. Prohibited AI Practices in the AI Act and Biometrics

At the top of the risk pyramid are AI practices that present an unacceptable risk and are thus prohibited. The AI Act prohibits the following practices: AI systems that use subliminal techniques; AI systems that target the vulnerabilities of natural persons such as their age or disability; social scoring AI systems (by which public services are tied to how well a person behaves); AI systems that calculate the risk of committing crimes but that are based solely on the characteristics of that natural person or profiling. It is clear that many, if not all, of these

[357] ibid, Recital 28.
[358] ibid, Recital 46.
[359] ibid, Article 9.
[360] ibid, Recital 132.
[361] ibid, Annex X.
[362] The biometric legal aspects of these systems and interoperability are analysed in 3.4 of the thesis.
[363] Article 111 Regulation (EU) 2024/1689.
[364] F Paolucci, "From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights" in Natalia Menéndez González and Giuseppe Mobilio (eds), *Facial Recognition Technology* (Springer, 2024) (forthcoming), https://ssrn.com/abstract=4929132.

systems could not be deployed anyway as they would seriously infringe fundamental rights or the data protection framework. For these reasons, it could be argued that prohibition of these systems in the AI Act is primarily a symbolic or political statement.

Also prohibited are AI systems that create or expand facial recognition databases, which is the practice conducted by Clearview AI, as to be explained later.[365] There is a striking loophole in this prohibition. Namely, scraping from the internet or CCTV can be done to create other types of biometric databases, including, for example, iris databases, or biometric databases that use algorithms to identify persons by the way they walk (gait), type on the keyboard, or the shape of other parts of the body besides the face. The possibilities are limitless. Therefore, it would be much better to understand facial recognition as a type of biometrics and prohibit all *biometric* databases that are made by untargeted scraping from the internet or CCTV instead of prohibiting in particular facial recognition databases.

Further prohibited in the AI Act are emotion recognition systems in the context of work or education, as already mentioned. Prohibited are also biometric categorisation systems which categorise individual natural persons based on their biometric data to determine their race, political opinion, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.[366] In other words, categorisation based on special categories of data is forbidden. The last to be mentioned, but taking most space in Article 5 of the AI Act, is the real-time remote biometric identification system, which is notionally prohibited, but the conditions for its use are laid out in the Article, as explained above.

Finally, the AI Act stipulates the right to lodge a complaint with the national market surveillance authority.[367] The Act affirms the right to an explanation of a decision regarding a high risk AI system.[368] Certain national authorities are granted the power to request and access documentation.[369] In the last analysis, the AI Act institutes what it calls a fundamental rights impact assessment, which appears to be a symbolic exercise for high risk AI systems prior to deployment.[370]

[365] See 2.9 of the thesis.
[366] Regulation (EU) 2024/1689, Article 5(1)(g).
[367] ibid, Article 85.
[368] ibid, Article 86.
[369] ibid, Article 91.
[370] ibid, Article 27.

2.8. The Council of Europe and Its Influence on EU Biometric Law

The Council of Europe (CoE) legal sources, namely Convention 108 and the ECHR (along with the case law of the ECtHR) have been influential, particularly in respect of how the definition of biometric data has developed in EU law and how biometrics are generally framed as an infringement of privacy that must be justified in a rights and interests (balancing) deliberation.

2.8.1. Convention 108: Influencing EU Biometric Law

Convention 108 was adopted in 1980 by the CoE as the first legally binding international data protection instrument concerned with the legal protection of individuals with regard to automatic data processing.[371] It has served as the foundation text for the data protection legal frameworks of dozens of CoE Member States.[372] It was adopted before the widespread use of the internet, social networks, mobile phones, not to mention the recent proliferation of AI. Thus, the fact that it is still relevant (even though it was updated in 2018 as "Convention 108+") testifies to the "technology neutral" approach to the regulation of data protection that is also the hallmark of the GDPR. Technological neutrality implies that the data protection regime is not organised around a particular technology that is being used. Instead, the focus is on the process or the outcome.[373] Convention 108 obliges States parties to implement the principles of this Convention in their domestic legislation. It is binding upon members of the CoE, which include the EU Member States. More importantly, Convention 108 served as a basis for the data protection regimes of the EU Member States.[374] In addition, it greatly influenced the EU Data Protection Directive (Directive 95/46).[375] Finally, Convention 108 and its current, updated version of 108+ closely resemble the EU law approach to biometric data, to the point that the definitions of biometric data are almost perfectly aligned. This shows the closeness of the relationship between Convention 108 and the EU biometric legal regime.

---

[371] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS, No. 108, 28 January 1981, Strasbourg (Convention 108).

[372] C de Terwangne, "Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data", Computer Law & Security Review, volume 40, 2021, 105497, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105497.

[373] P De Hert and G Bouchagiar, "Facial Recognition, Visual and Biometric Data in the US. Recent, Promising Developments to Regulate Intrusive Technologies", Brussels Privacy Hub, Working Paper 7(29)(2021b).

[374] C de Terwangne, "Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data" (2021) 40 Computer Law & Security Review, 105497, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105497, 1.

[375] E Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data" (2017) 34(3) Computer Law & Security Review, 12.

There was no definition of biometric data in the "founding texts" of personal data protection in supranational legal instruments in Europe, which were the Convention 108 of the CoE and the EU's Data Protection Directive (DPD).[376] The Consultative Committee's Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005) was also the first CoE document to define biometrics, but as "systems that use measurable, physical, or physiological characteristics or personal behaviour traits to recognize the identity or verify the claimed identity of an individual".[377]

The 2005 Report uses the terminology of verification instead of authentication, even though the deprecated term of authentication will return to be used to describe verification in the current GDPR.[378] Biometric data were not defined with any precision in the Report (even though the Report uses "biometric data" almost a hundred times) probably because it seemed self-explanatory at that time. The 2005 Report states that:

> There are different views as to whether biometric data constitute personal data. (...) The Committee finds it unnecessary to decide whether biometric data are personal data in themselves or whether this is only the case under certain circumstances. It is of the opinion that as soon as biometric data are collected with a view to automatic processing there is the possibility that these data can be related to an identified or identifiable individual. In those cases, the Convention applies.[379]

Finally, the Convention 108 Consultative Committee's Progress Draft Explanatory Report of 2013, which preceded the adoption of the modernised Convention 108 by five years, defines biometric data in the now familiar (GDPR) terms. According to the 2013 Report, biometric data are:

> data resulting from a specific technical processing of data concerning the physical, biological, or physiological characteristics of an individual which allows the unique

[376] See 2.5 of the thesis.

[377] CoE, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data" (2005) https://rm.coe.int/16806840ba. Also discussed in C Jasserand, "Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective" International Data Privacy Law (2016) 6(1), 67.

[378] The term authentication should not be used, as explained in 1.7.2 of the thesis.

[379] Council of Europe, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data (Strasbourg 2005), paragraphs 51–52.

identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject.[380]

Here, what can be seen are the building elements of the definitions of biometric data now in Article 4(14) GDPR and "biometric data for the purpose of uniquely identifying a natural person" of Article 9(1). To summarise, there was no definition of biometric data (or even any mention of biometrics) in the original Convention 108. However, as was shown, the reports issued by the Consultative Committee of Convention 108 were instrumental in forming the EU's legislation concerning biometrics.

Convention 108 was amended in 2018.[381] This modernised version is known as Convention 108+,[382] which counts biometric data for the purpose of unique identification among special categories of personal data,[383] much like Article 9(1) GDPR. Biometric data are defined in Convention 108+ in the same manner as in GDPR Article 4(14), including generally both biometric verification and identification. Convention 108 contains principles, while the GDPR sets out detailed rules. Together, these can be considered to represent a "double European data protection regime".[384]

Convention 108+ contains (almost) the same explanation concerning photographs and biometric data that is the source of confusion in the GDPR. Namely, the "processing of images will not generally involve processing of sensitive data as the images will only be covered by the definition of biometric data when being processed through a specific technical means which permits the unique identification or authentication of an individual".[385] This implies, as in GDPR Recital 51 (which speaks of photographs, not images) that sensitive biometric data may be interpreted to include both identification and verification. This point was previously analysed in the GDPR context. Here, one can see that the root of this confusion in the GDPR can be

[380] Paragraph 56, CoE, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [Ets No. 108] Draft Explanatory Report (2016) https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-to-automatic-/16806b6ec2.

[381] CoE, Amending the Protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data CM/Del/Dec(2018)128/5.

[382] CoE, Convention 108 + Convention for the protection of individuals with regard to the processing of personal data https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[383] Article 6 Convention 108+.

[384] C de Terwangne, "Privacy and Data Protection in Europe: The Council of Europe's Convention 108+ and the European Union's GDPR" in G González, R Van Brakel and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Elgar, 2022) 10-35, 12 https://doi.org/10.4337/9781786438515.00007.

[385] Point 57-58, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [Ets No. 108] Draft Explanatory Report (2016).

traced to Convention 108, or more precisely to its reports.[386] Some authors consider that there is less vagueness in the Convention 108+ approach to the difference between sensitive and non-sensitive biometric data than there is in the GDPR.[387]

2.8.2. The European Convention of Human Rights and the Case Law of Its Court: A Vital Inspiration for EU Biometric Law

2.8.2.1. The Relationship Between EU Biometric Law and the ECHR

The European Convention on Human Rights (ECHR) is a longstanding and influential international instrument. The ECHR grants enforceable rights to individuals, so that any person can invoke a human right and freedoms under the ECHR before a domestic court. If there is no recourse left domestically, an individual can appeal before the European Court of Human Rights (ECtHR) situated in Strasbourg. Particularly important is the similarity between the (proportionality) assessment mandated in Article 8 ECHR as compared to Articles 7 and 8 CFR.[388]

The ECtHR and CJEU share similarities, and each exerts influence over the other. However, there are also differences. The ECtHR safeguards human rights protected under the ECHR. Most important is the right to respect for private and family life of Article 8 ECHR. It is from judgments invoking this Article that both the privacy and data protection case law of the ECtHR developed. In contrast, the EU legal order contains in its European Charter of Fundamental Rights separate rights to privacy and data protection, but which are nevertheless decided together in cases concerning biometrics, without the CJEU differentiating between them.[389]

There is no direct right to data protection in the ECHR, but the ECtHR has interpreted Article 8 (the right to privacy) to cover the problem of data protection as well.[390] In addition, secondary EU legislation, such as the GDPR, plays a crucial role in EU biometric law, and consequently in EU biometric case law. The jurisdiction of the ECtHR binds all member states of the Council

[386] Tosoni Bygrave, "Article 4(14). Biometric data" in C Kuner et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), 210.
[387] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity, 193–217, footnote 18.
[388] See 3.2 of the thesis, particularly 3.2.1 and 3.2.6 where the case of the CJEU which expounded on the judgment of the ECtHR in the *Marper* case is analysed.
[389] Concerning the differentiation between privacy and data protection, see 4.2 of the thesis.
[390] J Kokott and C Sobotta, "The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" (2013) 3(4) International Data Privacy Law, 222–228, 223.

of Europe, which includes more countries than the EU. All individual EU Member States are also members of the CoE.

The ECHR is particularly important for individuals who can bring a claim before the ECtHR against their State if their right under the ECHR has been violated.[391] The path of individuals to achieve redress against the action of public authorities before the CJEU is much more complicated and narrower. The relationship between the CJEU and the ECtHR has been determined in recent years by the CJEU's Opinion 2/13, by which this Court held that the EU cannot accede to the CoE under the agreements reached at that point.[392] The ECtHR continues to apply the doctrine by which EU law is presumed to offer, in principle, protection equal to that of the ECHR.[393]

There is evidence that the CJEU minimised the effects of Article 52(3) CFR, which requires a consistent interpretation of the Charter with the case law of the Strasbourg Court; generally, the CJEU examines and cites ECtHR case law less since the Lisbon Treaty came into force in 2009.[394] The CJEU has started to refer to the CFR instead of the ECHR, even if the right in question is protected by the ECtHR and is also a general principle of EU law.[395]

Importantly, the ECHR, interpreted by ECtHR judgments, acts as a benchmark for assessing the legality of the application of the Return Directive and it is further used by the CJEU and national EU courts for interpretation.[396] Kokott and Sobotta have explored the distinction between data protection and privacy in the jurisprudence of the CJEU and the ECtHR and have drawn a number of conclusions. First of all, the CFR in its separate Article on data protection sets specific additional guarantees, by which data must be processed fairly, on the basis of the consent of the person concerned or on a legitimate basis laid down by law, and further, that persons are given the right to access and rectify data. These additional rights are not enumerated in Article ECHR. Further, the authors detected that the ECtHR may understand what amounts

[391] ibid, 222.
[392] Opinion 2/13 ECLI:EU:C:2014:2454.
[393] R Lawson, "Atlas Shrugged: An Analysis of the ECtHR Case Law Involving Issues of EU Law Since Opinion 2/13" (2024) 9(2) European Papers, 647-671, 665.
[394] T Molnár, "The Impact of ECtHR Case-law on the CJEU's Interpreting of the EU's Return Acquis: More Than It First Seems?' (2022) 62(4) Hungarian Journal of Legal Studies, 273 https://doi.org/10.1556/2052.2022.00354
[395] R Tinière, "The Use of ECtHR Case Law by the CJEU: Instrumentalisation or Quest for Autonomy and Legitimacy?" (2023) 8(1) European Papers, 323-330, 325 ISSN 2499-8249 - doi: 10.15166/2499-8249/654.
[396] T Molnár, "The Impact of ECtHR Case-law on the CJEU's Interpreting of the EU's Return Acquis: More Than It First Seems?' (2022) 62(4) Hungarian Journal of Legal Studies, 260-261. https://doi.org/10.1556/2052.2022.00354.

to personal information in slightly different terms from the CJEU.[397] The ECtHR has established that interference with privacy is caused by the collection, storage, or disclosure of information relating to private life. Under Article 8 ECHR, this interference must be justified. The conditions for the justified interference of privacy are that it is in accordance with the law, that it pursues legitimate aims, and that it is necessary in a democratic society to achieve those aims.[398]

Concerning the requirement of a sufficient legal basis, the key requirement is that it is foreseeable, which is not achieved if the rule is of a very general nature. A legal basis for the collection and storage of personal information must develop limitations of these powers, and establish safeguards against abuse and against measures which are not proportionate. Regarding legitimate aims for the restriction of the privacy of individuals, Article 8(2) has a limited list of admissible grounds. These include the interests of national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others. The CFR has an open list of objectives of general interests recognised by the EU or by the need to protect the rights and freedoms of others.[399]

2.8.2.2. ECtHR Case Law Concerning Biometrics and the Right to Privacy

There now follows a short introduction to some of the more important judgments of the ECtHR which concern biometrics, and which have influenced EU biometric law. Some of these cases will be further discussed at various points in the thesis. The most important case of the ECtHR which decisively influenced how the CJEU understands biometrics is the *Marper* case.

Marper was a landmark case before the ECtHR from 2008. The case concerned the retention (storage) of DNA samples and of fingerprints of persons who were accused of a crime. Even if these persons were not convicted, the biometric data were stored for an indefinite period. The ECtHR does not explicitly discuss the term biometric data in this judgment. The critical aspect is that the retention of fingerprint data and DNA for an indefinite period, without the possibility to challenge this, was contrary to Article 8 ECHR, which defines the human right to private and

[397] J Kokott and C Sobotta, "The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR" (2013) 3(4) International Data Privacy Law, 222–228, 224.
[398] ibid.
[399] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) Article 8(2); Charter of Fundamental Rights of the European Union [2012] OJ C 326/392 (CFR), Article 52(1).

family life. The way the ECtHR conducted the analysis in *Marper* has been influential to the development of the case law before the CJEU, particularly when it concerns justifying the processing of biometric data in view of fundamental rights. It can be said that *Marper* set the outer limits of the use of biometrics by stating that the retention of biometric data, for an unlimited period, of persons who were not convicted of a crime, and without them having the possibility to challenge this retention, fails to strike a fair balance between competing private and public interests, and that such retention is a disproportionate interference of the right to privacy and is not necessary in a democratic society.[400] The Court gives national authorities a certain "margin of appreciation" in their assessment of whether such a procedure is necessary in a democratic society, whether it follows a legitimate aim in answering a "pressing social need" and if it is proportionate to the legitimate aim pursued and if the reasons provided by the national authorities are "relevant and sufficient".[401] But in *Marper*, the national authorities overstepped such a margin.[402]

Subsequent case law of the ECtHR then drew the limits more precisely when it comes to conditions for the use of biometrics by public authorities. The ECtHR considers these cases as an important part of its data protection and privacy case law.[403] But these cases can be interpreted as belonging to a more specific area that can be named biometric (case) law of the ECtHR, because they concern the use of biometric technologies for the identification or verification of identity and their impact on the right to privacy. A few examples of other important cases which build upon *Marper* can also be mentioned.

Both Peruzzo and Martens were convicted of a number of crimes in Germany. Their DNA samples were stored in a database because German law allowed for this in cases of convicted criminals where there is a risk of future offences. There was no limit on the retention period, but there was a statutory review at regular intervals to test whether the retention continues to be necessary.[404] Therefore, unlike in *Marper*, there was no blanket or indiscriminate taking and retention of DNA profiles.[405] Consequently, the ECtHR decided that there was no infringement of the right to privacy by the German authorities in *Peruzzo and Martens v Germany.*

---

[400] *S and Marper v United Kingdom* App. nos. 30562/04 and 30566/04 (ECtHR, 2008) para 125.
[401] ibid, para 101.
[402] ibid, para 125.
[403] Guide to the Case-Law of the of the European Court of Human Rights, Data protection, 2020 https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0.
[404] *Peruzzo and Martens v Germany*, App. nos. 7841/08 and 57900/12 (ECtHR, 4 June 2013) para 46.
[405] ibid, para 47

MK v France was decided before the ECtHR in 2013. It concerned the retention of fingerprints of persons who were not convicted of a crime. The storage period was limited to 25 years.[406] The possibility to delete the data before the limit is only theoretical and illusory.[407] Therefore, the ECtHR ruled that France had overstepped its margin of appreciation and that such a practice of storing biometric data is contrary to the applicants' right to private life.[408]

Gaughran v UK is an important judgment before the ECtHR concerning biometrics and data protection.[409] Mr Gaughran was convicted (which distinguishes the facts of the case from those of *Marper*) but only of an offence of driving with excess alcohol, which was punishable by a prison sentence. Thus, this case tests whether the seriousness of the crime determines the legality of storing biometric data, taking into consideration Article 8 ECHR. The period of retention of the said data was indefinite. The Court makes the distinction between this case and *Peruzzo and Martens v Germany.* In *Peruzzo*, persons were convicted of serious crimes.[410] The government argued that the more that data are retained, the more crime is prevented, which the Court countered by stating that this would justify the indefinite storage of (biometric) data of the whole population "and their deceased relatives", recalling a similar argument from *MK v France*. This kind of general, preventative retention is excessive and irrelevant, according to the Court.[411] Since the UK opted for an indefinite retention period, this must be offset by other circumstances, such as effective safeguards for the applicant in relation to their data and by the seriousness of the offence.[412] It should be noted here that the author of the thesis used the approach of biometric parameters in assessing a biometric system, where the parameter of the storage period is analysed in the context of EU law, bearing similarities to the logic of the ECtHR in *Gaughran*.[413] The Court concluded that the indefinite period of retention, the absence of a real possibility of review, and not taking into account the seriousness of the crimes fails to strike a balance between public interests and private interest. The State has a slightly wider margin of appreciation in cases where the data of a person convicted of a crime are retained,

[406] *MK v France*, App. no. 19522/09 (ECtHR, 18 April 2013), para 45
[407] ibid, para 44.
[408] ibid, paras 46-47.
[409] *Gaughran v UK*, App. no. 45245/15 (ECtHR, 13 June 2020).
[410] ibid, para 87.
[411] ibid, para 89.
[412] ibid, para 94.
[413] See 3.2.6.2 of the thesis.

although the margin is not sufficient for the said circumstances of *Gaughran*. Thus, the Court ruled that there had been a violation of Article 8 ECHR.[414]

The case of *Trajkovski and Chipovski v North Macedonia* was decided on the same day in 2020 as *Gaughran*. It can be distinguished from *Marper* by the fact that the person in question was convicted of a crime. However, in *Trajkovski*, the storage period was also unlimited, and there was no practical possibility to review this decision or for the removal of the biometric data from the police database.[415] For this reason, the ECtHR in *Trajkovski* concluded that there was a violation of the right to privacy, even though the person in question was convicted of a crime.[416]

The last case to be mentioned is that of *Glukhin v Russia*. This case is quite different from the previously mentioned cases because it concerns the use of biometric surveillance. A sole protestor in a Moscow subway station was identified through the means of facial recognition from camera footage. The Russian police soon arrested him. The case is discussed in 2.7.5 of this thesis concerning how the AI Act allows biometric surveillance on European streets. The ECtHR ruled that there had been a violation of both Article 8 (private life) and Article 10 concerning freedom of expression.[417] The Court stressed that facial recognition and biometric surveillance of public places can cause a chilling effect related to a number of human rights, because the persons do not engage in free behaviour out of fear that these modern technologies will be used to prosecute them when they engage in free speech, protests or similar behaviour.[418] Therefore, *Glukhin* is not only important as a new entry into the data protection case law of the Court, but it is one of the first cases to scrutinise the use of a biometric technology of facial recognition in terms of human rights.[419]

2.9. Clearview AI: Theft in Broad Daylight

The business model of Clearview AI and subsequent decisions of multiple EU Data Protection Authorities (DPAs) are an excellent demonstration of how the existing EU legal regime copes with biometrics and AI. It shows the application of GDPR rights and principles in relation to

---

[414] *Gaughran v UK*, App. no. 45245/15 (ECtHR, 13 June 2020), para 98.

[415] *Trajkovski and Chipovski v North Macedonia*, App. no. 53205/13 and 63320/13 (ECtHR,13 February 2020) para 53.

[416] ibid, para 54.

[417] *Glukhin v Russia*, App. no. 11519/20 (ECtHR 4 July 2023).

[418] ibid, para 88.

[419] For an analysis of the case, though less centred on biometrics, see F Palmiotto and N Menéndez González, "Facial Recognition Technology, Democracy and Human Rights" (2023) 50 Computer Law & Security Review, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2023.105857.

biometrics, the problem of defining a proper legal basis for the processing of biometric data and finally the powers of Data Protection Authorities (DPAs) to enforce EU (biometric) law when faced with novel technologies.

Two decisions concerning Clearview AI are analysed further in text. The decisions in question were reached by the French and Greek DPAs, both in relation to Clearview AI.[420] The Commission nationale de l'informatique et des libertés (CNIL) is the French data protection authority which reached the decision in question in October 2022.[421] The Hellenic Data Protection Authority (HDPA) reached its decision concerning the biometric practices of Clearview AI on 13 July 2022.[422] Both decisions concern similar facts and offer a similar legal analysis, and thus will be analysed here together.

2.9.1 The Facts Concerning Clearview AI.

The practice of Clearview AI was to scour the internet for available photographs and video of natural persons' faces. Clearview AI collected images which were publicly available on the internet, most often on Facebook and Twitter, but also from video material from sites such as YouTube by so-called data scraping (automatically collecting data from the internet). These images were processed by Clearview's software so that the facial images were stored as numerical information that is machine readable (biometric templates). When a user of Clearview's services wants to identify a person, it can upload an image of that person and perform a search on Clearview's database. Clearview uses publicly available personal data to create its own private biometric database that it then sells as a recognition tool. If police in the US, or in Germany, for example, obtain footage of a store robbery, they can upload a screenshot of the suspect and search on the Clearview database for matches, for a fee.[423] The photographs obtained are often far from ideal for facial recognition to work optimally, since they might have been taken to document a family picnic instead of being used as a passport photograph. The results can go spectacularly wrong, as was the case reported by the media concerning an eight

[420] There were other DPAs in the EU that reached a decision concerning Clearview AI, such as the Italian and Irish DPAs.
[421] CNIL "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI" https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf.
[422] Hellenic Data Protection Authority (HDPA), Decision 35/2022 Ref. No. 1809 https://www.dpa.gr/sites/default/files/2022-08/35_2022%20anonym_EN_FINAL.pdf.
[423] For a description of the facts, see either of the decisions analysed, e.g. (CNIL) "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI" Part C.

months pregnant (Black) woman falsely identified by Clearview AI as being involved in a carjacking and robbery.[424]

2.9.2. The Scope of the GDPR and Clearview AI Activities

Both the Greek and French DPA started the analysis by determining that Clearview's activities are within the scope of the GDPR. Namely, Clearview AI is a US company, without EU establishment and one that does not provide services in the EU. However, Clearview AI was processing personal data of data subjects located in the EU, doing so in a way that constitutes monitoring their behaviour, which is covered by Article 3(2)(b). This was a crucial step in both decisions, because without proving the existence of "monitoring", the practice of Clearview AI would not be under the scope of the GDPR. Thankfully, the GDPR in its recitals and articles describes monitoring in very similar terms to what Clearview AI was doing.[425] Monitoring is understood as tracking persons on the internet, including the potential subsequent use of personal data processing techniques which consist of profiling a natural person.[426] Clearview AI engages in monitoring because it collects photographs and other data of natural persons and then creates behavioural profiles of such persons, given that it links an image of a person with additional information such as where the photograph was taken (geolocation data) and the contextual data around the photograph that may reveal a great deal about the data subject (whether the photograph was taken in the context of professional or family life).[427] Monitoring and profiling (the automated processing of personal data) as defined in the GDPR essentially describe the business model of Clearview AI. In addition, the Greek DPA laconically concluded that photographs are biometric data, and that this kind of processing concerns sensitive personal data.[428] Therefore, a legal basis according to Article 9(2) GDPR which concerns the processing

[424] Kashmir Hill, 'Eight Months Pregnant and Arrested After False Facial Recognition Match" The New York Times 6 August 2023 https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.
[425] Regulation (EU) 2016/679, Recitals 24 and 80.
[426] ibid, Recital 24; Commission Nationale de l'Informatique et des Libertés (CNIL) "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", point 34; Hellenic Data Protection Authority (HDPA), Decision 35/2022 Ref. No. 1809, 7.
[427] Also invoked by both DPAs in the context of monitoring was EDPB "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)" Version 2.1 (2019).
[428] "From all the information brought to the attention of the Authority, it emerged that the processing in question does not concern a simple collection of data, but results in the conversion of the photographs collected into biometric data, the processing of which is subject to the strictest provisions of Article 9 GDPR". HDPA, Decision 35/2022 Ref. No: 1809, para 16.

of special categories of personal data should have been satisfied in addition to the legal basis under Article 6 GDPR.[429]

2.9.3. Legitimate Interests and Reasonable Expectations

This practice of Clearview AI was characterised by the DPAs as the processing of personal (or biometric) data based potentially on legitimate interests, as under Article 6(1)(f) GDPR. However, these legitimate, or more precisely economic, interests must be balanced against the interests of the data subjects. Data subjects have certain reasonable expectations concerning the nature of their relationship with Clearview AI.[430] These reasonable expectations are assessed in the light of recital 47 GDPR (which defines this concept) and Opinion 6/2014 A29 WP[431] on the notion of legitimate interest. There are two key legal insights made similarly by CNIL and HDPA.

First, both Greek and French DPA decisions raise the point of reasonable expectations. Namely, data subjects should be able in advance to determine the scope of the processing of their data. Further, data subjects should not be surprised by the ways in which the personal data were processed, which is required to satisfy the legal basis of legitimate interests pursued by the controller.[432] This is clearly not the case with the practice of Clearview AI. No person expects their photographs to be used to enrol them into a biometric database that may be used to establish them as suspects of crime. Since there is no relationship between the data subjects and Clearview AI nor the possibility of the data subjects knowing that Clearview AI is processing their data, the legitimate interest basis is not satisfied.

The second key point is that even if personal data are made publicly available by the data subjects themselves, they remain personal data.[433] If someone makes photographs public on the internet, this does not provide a legal basis for the processing of those data. Consequently, the

[429] HDPA, Decision 35/2022 Ref. No. 1809, para 8.
[430] CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI" para 63; HDPA Decision 35/2022 Ref. No. 1809, para 16; Recital 47 Regulation (EU) 2016/679.
[431] A29WP, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (2014) 844/14/EN WP 217".
[432] HDPA, Decision 35/2022 Ref. No: 1809, para 9.
[433] Point 61 CNIL.

data protection framework is still applicable to personal data made available online. This means that scraping the internet for publicly available data is not allowed.[434]

Scraping biometric data is not justified by the fact that the personal data were made available by the data subjects. This legal analysis counters the (intuitive) reasoning applied by businesses scraping facial images who are of the persuasion that publicly available data can be used without restriction. The idea of repurposing data posted by users on social networks was already debunked as illegal in 2014, when the A29WP issued an Opinion which stated that if someone manifestly discloses their sensitive personal data it does not follow that all the conditions for the processing of such data are satisfied.[435] It can be added at this point that the AI Act prohibits AI systems that create facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.[436] Recital 43 of AI Act explains that this practice should be prohibited because it provokes a feeling of constant surveillance and can lead to gross violations of fundamental rights.

2.9.4. The Lessons of the Clearview AI Case

There were a number of breaches committed by Clearview AI that the DPAs found in their respective opinions. Both the Greek and French decisions established a breach of the legal basis of processing personal data that Clearview had carried out since the prerequisites for the legal basis of legitimate interest were not met.[437] Both the CNIL and HDPA concluded that biometric data were processed by Clearview AI when it processed the photographs, but the HDPA explicitly established that Clearview AI also did not satisfy the Article 9(2) legal bases for the processing of biometric data, which have to be satisfied in addition to the legal bases of Article 6 GDPR.[438] Since there was no proper legal basis for the practice used by Clearview AI, a breach of the principle of lawfulness of processing of personal data was also found.[439]

The CNIL did not specify breaches of particular principles, but only noted as a conclusion that the "breaches committed are particularly serious, notably with regard to the infringement of the

[434] This has significant ramification for the emerging economy of large AI models that "feed" themselves on available data, but this is beyond the reach of this thesis.
[435] A29WP, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (2014) 844/14/EN WP 217", 15.
[436] Regulation (EU) 2024/1689, Article 5(1)(e).
[437] CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", paras 49-69.
[438] HDPA, Decision 35/2022 Ref. No. 1809, para 17.
[439] ibid, para 18.

fundamental principles provided for by the GDPR(...)".[440] On the other hand, the HDPA specified breaches of GDPR principles, in addition to breaches of rights and other obligations of the GDPR committed by Clearview AI. The HDPA also established a breach of the obligation of Clearview AI to designate a representative in the EU, since it is not established in the EU (Article 27 GDPR).[441] There was a breach of the principle of transparency (Article 5(1)(a) GDPR in combination with a breach of Article 14 GDPR, because Clearview AI did not inform subjects clearly about the processing of their personal data.[442] Clearview AI also breached the rights of data subjects to access information (Articles 12 and 15) on the personal data it processed.[443] The French CNIL determined a breach of the right to erasure of Article 17 GDPR, since data subjects were not able to achieve this in respect of the Clearview AI database.[444] The breach of this Article was not raised by the HDPA. There was a breach of the obligation to cooperate (Article 31 GDPR) with the CNIL committed by Clearview AI, which ignored the CNIL's inquiries throughout. This is another point of difference between the CNIL and HDPA, since the latter did not raise this point in its decision.

The supervisory powers of the HDPA and CNIL are based on Articles 55 and 56 GDPR. The HDPA specified that it invoked its corrective powers under Articles 58(2)(i) to impose a fine, to order a ban on the further processing, and to order the erasure of personal data of data subjects in Greek territory in accordance with the corrective powers of Article 58(2)(f) and (g).[445] Both the CNIL and HDPA imposed the maximum fine of EUR 20 million. The CNIL and HDPA also made the decision publicly available (with official English translations). The CNIL justified this by the severity of the breaches, the scope of processing and the number of data subjects involved in the scheme.[446] The purpose was clearly not only to sanction the behaviour of Clearview AI, but to send a message to AI companies as well to European citizens that tools to prevent such novel behaviours are already in place.

[440] CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", para 97.
[441] HDPA, Decision 35/2022 Ref. No: 1809, para 18.
[442] ibid; CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", paras 70-79.
[443] ibid, para 86.
[444] CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", paras 80-86.
[445] HDPA, Decision 35/2022 Ref. No. 1809, para 19.
[446] CNIL, "Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI", para 113.

Two takeaways from these decisions can be stressed here. First, both the CNIL and HDPA focused on the lack of a legal basis for processing. Clearview AI could not rely on their legitimate interests because data subject could not expect in advance that their data would be processed, which is contrary to the reasonable expectations of data subjects. The second point is that there is no single way to use the GDPR and fundamental rights legal framework to resolve challenges posed by actors such as Clearview AI. The HDPA and CNIL raised several different points on GDPR rights and principles. This flexibility of the legal reasoning came to the fore particularly in the even more extreme case of Worldcoin biometric practices.

2.10. Worldcoin: Explicit Consent for Biometric Identification

Worldcoin had the business idea of scanning biometric data of as many people as possible and storing these data on a blockchain. These biometric data could be used to create international biometric identities on a planetary scale. The biometric data were harvested by a physical device called Orb, a shiny ball which collects and processes iris scans, eye images, and facial images to create a unique personal Worldcoin ID. The Portuguese Data Protection Authority (CNPD) issued a temporary ban on Worldcoin's collection of biometric data.[447] What may sound like a pulp science fiction story takes a sinister turn when one finds out that as many as 300,000 people volunteered their iris scans in Portugal alone by visiting their local Orb; people waited in queues which included children.[448] Worldcoin was founded by Sam Altman, famous for being CEO of OpenAI which developed ChatGPT.

From a legal perspective, the striking feature of the Worldcoin affair is that people gave their explicit consent for the processing of their biometric data, made clear by their active efforts to approach the Orbs. The Portuguese DPD had to focus on other reasons for banning this practice, because there was indeed a (potential) legal basis for the processing of biometric data, namely explicit consent, contained in Article 9(2)(a) GDPR.

The Portuguese CNPD banned Worldcoin practice on the basis that information provided by Worldcoin to data subjects was inadequate in relation to the requirements of Article 13 GDPR.[449] The CNPD concluded that this in turn breached the principle of transparency of

[447] Comissão Nacional de Proteção de Dados (CNDP) DELIBERAÇÃO/2024/137 https://www.cnpd.pt/media/imub4o4i/pt-sa-decision-worldcoin_temporary-limitation-of-processing_20240325.pdf.
[448] CNDP, "DELIBERAÇÃO/2024/137", para 5.
[449] ibid, para 70.

Article 5(1)(a) GDPR. A further breach of the GDPR was that data subjects were not informed of their right to withdraw consent, as required by Article 13(2) GDPR.[450] The processing of the biometric data of children was a further infringement of the data protection legal framework since children are unable to provide valid consent for processing. Furthermore, there was no possibility to exercise the right to the erasure of personal data (Article 17 GDPR). Indeed, Worldcoin stated that once an individual has signed up for the Orb, there is no possibility of deletion due to the nature of blockchain technology.[451] The CNPD finally referred to fundamental rights, of which persons cannot avail themselves, in particular the right to data protection under Article 8 CFR which was infringed by the practice of Worldcoin. The decision concerning Worldcoin is a genuine example of how AI and biometrics (along with old-fashioned human naivety) raise legal challenges that require imaginative legal thinking, particularly concerning cases where the data subjects express explicit consent to the processing of their sensitive data.

[450] ibid, para 73.
[451] ibid, paras 78-80.

Chapter 3: Biometric data in Migration and Asylum: Analysis of Biometric Law Through Case Law, Information Systems of the EU, and Interoperability

3.1. The Aim and the Structure of This Chapter

The objective of this chapter is to explain how the biometric data of migrants and asylum seekers is used, primarily using the example of a large-scale information system, which is Eurodac. The previous chapter concerned the general provisions of biometric law which apply to any processing of biometric data. This chapter will explain biometric law in the more specific context of migration and asylum. These conclusions will be the basis for the discussion of fundamental rights and privacy challenges of biometrics in Chapter 4 and the proposals for solutions in Chapter 5.

The chapter is structured in four sections. A detailed analysis of crucial judgments of the CJEU concerning biometrics will follow this introduction. These decisions of the Court together make up what can be considered biometric case law. The judgments provide a step-by-step analysis of how to assess the legality of biometrics in the sphere of EU law, particularly concerning the use of biometrics in EU migration law. Even though many aspects of the judgments will be mentioned in the first part of this chapter, as part of an assessment of the provisions of Eurodac, it is important to give a coherent overview as these judgments unfolded over the last decade. They show the growing importance of biometrics as well as the growing understanding of the Court of biometric issues.

After the biometric case law, an analysis of the Eurodac information system will serve as a study to examine what the author considers are the basic parameters of any biometric system. Eurodac is the most important large-scale information system for asylum seekers and irregular migrants and is a system reliant on biometric data to identify a person. Eurodac thus most closely corresponds to the personal and material scope of this thesis. The parameters are the basic elements of any biometric system, examples of which are the place and length of the storage of biometric data or the rules for access to biometric data. Examining a biometric system through parameters will allow for a better understanding of the close connection of the legal and technological issues concerning biometrics.

The fourth section of this chapter will critically discuss the biometric aspects of interoperability and the biometric template, which follow from the previous analysis of Eurodac, as one of the interoperable biometric systems. Interoperability represents the links between various large EU information systems and in some respects rises to an overarching database of all EU biometric databases, effectively changing the meaning of compartmentalised EU information systems. An essential prerequisite for interoperability is to store biometric data in the same format so that it can be accessed by all the connected databases. The key question is whether or not the biometric template, as imagined in the interoperability scheme, is biometric data. This is vital because it is the biometric template that is stored in a database and that can further be protected by encryption and other privacy enhancing schemes, which will be the subject of Chapter 5.

3.2. Biometric Case Law: CJEU Justifies the Use of Biometrics

The aim of this part of the thesis is to show the development of biometric case law in chronological order, so that there is a clear sense of both the changes and the continuity in the development of biometric law. The second aim is to show how the CJEU applies the fundamental rights of privacy and data protection to issues of biometrics. This analysis will be important for the following chapter dealing with fundamental rights and biometrics.[452]

The case law of the CJEU concerning biometrics can be divided into two eras. In the first, biometric cases concerned how biometrics generally relate to EU law (*Schwarz*),[453] whether EU law prohibits biometric databases (*Willems*), and if national rules requiring the collection and storage of biometric data are justified as restrictions on the free movement of migrants (*A, B and P*).[454] In all cases, the Court decided in favour of allowing (greater) processing of biometric data, but in doing so it also provided a framework for relating biometrics to EU law. All these cases concerned biometric data collected primarily for travel documents. Biometric data are explicitly mentioned in these cases, but they are not defined in the abstract, only as fingerprints or facial images. These cases show the growing need to provide a general definition of biometric data, which would be set out in the GDPR that followed.

In the second era, a number of biometric cases appeared before the CJEU with certain common features. There is no longer any doubt that biometrics are framed as a (justified) limitation of

[452] See Chapter 4 of the thesis, particularly 4.2.3 which represents an analysis of the fundamental rights of privacy and data protection in biometric case law.
[453] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670.
[454] Case C-70/18 *A, B and P* ECLI:EU:C:2019:823.

privacy and data protection. The new cases show the growing importance of biometrics and serve the Court to open and then close newer questions concerning the legitimacy of biometrics. These newer cases provide insight into the limits that EU law poses on the use of biometrics by public authorities. The most significant judgment in the newer era was *RL v Wiesbaden*,[455] which is a clear continuation of *Schwarz*[456] from ten years previously, and revisits many of the fundamental issues raised by the processing of biometric data in the legal and biometric landscape that had changed over the ten years.

Taken together, these judgments represent a distinct case law that features EU law in relation to biometrics and the rights of individuals. What is missing is not just a more critical approach to biometrics that should have been taken by the Court but a conspicuous lack of cases to address the elephant in the room. Namely, there are no cases relating to the application of Eurodac or other information systems in relation to how these systems process the biometric data of migrants, third-country nationals (TCNs) and asylum seekers. Indeed, there were millions of migrants being fingerprinted, many of them fingerprinted forcefully. Irregular migration is a crucial political issue in many EU countries, which can sweep extreme forces into power. The case law concerning biometrics has been developed primarily from cases concerning EU citizens objecting to having their biometric data processed. Nevertheless, fundamental rights are applicable to all persons, and therefore the interpretation of the Court in biometric case law is applicable in the context of migrants and asylum seekers as well.

3.2.1. Case C-291/12 *Schwarz*

Schwarz is still arguably the most important judgment reached by the CJEU concerning biometrics. In this judgment, the CJEU applied a thorough proportionality analysis by which it concluded that the obligation to give fingerprints in the context of the Passport regulation is not contrary to fundamental rights. The processing of biometric data is a justified limitation of the right to privacy. In this way it framed biometrics as the legal issue of justifying interference with data protection and privacy against certain general interests of the Union. More broadly, biometrics can be framed as a proportionality exercise of weighing the interests of the privacy of the individual against the security concerns of the public authorities.[457]

[455] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251.
[456] Case C-291/12 *Schwarz* ECLI:EU:C: 2013:670.
[457] This is true for the biometric legal framework in the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (secondary EU legislation) and the mutually intertwined fundamental rights framework of the CFR. That a certain application of biometrics stands or falls on the proportionality exercise is also true in the context of the ECHR.

The *Schwarz* case considered the impact of biometrics on fundamental rights and EU data protection law in the context of storing biometrics within a travel document. Thus, it would be wrong to transplant the legal analysis of the Court to the context of the use of biometrics in databases, which raises greater privacy (and proportionality) concerns (even though that is exactly the critique towards the Court's decision in the subsequent case of *Willems* which relied on *Schwarz*). *Schwarz* did not provide a definition of biometric data. It referred to biometric data as mentioned in Article 4(3) of the amended Regulation 2252/2004[458] where biometric data meant two fingerprints and a facial image. But it is still the judgement that answered how biometrics are legally framed in the context of EU law.

Regulation 2252/2004 mandated that Member States adopt biometric passports which contain in a storage medium on the passport itself two fingerprints and a facial image. Mr Schwarz refused to have his fingerprints taken when applying for a new passport. His application for the passport was thus rejected, and he lodged an action before a court to have his passport issued but without taking his fingerprints. Mr Schwarz claimed that the obligation to have his fingerprints taken is contrary to Article 7 CFR on the right to data protection and Article 8 CFR on the right to respect for private life. The German Court referred a question to the CJEU asking simply whether the obligation to contain two fingerprints and a facial image in a passport is valid.[459]

3.2.1.1. The Court's Analysis in *Schwarz*

The CJEU first acknowledged that any processing of personal data may constitute a threat to the right to respect for private life (Article 7 CFR) and the right to protection of personal data (Article 8(1) CFR) which the Court examined jointly, without making a distinction between those two rights.[460] In *Schwarz*, the Court confirmed that fingerprints are personal data. What is more, it considered fingerprints biometric data, but only in the sense of Article 4(3) of Regulation 2252/2004, since there was no general notion of biometric data in data protection legislation in the DPD, the predecessor of the GDPR. Fingerprints are personal data because

---

This will be shown later, since now the focus is on *Schwarz*. However, what must be considered in the balancing exercise is the particular factual considerations concerning the type of biometric technology, how long biometric data are retained, who can access them, the purpose of processing biometric data, and other important items on a biometric "checklist".

[458] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1.

[459] Case C-291/12 *Schwarz* ECLI:EU:C: 2013:670, para 13.

[460] ibid, paras 23-25.

they contain unique information about individuals which allows those individuals to be precisely identified, and to that effect the Court recalled the ECtHR decision in *S and Marper*.[461]

The act of processing personal data means any operation upon it by a third party, including collecting, storage and so on, which transpires from Article 2(b) DPD, and measures concerning fingerprints based on Regulation 2252/2004 constitute the processing of personal data.[462] The Court thus had no qualms about establishing that the taking and storing of fingerprints as required by Article 1(2) of Regulation 2252/2004 are the processing of personal data which represents a threat to the fundamental rights of privacy and data protection. The Court clearly stated in *Schwarz* that a person cannot be deemed to have consented to fingerprinting just because the person is requesting the issuance of a passport, and that there must be a clear legal basis for the processing of fingerprints.[463] This insight has relevance in other similar circumstances. By analogy, an asylum seeker cannot be understood to have consented to have their fingerprints taken for the asylum procedure by the act of requesting asylum: the legal basis for processing must be based on law and must be examined in the context of a proportionality test.

In the following crucial part of the judgment, the Court considered how such processing of personal data is justified. Article 8(2) CFR requires that personal data must be processed fairly and on a legitimate basis laid down by law. Articles 7 and 8 CFR are not absolute rights. Article 52(1) CFR provides conditions for limitations of the exercise of those rights. These four conditions are that the limitation is provided for by law, it respects the essence of those rights, and, in accordance with the principle of proportionality, the limitations are necessary and genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[464]

The first condition that the limitation is provided for by law is satisfied because Article 1(2) of Regulation 2252/2004 requires the processing of fingerprints.[465] The second condition is that the limitation of fundamental rights which occurs with the processing of personal data meets the objectives of general interests recognised by the Union. The CJEU states that the said Regulation has two aims: to prevent the falsification of passports and to prevent fraudulent use

[461] ibid, para 27.
[462] ibid, para 28.
[463] ibid, para 32.
[464] ibid, para 34.
[465] ibid, para 35.

of passports. These two aims together contribute to preventing illegal entry into the EU, which is an objective of general interest.[466] One can criticise this by asking how exactly the objective of preventing illegal entry into the EU is achieved by imposing additional obligations on EU nationals? Should it not be the other way around, that preventing illegal entry requires imposing additional security features on travel documents of third-country nationals, not on citizens? There is no indication that passport fraud committed by EU citizens was a problem of significance before the introduction of biometrics.

Regarding the third condition, the Court simply stated that there is nothing to suggest that the essence of the rights of Article 7 and 8 CFR were not respected by these limitations.[467] The Court did not engage with the condition that the essence of the fundamental right has to be preserved, summarily dismissing the possibility that fingerprint collection and storage infringe the essence of privacy and data protection. The concept of essence may be useful for limiting the most egregious uses of biometrics (such as DNA profiling of migrants or biometric surveillance).

The fourth condition represents the proportionality test. According to the formulation in this judgment, limitations on the fundamental rights of privacy and data protection must be proportionate to the aims pursued by Regulation 2252/2004 and by extension to the objective of preventing illegal entry into the EU. The Court examined proportionality in two steps: whether the measure of processing fingerprints is appropriate for the stated aim and whether the processing of fingerprints does not go beyond what is necessary.[468] The Court stated that the "storage of fingerprints on a highly secure storage medium" contributes to the aim of reducing passport fraud.[469] To the argument of Mr Schwarz that ascertaining identity by fingerprints is liable to mistakes, the Court held that absolute reliability is not needed. It is enough that this method significantly reduces mistakes or fraud, which it does.[470] The third argument in favour of the appropriateness of the measure is an "even-if" argument. Even if there is a mismatch between the fingerprints of the holder of the passport and the data in the document, this will not lead to the automatic refusal of entry into the EU. Article 4(3) of Regulation 2252/2004 states that such a mismatch will merely draw the attention of the

[466] ibid, paras 37-38.
[467] ibid, para 39.
[468] ibid, paras 41-43.
[469] ibid, para 41.
[470] ibid, para 43.

authorities. With these arguments, the Court was satisfied that the measure of processing fingerprints is appropriate for the stated objective.

Then the Court turned to the second step of the proportionality assessment, "whether such processing is necessary".[471] The first argument was that the operation involves only two fingers, which is not an operation of an intimate nature, nor does it cause discomfort any greater than the taking of a facial image. The fact that both facial image and fingerprints are taken does not, according to the Court, give rise to a greater interference with fundamental rights.[472]

3.2.1.2. Interpreting the Further Arguments of the Court in *Schwarz*

The Court's argument that collecting facial images and fingerprints does not cause greater discomfort than either one on its own is not convincing. First, the issue should not be about the level of comfort of the procedure, but how it affects privacy. Secondly, it is strange to claim that one plus one equals one. The Court does not clearly address the fact that two, not just one, biometric technologies are used, because that would lead to raising the following question: are not fingerprints alone dependable enough without the facial image (or vice versa)? This issue of multimodal biometrics (using multiple biometric technologies to increase accuracy and security) is an increasingly important issue and poses the question of how many biometric technologies, used in parallel, would be too many. This was not reflected upon by the Court, which probably sought to avoid such a problematic question.

The only alternative to the taking of fingerprints that the Court was able to conceive was an iris scan. Iris scans would not interfere less with the privacy and data protection rights of individuals. Further, according to the Court, iris recognition is less advanced than fingerprint recognition, is more expensive, and is thus less suitable.[473] It was rather naive of the Court to imagine that the only alternative to fingerprint recognition was iris recognition, a technology that was a curiosity at the time, and even today is not applied in any biometric system of the EU. Following this conclusion, the Court then had no problem in finding that iris recognition was inferior to fingerprint recognition.[474] The real alternative that the Court does not take into consideration is passports without fingerprints and how they compare. It would again require the Court to engage in a comparison of the system that was in place before the mandate for

[471] ibid, paras 46-63.
[472] ibid, paras 48-49.
[473] ibid, paras 51-52.
[474] ibid, para 52.

fingerprints in passports, and the Court does not engage in this analysis. An analysis of the benefits of fingerprint recognition would be needed, notwithstanding the fact that the US after the 9/11 attacks started to require biometric passports from incoming travellers and thus spurred the EU to adopt this measure.

The second line of argument was that personal data processing must be secure from misuse and abuse, for which the Court recalls the ECtHR's case of *Marper*.[475] The Court in *Schwarz* offered a crucial argument: it stated that the processing of fingerprints is protected from abuse by the fact that Article 4(3) of Regulation 2252/2004 explicitly states that fingerprints are collected only for the purpose of the Regulation.[476]

It must be stressed at this point that in the subsequent judgment of *Willems*, the Court concluded the opposite (of course, by framing it as a continuation of *Schwarz*): that there is nothing in Article 4(3) of Regulation 2252/2004 which guarantees that collected fingerprints would not be used for other purposes, such as a national database of fingerprints.[477] The Court thus bases the proportionality assessment in *Schwarz* on the fact that fingerprint data are used only for the verification of identity, that the data are stored only locally, and that they may be used for this purpose only. In *Willems* it would rely on the conclusion of the proportionality assessment carried out in *Schwarz*, but the underlying argument is different. The facts in *Willems* concern the reuse of fingerprints for other purposes and moreover to create remote biometric databases, while in *Schwarz* the positive outcome of the proportionality analysis was that no national databases are allowed. It could be argued that the whole of "EU biometric law" depends on this twist of legal logic from *Schwarz* to *Willems*. Without it, it would be dubious whether the processing of biometric data, especially for the purpose of creating biometric databases, is justified in view of the fundamental rights of the natural persons in question.

Turning to the conclusion of the Court in *Schwarz*, the Court states that Regulation 2252/2004 does not provide a legal basis for a fingerprint database.[478] If a question concerning a centralised database arises in the future, a competent court should address it. In summary, the processing of fingerprint data does not go beyond what is necessary and is therefore justified by its aim of preventing illegal entry into the EU.[479] It should be underlined how the Court avoided the real,

[475] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008).
[476] Case C-291/12 *Schwarz* ECLI:EU:C: 2013:670, para 56.
[477] Case C-446/12 *Willems* ECLI:EU:C: 2015:238.
[478] Case C-291/12 *Schwarz* ECLI:EU:C: 2013:670, paras 60-61.
[479] ibid.

pertinent question in *Schwarz*. The question is not whether Regulation 2252/2004 provides a legal basis for biometric databases – it clearly does not. The question at stake is whether the fundamental rights of privacy and data protection preclude the reuse of personal data collected on the legal basis of Regulation 2252/2004 for other purposes – for creating national databases. It is then a fiction that the fingerprints are stored only locally on the passport since the Court refuses to acknowledge that the same fingerprint data may also be enrolled in biometric national databases. The fundamental rights analysis is conducted as if national databases do not exist, by claiming that the issue does not concern EU law. This is not true, since any processing of biometric data causes limitations of fundamental rights, so that should also apply to the collection and storage of fingerprints for national databases. The Court did not want to address this question. It will be more directly posed in *Willems*, but again without the Court giving a straight answer.

The Court acknowledged that any processing of personal data is a threat to the fundamental rights of privacy and data protection which must be justified. The proportionality test conducted in *Schwarz* is detailed and revealing. First, this judgment clearly frames the issue of biometrics as essentially a proportionality exercise between the individual's right to privacy and certain societal interests (here as an objective of general interest recognised by the Union). This removes any doubt that indeed where biometrics are concerned, the issue of the fundamental rights of privacy and data protection are at stake. However, the Court did not go into the relationship between these two fundamental rights.[480]

Secondly, the Court identified *S and Marper* as a key judgment of the ECtHR concerning biometrics, upon which the Court repeatedly reflected in *Schwarz*.[481] Some legal scholars are of the view that the *Schwarz* judgment actually runs counter to the position taken by the ECtHR in *S and Marper* in that the retention of the fingerprints of persons not convicted is a disproportionate interference with privacy.[482] However, *Schwarz* can be clearly distinguished from the facts of *S and Marper*. In *Schwarz*, the case concerned the storage of fingerprints locally, for the purpose of verification, while *S and Marper* concerned the indefinite storage of fingerprints in a database. Nevertheless, both are key judgments concerning biometrics in their respective authorities.

[480] The relationship between privacy and data protection is discussed in 4.2 of the thesis.
[481] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008).
[482] P de Hert and G Bouchagiar, "Visual and Biometric Surveillance in the EU. Saying 'No' to Mass Surveillance Practices?" (2022) 27(2) Information Polity, 193–217, footnote 28.

Finally, it is important to note that the conclusion in *Schwarz* should not be applied universally in biometric cases, even though it is a landmark judgment for biometrics. In *Schwarz*, the Court did a proportionality exercise with the facts concerning biometric verification, not biometric identification, and the storage of biometric data locally within the control of the person instead of in a database. These were some of the determining factors in the Court's assessment that the limitation posed to fundamental rights was justified. The *Schwarz* analysis should thus apply primarily to cases concerning biometric verification. However, in *Willems* the Court used the conclusions from *Schwarz* even though the facts were significantly different from those in *Schwarz*. The cases concerned different types of storage, there were different purposes or legal bases that justified the biometric schemes, and the conditions for access were also different in the two cases. The Court nevertheless presented *Willems* as a logical continuation, a legally necessary conclusion to *Schwarz*.

3.2.2. Joined Cases C-446/12 to C-449/12 *Willems:* National Biometric Databases Are Allowed.

Willems concerned four private individuals from the Netherlands who refused to give their biometric data for the purpose of being issued with a passport (in three of the cases) or an identity card (in one of the four cases). As in *Schwarz*, their request for the issuance of the document was refused. All four cases were the subject of one judgment of the CJEU, and it is often called the *Willems* case as that was the surname of the first person whose case reference for a preliminary ruling was lodged on 3 October 2012.[483] The *Willems* judgment was reached by the CJEU in 2015, less than two years after the judgment in *Schwarz*. The applicants in *Willems* were concerned that their biometric data were not only stored on the passport or identity card, but also in a database. They were worried that authorities could use the biometric data for purposes other than those of Regulation 2252/2004 and that their data may be used for intelligence, judicial or security purposes. In addition, the applicants were worried that it was not clear who would have access to their biometric data and that these considerations ran counter to their fundamental rights.[484]

Dutch national law provided that the Netherlands identity card must contain a facial image, two fingerprints and the signature of the holder and that the issuing authorities keep the records of the travel documents. Likewise, Dutch law required that passports contain the fingerprints of

[483] Case C-446/12 *Willems* ECLI:EU:C:2015:238.
[484] ibid, paras 18-20.

the holder.[485] The referring national court asked in its first question whether Regulation 2252/2004 applies to identity cards which may be used as travel documents. The Court, after a textual analysis of the different language versions of Regulation 2252/2004 and its *travaux préparatoires*, answered the first question by concluding that Regulation 2252/2004 does not apply to identity cards issued by Member States.[486] In *Willems*, the Court refers to "biometric data" simply meaning fingerprint data.

In the more important, second question, the national court asked whether Regulation 2252/2004, read in light of Articles 7 and 8 CFR as well as the DPD, can be interpreted to mean that there is a guarantee that biometric data collected and stored pursuant to Regulation 2252/2004 may not be processed for any other purpose.[487] The Court refers to *Schwarz* to conclude that the use and storage of biometric data for the purposes of Article 4(3) of Regulation 2252/2004 are compatible with Articles 7 and 8 of the Charter.[488] The Court refers to Recital 5 of Regulation 444/2009 (the Regulation that amended Regulation 2252/2004) by which other use of personal data collected for Regulation 2252/2004, such as setting up national databases, is not provided by that Regulation.[489] According to the Court, it follows that Regulation 2252/2004 does not require Member States to guarantee that biometric data will not be used for other purposes.[490] This crucial logical step in *Willems* requires immediate attention. Contrary to the Court's view, it may be argued that it does not follow from the mentioned recital that Member States must not use biometric data for other purposes. Recital 5 clarifies that Regulation 2252/2004 does not provide a legal basis for any other use of biometric data than for biometric verification from the data contained on the passport. But this does not answer the different question on whether the provisions of the CFR, DPD and Regulation 2252/2004, all taken together, do not amount to the prohibition of using biometric data for setting up biometric databases. The Court relied on *Schwarz*, but in *Schwarz* the proportionality test was based on the fact that biometric verification was at stake, and that data are on the passport itself. In *Willems*, which concerned using biometric data for biometric databases, the Court referred to *Schwarz* without accounting for this distinction.

[485] ibid, paras 13-14.
[486] ibid, paras 33-42.
[487] ibid, para 29.
[488] ibid, para 46.
[489] ibid, para 47.
[490] ibid, para 48.

The question in *Willems* can be phrased as follows: "does EU law, and fundamental rights of privacy and data protection in particular, prohibit biometric databases set up from the biometric data collected for passports?" The Court answered something else, that Regulation 2252/2004 does not require Member States to guarantee that biometric data will not be used for other purposes. The Court achieved this by claiming that the CFR is not applicable to the second question because Regulation 2252/2004 does not govern biometric national databases, and therefore the questions is outside of scope of EU law.

The Court provided a narrow reading of the *Åkerberg Fransson* doctrine by stating that the applicability of EU law entails the applicability of the fundamental rights of the Charter, and since Regulation 2252/2004 is not applicable to the question of national biometric databases, so likewise the CFR is not applicable.[491] In essence, the Court stated that because Regulation 2252/2004 does not regulate national biometric databases, the issue of national biometric databases does not concern EU law (or fundamental rights). In *Åkerberg Fransson*, the Court reflected on the scope of application of fundamental rights and the relation between fundamental rights and the national law of Member States, concluding that the Court cannot examine the compatibility of the CFR with national law which is outside its scope.[492] However, by applying such a narrow, out-of-context reading of *Åkerberg Fransson* to *Willems*, the Court essentially held that national law concerning the processing of personal data of EU citizens is outside the scope of EU law because Regulation 2252/2004 does not mention such processing. But this misses the point that the processing of biometric data limits fundamental rights and must be justified, as the Court already established in *Schwarz*. The processing of biometric data, even in the context of national databases, is an issue of EU law because such processing limits fundamental rights. *Willems* means that if Member States use biometric data for purposes other than those stated in Regulation 2252/2004, then this is an issue not covered by EU law (and thus not prohibited by EU law). The effect is that Member States may freely create biometric databases from biometric data collected for the purpose of Regulation 2252/2004, even though the Regulation stipulates that such biometric data are used only for the purposes of verification of the identity of the traveller and the authenticity of the passport. This logic of deference to

[491] Case C-617/10 *Åkerberg Fransson* ECLI:EU:C: 2013:105.
[492] ibid.

Member States at the expense of the fundamental rights of individuals was criticised at the time.[493]

The correct decision should have been that the processing of biometric data limits fundamental rights, as was established in *Schwarz*. Further, the decision should have stated that setting up biometric databases is such a limitation which must be justified and that biometric databases limit fundamental rights more severely than biometric verification from biometric data contained on the passport medium. Thus, biometric identification and biometric databases require a different proportionality assessment, which must consider the greater infringement caused to the privacy and data protection of individuals. The Court wanted to avoid this more challenging proportionality assessment altogether, so it employed some of its tools of smoke and mirrors to slightly misuse *Schwarz*, answer a different question from the one that was really posed by the national court, and provide an extraordinarily narrow interpretation of the scope of fundamental rights.

The *Willems* judgment can also be juxtaposed with the *Digital Rights Ireland* judgment. In *Digital Rights Ireland*, the Court examined the compatibility of the Data Retention Directive (DRD) with Articles 7 and 8 CFR. The Court stated that the DRD failed the necessity and proportionality test of Article 52(1) CFR, because there were insufficient guarantees that the personal data would not be misused. In *Digital Rights Ireland*, the Court further stated that the existence of interference with fundamental rights is not related to the level of inconvenience that the persons affected suffered.[494] Another important points raised by Court in *Digital Rights Ireland* is that subsequent use of personal data without the knowledge of the person affected is likely to generate the feeling that their private lives are the subject of constant surveillance,[495] something that is perhaps even more applicable in the case of biometric databases. The Court in *Willems* avoided the issue of fundamental rights compliance by framing the issue as a matter of purely national law.

3.2.3. Case C-70/18 *A, B and P*

This case concerned Turkish nationals who applied for temporary residence permits in the Netherlands. They were required to submit fingerprints and a facial image for a Dutch national

[493] Steve Peers, "Biometric Data and Data Protection Law: The CJEU Loses the Plot' EU Law Analysis (17 April 2015) https://eulawanalysis.blogspot.com/2015/04/biometric-data-and-data-protection-law.html.
[494] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238, para 33.
[495] ibid, para 37.

database. The applicants appealed because they did not want to submit their biometric data. The appeal was dismissed. A legal action was filed by the applicants before the Hague District Court. This court decided their action was founded, but on appeal of this decision, the Dutch Council of State referred the issue to the CJEU. The question posed by the Dutch court to the CJEU was whether the requirement of Dutch law to collect biometric data is a measure restricting the free movement of legally residing Turkish citizens. Such a measure is prohibited under Article 7 of Decision 1/80 (EEC - Türkiye Association Agreement). If the requirement to collect such personal data is a prohibited measure, the question then is whether this measure can be justified by the objective of preventing identity and document fraud. The CJEU quickly established that the measure in the case at hand was indeed prohibited by Decision 1/80; that is, unless it falls under Article 14 of Decision 1/80 or is "justified by an overriding reason in the public interest, [it] is suitable to achieve the legitimate objective pursued and does not go beyond what is necessary in order to attain it".[496]

The Court proceeded with an analysis of whether the requirement to collect and store biometric data of Turkish nationals who apply for a residence permit in the Netherlands can be justified as an overriding reason in the public interest. The Court first stated that the objective of preventing unlawful entry and residence constitutes an overriding reason in the public interest.[497] Secondly, the Court reiterated *Schwarz* by stating that preventing fraudulent use and falsification of passports is an objective of public interest recognised by the European Union, namely the prevention of illegal entry into its territory[498] Thus, the Court compared on equal grounds the overriding reasons in the public interest that justify the limitation of Decision 1/80 and the objectives of general interest which justify the limitation of fundamental rights. In the factors analysis in this thesis, one factor is the "purpose" of a biometric scheme, which in a similar manner examines the different types of reasons that can be equally useful in justifying a biometric scheme.[499]

The method of the collection and retention of fingerprints pursues such an objective of prevention of illegal entry into the territory.[500] Thirdly, the Court in *A, B and P* then highlighted the importance of the fight against identity fraud, which is apparent from Article 2(c) of Regulation No 767/2008 and Article 2(2)(b) of Regulation 2019/817. Taking these reasons into

[496] Case C-70/18 *A, B and P* ECLI:EU:C:2019:823, para 44.
[497] ibid, para 46.
[498] ibid, para 47.
[499] See 3.3.2.9 of the thesis.
[500] Case C-70/18 *A, B and P* ECLI:EU:C:2019:823, para 47.

account, the Court safely concluded that the objective of preventing and combating identity and document fraud may constitute an overriding reason in the public interest which can justify a "new restriction" within the meaning of Article 13 of Decision No 1/80.[501] After establishing that an overriding reason in the public interest exists, the second requirement for justifying a measure is whether the national measure of collecting and storing fingerprints is suitable for achieving the objective. The Court concluded that the collection of ten fingerprints and a facial image of third-country nationals in a database indeed makes it possible to determine identity and discover document fraud by comparing the biometric data in the database against the biometric data of the applicant.[502]

The Court then turned to the question whether the measure at hand went beyond what is necessary for the stated objective. The Court recalled the *Schwarz* judgment where it determined that fingerprints and facial image are personal data. The derogation and limitation of rights contained in Article 7 and 8 CFR are allowed only if strictly necessary, for which the Court, in paragraph 56 of *A, B and P* recalls the important Opinion 1/15.[503] Member States must verify that the applicant for a temporary residence permit has not previously submitted an application under a different identity.[504] Citing *Schwarz,* the Court stated that the collection of such data as ten fingerprints and a facial image is not of an intimate nature and does not cause discomfort.[505] Moreover, Regulation No 767/2008 requires similarly the processing of fingerprints and facial images.[506] The Dutch measure of collecting biometric data applies to all third country nationals and the objective cannot be achieved if the measure is limited to a certain category of third country nationals.[507]

The Court then proceeded to analyse the concrete conditions of the processing of biometric data, such as that the access and use of biometric data is limited to officials who are tasked with establishing or verifying the identity of third country nationals.[508] A further argument in this analysis of proportionality *strictu sensu* is regarding the duration of the retention of biometric data, "objective criteria that establish a connection between the personal data to be retained and the objective pursued" according to Opinion 1/15. Namely, biometric data are retained for

[501] ibid, para 49.
[502] ibid, para 51.
[503] ibid, para 56; Opinion 1/15 of the Court ECLI:EU:C:2017:592.
[504] Case C-70/18 *A, B and P* ECLI:EU:C:2019:823, para 57.
[505] ibid, para 58.
[506] ibid, para 59.
[507] ibid, para 61.
[508] ibid, para 62.

(only) five years following either the rejection of the application, the end of legal stay or the expiry of the period of validity of an entry ban or a declaration of undesirability.[509] Biometric data are also immediately destroyed if the person is naturalised.[510] The Court concluded thus that the five year retention period in all these cases is not excessive.[511] With these considerations in mind, the measure which requires the collection and storage of biometric data is justified by the objective of preventing and combating identity and document fraud.[512]

The second question that the Dutch court posed to the CJEU is provoking and also reveals some of the main concerns related to the collection of biometric data. The Dutch court asked whether national law which allows biometric data to be shared with third parties[513] for the purposes of law enforcement is also a restriction of free movement of Turkish citizens in the scope of Decision 1/80.[514] The Court managed to avoid answering the question about whether not only the collecting and storing of sharing biometric data but also the sharing of them with third parties is allowed. The Court stated that the issue of sharing biometric data with third parties is purely hypothetical and thus not suitable for being answered in the case at hand. The Court claimed that this is because the biometric data of Turkish citizens subject to the said Decision can be shared with third parties only for the purpose of the detection and prosecution of criminal offences. Moreover, this sharing of biometric data can only happen in cases of criminal offences for which detention may be imposed and where there is a suspicion that the third country national committed those offences. Since in the case at hand there was no indication that A or B were suspects of such crimes, the Court considered the issue of sharing their biometric data with third parties was hypothetical and thus not suitable to be answered.[515]

Biometric data are a key issue in this judgment. Biometric data were gaining in importance because travel documents required them as did many databases. The *A, B and P* case is a significant one concerning biometrics and can be put together with *Schwarz* and *Willems* among the core judgments of the CJEU that still determine what can be called EU biometric law. *A, B and P* is a clear continuation of the Court's jurisprudence from *Schwarz*, and it raises a number of important points. These are considerations of proportionality in biometrics and the importance of legal distinction between biometric verification and identification. Further, *A, B*

[509] ibid, para 64.
[510] ibid, para 64.
[511] ibid, paras 63-68.
[512] ibid, paras 69-70.
[513] See also 3.3.2.7 of the thesis where the issue of access to biometric data by third parties is discussed further.
[514] Case C-70/18 *A, B and P* ECLI:EU:C:2019:823, para 72.
[515] ibid, paras 72-76.

and P brings to the forefront the importance of the length of the retention period for biometric data. Finally, *A, B and P* is important because it touches upon extending the permissive approach of *Schwarz* to biometrics towards the use of biometrics in EU biometric information systems, such as VIS and their interoperability. In *A, B and P* the CJEU demonstrated an increasing understanding of biometrics in the legal context. The Court considered the method of collection of biometric data, the length of storage, the purpose of processing biometric data and the possibility of access to biometric data by third parties. These will be assessed as some of the parameters in the case study of Eurodac further in this chapter of the thesis.

In *A, B and P*, the Court relies on *Schwarz* but does not recalculate the proportionality exercise due to the fact that there are ten fingerprints mandated for collection and storage, not two as was the case in *Schwarz*. How is it that two fingerprints are enough in the case of *Schwarz*, but ten are necessary in *A, B and P*? If the collection of ten fingerprints is equally burdensome to the privacy of individuals as the collection of two fingerprints, how is it the Court stressed in *Schwarz* that the fact that only two fingerprints are collected, and no more, speaks of the proportionality of the measure in *Schwarz*? These questions remained unanswered after *A, B and P*. If the Court found it (politically) prudent, it could have struck down the collection of ten fingerprints in *A, B and P* as unproportionate, relying exactly on its analysis in *Schwarz*. Of course, the Court writes the narrative as it sees fit, and the narrative is that *A, B and P* follows on from *Schwarz* legally and logically. It could be said that in *Schwarz*, the Court used the proportionality test as a tool, but not a tool of weighing conflicting rights and interests, but as a tool that allowed the Court to frame the decision in the way that the Court wanted it framed.

In the case of *A, B and P*, the retention period of biometric data was five years in a number of cases, including from the end of the legal stay. This means that in practice the biometric data would be retained in the database for many years, and the five-year retention period would only start to count after the end of the legal stay. Thus, a person staying legally in the Netherlands for decades, and never raising any law enforcement interest, would have his biometric data retained for much longer than the person whose application to stay was rejected. This fact could have easily been interpreted as not proportionate to the purpose of the measure, but the Court did not go there.

The most important message of the Court in *A, B and P* comes from not answering the second question. The Court declared inadmissible the question submitted by the Dutch Court on whether the access to biometric data that may be given to law enforcement authorities also

constitutes a new measure because the Court considered such a question hypothetical. This is an important issue since it touches upon whether and how biometric data can be repurposed. The reasoning of the Court in *A, B and P* makes way for the centralised storage of personal data. Thus, *A, B and P* is relevant for implicitly allowing the collection, storage and sharing of biometric data, particularly of migrants, in EU biometric information systems such as Eurodac, SIS and VIS and justifying their interoperability as proportionate to the goals of public authorities.

3.2.4. Case C-205/21 *Ministerstvo na vatreshnite raboti:* Processing of Biometric Data for Law Enforcement Purposes

In the last few years, there has been a series of judgments before the CJEU which originate from Bulgarian courts. These cases concern the processing of biometric data, but in the specific circumstances of criminal procedure. These cases exemplify that when it concerns law enforcement, conditions concerning the storage of biometric data, the type of biometric technologies and other factors are stricter. It is more justified to restrict fundamental rights of persons who are associated with criminal activity than it is for migration or border control purposes. The same dynamic of greater permissiveness for biometric data in the context of law enforcement can be observed before the ECtHR, where that Court has allowed longer storage periods especially in cases concerning serious crimes, or in cases concerning convicted persons as opposed to persons only suspected of a (serious) crime.[516]

Case C-205/21 *Ministerstvo na vatreshnite raboti* concerned criminal proceedings against two companies for tax fraud. The natural person V.S. was accused of participating in a criminal organisation. V.S. refused consent to the collection of dactyloscopic and photographic data and to the taking of a sample for creating her DNA profile.[517] The police did not collect the data, and the matter was brought before the referring court. What is already interesting is that the police did not forcefully take the required biometric data. In the case of an irregular migrant, the police would use coercion to forcefully fingerprint the migrant. This shows the different status that even suspected criminals enjoy in relation to the processing of biometric data.

At the point of the referral, there was a certain level of evidence of guilt of V.S., collected by the police, but there was no conviction. The referring Bulgarian court was not sure whether

[516] See the analysis of the case law of the ECtHR in 2.8.2 of the thesis.
[517] Case C-205/21 *Ministerstvo na vatreshnite raboti* ECLI:EU:C:2023:49, para 37.

Bulgarian legislation that prescribes the creation of police records is compatible with EU law. Bulgarian law which stipulates the creation of such police records including biometric data refers, wrongly, to the GDPR instead of the LED as the basis for the processing of biometric data. Thus, one task of the CJEU was to answer whether this mistake is relevant for the procedure in question. The Bulgarian criminal court referring the questions stated that Article 9(2) GDPR seems to prohibit the processing of biometric and genetic data, and that law enforcement was not an exception listed in that Article.[518] The purpose of the processing of biometric data was national security, combating crime, and maintaining law and order.[519]

In Case C-205/21 *Ministerstvo na vatreshnite raboti*, the CJEU found that the processing of biometric (and genetic) data by police authorities is allowed for the purpose of law enforcement if based on a sufficiently clear and precise national law prescribing such processing, even if this national law mistakenly refers to the GDPR instead of the LED. The CJEU determined that the processing of biometric data under the LED is allowed only if it is strictly necessary, with required safeguards, while the processing of biometric data under the GDPR is prohibited, but with a list of exceptions. Thus, there must no ambiguity in the interpretation of national law about which one is the correct legal basis. If there is a conflict between national provisions that seem to allow and those that seem to preclude data processing, the solution to the conflict is to favour the interpretation that secures the effectiveness of the LED. The CJEU stated that distinct categories of data subjects, such as those convicted as opposed to those only suspected of a crime, must be treated differently regarding interference with their fundamental rights. The CJEU concluded that Article 10 LED, which sets the conditions for the processing of special categories of data (including biometric data) read with the LED principles of lawfulness, fairness, legitimate purpose and data minimisation, prohibits national legislation which requires the systematic collection of biometric and genetic data of persons accused of an intentional offence if such national legislation does not provide that the competent national authorities can verify that it is strictly necessary and that there are no other means available that cause less serious interference with the rights and freedoms of the data subject.[520]

Another CJEU judgment as a direct continuation of the case above was issued in Case C-80/23[521] where the same Bulgarian court was unsure of how to implement the strict necessity

[518] ibid, para 40.
[519] ibid, para 48.
[520] This paragraph was previously published by the author in "Biometric Borders Envisaged by Frontex: Fundamental Rights in the Backseat" (2024) 9(2) European Papers, 621-640.
[521] Case C-80/23 *Ministerstvo na vatreshnite raboti* ECLI:EU:C: 2024:991.

review of processing biometric data for the purpose of police records. The CJEU did not break new ground, but reiterated its conclusions from Case C-205/21 *Ministerstvo na vatreshnite raboti*, stating that it is up to competent national authorities to carry out the assessment of compliance of processing biometric data with Article 10 LED.

3.2.5. Conditions for the Storage of Biometric Data in Police Records: Case C-118/22 *NG v Direktor na Glavna direktsia "Natsionalna politsia" pri Ministerstvo na vatreshnite raboti*

The facts of this case concerned a person, NG, whose request to be removed from the national records following rehabilitation was refused.[522] The question was, in essence, whether EU law, in particular the LED provisions concerning data minimisation and the rights of the data subject, prevented Bulgarian national law from the indefinite storage and access to biometric data, even after the person has otherwise been rehabilitated. NG was convicted for failing to tell the truth as a witness and was given a one-year suspended sentence. After serving that sentence, NG was rehabilitated. NG requested that his genetic and biometric data be removed from the police database. His request was denied by a Bulgarian court on the grounds that legal rehabilitation is not a ground for erasure from police records.[523] NG brought an appeal before the Supreme Administrative Court in Bulgaria. This Bulgarian Court referred to the CJEU to answer whether such rules are contrary to EU law. The purpose of the storage of records was twofold. On one hand, the Bulgarian law required it for the purpose of prevention, investigation, and prosecution of criminal offences. On the other hand, the purpose was also the protection of national security, to which the LED does not apply.[524]

The CJEU, in this Grand Chamber judgment, again considered the matter considering Articles 7 and 8 CFR, that is, privacy and data protection. It stated that these are not absolute rights, but can be limited in accordance with Article 52(1) CFR.[525] The Court also stated that the principle of data minimisation is an expression of the principle of proportionality.[526] In this way, the Court connected the data protection legal framework of the LED with fundamental rights, particularly Articles 7 and 8 CFR. The Court observed that the storage of biometric data is an interference with the fundamental rights of privacy and data protection and that the period of storage must be proportionate, meaning no longer than necessary for the stated purposes.[527]

[522] Case C-118/ 22 *NG v Ministerstvo na vatreshnite raboti* ECLI:EU:C:2024:97.
[523] ibid, paras 21-25.
[524] ibid, para 38.
[525] ibid, para 39.
[526] ibid, para 41.
[527] ibid, paras 42-43.

Article 10 LED lays down the rules for the processing of sensitive data (broadly corresponding to Article 9 GDPR). This processing can only be allowed when strictly necessary and merits a particularly strict review of compliance with the principle of data minimisation.[528]

The Court stated that individuals have the right to the erasure of their stored personal data if the storage of the said data is no longer necessary.[529] It is for the Member States, said the Court, to determine the storage period, within the framework of EU data protection. As a consequence, there is no obligation of Member States to define absolute time limits.[530] The storage of the personal data of persons who have been convicted of a crime may prove necessary to achieve the objectives of general interest, namely the prevention, investigation and prosecution of crimes.[531] Legal rehabilitation does not in itself render the storage unnecessary because the purposes of storage are different from the purposes of recording the person's conviction.[532] There are a number of factors to take into account to assess the storage of biometric data, which pose significant risks for the rights and freedoms of data subjects.[533] These factors include how the storage contributes to the prevention of crimes or threats to public security, the seriousness of the committed crimes, and the specific circumstances of the biometric data processing.[534] Nevertheless, national legislation which provides for the systematic collection of biometric and genetic data of any accused person is in principle contrary to the strict necessity requirement of Article 10 LED.[535] The CJEU drew parallels with the ECtHR case law, where the blanket retention of the fingerprints and DNA profiles of persons suspected of crimes was deemed to fail to strike a fair balance, being necessary due to the seriousness of the crimes, citing the *Marper* and *Gaughran* cases in this regard.[536] Thus, circumstances which determine whether the storage of biometric data is strictly necessary include the nature and seriousness of the offence, the possible connection with other ongoing proceedings, or the profile of the convicted person.[537]

In this manner, both the CJEU and ECtHR consider similar parameters, even though the CJEU analysis centres on Article 52(1) CFR while the ECtHR analyses the justification of storage

[528] ibid, para 48.
[529] ibid, para 50.
[530] ibid, para 52.
[531] ibid, para 55.
[532] ibid, para 61.
[533] ibid, para 63.
[534] ibid, para 63.
[535] ibid, para 64.
[536] ibid, para 65.
[537] ibid, para 67.

under the conditions of Article 8(2) ECHR. In conclusion, the CJEU states that there is no hard and fast rule on the allowed length of the storage of biometric data, but certain circumstances must be taken into account and there has to be a periodical review of whether the storage is still necessary.[538] This judgment shows that the CJEU is not willing to put a strict limitation on how long public authorities can store biometric data, but it tries to provide points for assessing the legality of the length of storage developed from data protection and the privacy rights of individuals.

3.2.6. Case C-61/22 *RL v Wiesbaden:* Biometrics Reaffirmed as Justified

This crucial recent judgment concerning biometric data processing can be summarised in a deceptively simple way. In it, the CJEU decided that Regulation (EU) 2019/1157, requiring every identity card to contain biometric data in the form of two fingerprints and a facial image, is invalid. The reason for the invalidity is that the Regulation was adopted on a wrong legal basis. However, the Court also engaged in a fundamental rights analysis of the processing of biometric data, and determined, as in *Schwarz* which concerned a similar requirement for passports, that the limitations to fundamental rights posed by the processing of biometric data are justified. It was clearly important for the Court not to leave any doubt that, even if the legal basis is wrong, the processing of biometric data is justified. In this Grand Chamber judgment, the Court thus puts a new coat of paint on the legitimacy of processing biometric data that had not been tackled in such a sweeping manner since *Schwarz*. The judgment is extremely interesting because the referring German Court expertly identified the most problematic issues concerning EU law and biometrics with its line of questions. One such question raised is whether one can rely on the reasoning of *Schwarz*, particularly on the objectives of general interest as established there in the context of a biometric passport, here in a case concerning an even more universally used document, an ID. The CJEU recognised the challenge and engaged in justifying the processing of biometric data in the new circumstances.

3.2.6.1. The Second German Challenge to the Use of Biometrics in the EU After *Schwarz*

The case analysed here is referred to as *RL v Wiesbaden*, but it can be argued that RL and the Court in Wiesbaden acted in concert trying to determine that the processing of biometric data

[538] ibid, paras 71-72.

in this context is contrary to European law. The Wiesbaden Court used the opportunity to probe the chinks in the armour of what can be considered the biometric law of the EU.

The facts of the case were broadly like *Schwarz*. RL applied for a new identity card because the electronic chip was defective, but did not want the ID to contain his fingerprints.[539] The City of Wiesbaden rejected his application, first because an ID remains valid even with a defective chip, according to German law. Secondly, the inclusion of two fingerprints on the storage medium of the card is required by German law which transposed such a requirement from Article 3(5) of Regulation 2019/1157.[540]

The applicant brought an action before the Administrative Court in Wiesbaden to force the City of Wiesbaden to issue him with an ID without including the fingerprints. Unusually, this Administrative Court referred to the CJEU, because it held the view that Regulation 2019/1157 was adopted on a wrongful legal basis. In most cases, one would expect that if a person refuses to provide fingerprints which are required by both national and EU law, the court will not even entertain the appeal, let alone take it to the CJEU. The German Court further considered that there should have been a data protection impact assessment as required by Article 35(10) GDPR because the collection and storage of fingerprints constitute the processing of personal data which requires such an assessment. But the most direct attack on the processing of fingerprints is the third notion put forward by the German Administrative Court in Wiesbaden, by which it asked the CJEU to assess whether the requirement to process fingerprints for the purpose of IDs is compliant with Articles 7 and 8 CFR, namely privacy and data protection rights. This last question is really an existential threat to the use of biometrics in EU law. If the processing of fingerprints for the purpose of IDs is contrary to fundamental rights, then generally the use of biometrics in the context of migration and border control might also be unjustified. On the other hand, it is interesting that *Schwarz*, ten years earlier, responded that biometric processing is a justified limitation of fundamental rights. In *RL v Wiesbaden*, the Court decided to entertain the big question again.

The German referring Court provided three good reasons that call into question the validity of the processing of fingerprints for the purpose of storage in IDs. The argumentation reveals that the Wiesbaden Court had an excellent grasp of how biometrics relate to EU law. The first argument for the processing of fingerprints being contrary to fundamental rights, according to

[539] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, para 26.
[540] ibid, para 27.

the referring Court, is that the limitation does not meet the objective of general interest. The Wiesbaden Court anticipates the *Schwarz* analogy that the CJEU might raise by differentiating identity cards from passports. The identity card is not a travel document primarily, unlike passports, so the same objective of general interest should not be applicable in *RL v Wiesbaden*. Thus, combating illegal entry into the EU, which was recognised in *Schwarz*, might not be applicable here. Secondly, the limitation posed by fingerprints may not be proportionate. Again, the German court anticipates a counterargument by stating that the *Schwarz* reasoning is not applicable in this case, because *Schwarz* involves passports and not IDs. In particular, the German court stressed that the processing of fingerprint data for the purpose of IDs represents a greater limitation of fundamental rights than in the case of passports. This is because up to 370 million EU citizens are required to have an ID. Article 3(5) of Regulation 2019/1157 represents a limitation of fundamental rights for 85 per cent of the EU population, which in turn requires a stronger justification under the test of strict necessity than in the case of passports, which are less widely used.[541] It also adds that a strict review of proportionality follows from Article 9(1) GDPR, which generally prohibits the processing of biometric data unless there are exceptional circumstances.[542] The German Court stressed that there are techniques such as holograms and watermarks, which are less intrusive yet also prevent the falsification of documents and enable the verification of authenticity (of course, since the real reason is to check persons by their biometrics, and not, as it is claimed, to check the authenticity of documents).

The German court at the end provided an interesting additional argument by stating that the risk of unauthorised access to fingerprints that are stored locally on a chip is far from negligible, and thus local storage might not be more secure than storage in a remote database. Electronic chips could be read by unauthorised scanners.[543] This argument rings true. There is an implicit idea that local storage is better for the privacy of the person than remote storage, because with local storage the person controls their own data. But it is also true that a natural person might not be able secure their data properly and might be a victim of various security breaches and

[541] ibid, para 35.

[542] This interpretation by the German court also implicitly means that it considers the processing of fingerprints for the purpose of verification to be the processing of sensitive data, which is the position of this author as well, as previously stated. Interestingly, the Court agreed that in the case at hand, there is the processing of sensitive personal data (see para 72; 106-107). However, this was more due to the fact that neither court consistently analysed verification and identification in the present case than it was the result of a deliberate strategy to clear up the uncertainty concerning the definition of biometric data.

[543] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, para 40.

frauds. In some ways, local storage is less secure than remote storage. The advantage of local storage is that the responsibility for privacy lies with the person, but this does not make it more secure. Overall, the German court in *RL v Wiesbaden* provided a serious challenge to the use of biometrics by public authorities in the EU.

The Court considered the questions in three parts. First, it answered whether the legal basis for Regulation 2019/1157 is correct. Second, whether there should have been a data protection impact assessment. The largest part of the Court's analysis was taken by the third issue, namely whether the obligation to process two fingerprints for the purpose of an ID is contrary to Articles 7 and 8 CFR.

3.2.6.2. A First: The CJEU Strikes Down Biometric Legislation

In its first question, the referring national court inquired whether the legal basis for Regulation 2019/1157 is incorrect. Namely, Article 21(2) TFEU gives the EU the power to adopt provisions to facilitate free movement. This was the Article that served as the legal basis for the regulation which stipulated the requirement that IDs must have fingerprint and facial image data. On the other hand, Article 77(3) TFEU gives the EU power to adopt measures relating to ID cards, passports and residence permits. In *Schwarz*, the Court ruled that biometric passports are based on what is now 77(3) TFEU.[544] The Court in *RL v Wiesbaden* agreed that the legal basis for biometric IDs was wrong. Article 77(3) TFEU is the appropriate legal basis, not Article 21(2) TFEU, because 77(3) TFEU is more specifically envisaged for the purpose of regulating IDs. The arguments in favour of using Article 77(3) TFEU are extraordinarily strong. As the Court observes, Article 77(3) TFEU expressly gives power to adopt legislative acts concerning passports and IDs. This Article is found in Title V TFEU, which concerns the area of Freedom, Security, and Justice, or more specifically, in Chapter 2 which carries the title "Policies on border checks, asylum and immigration".[545] As a result, the Regulation is invalidated. The effects of the Regulation are maintained until a new Regulation based on Article 77(3) TFEU enters into force, but no longer than 1 January 2027.

The EU legislator can be criticised for the incorrect legal basis of Regulation 2019/1157. Article 21(2) TFEU provides the legal basis for provisions which facilitate the right to free movement. The Court rejected this legal basis, but it nevertheless upheld the fiction that the introduction of

[544] ibid, para 44.
[545] ibid, paras 50-51.

a new requirement (effectively, a new restriction) for a travel document facilitates free movement. It is as if the Court (or the Commission) claimed that the introduction of a non-tariff barrier to trade, such as an additional veterinary inspection of meat, facilitates the free movement of such goods by making sure it is good to consume. Likewise, requiring fingerprints and a facial image to be stored on an ID is an additional requirement, so it takes a leap of logic to claim that this additional requirement acts as a catalyst for free movement, instead of being a restriction. The approach shows just how genuinely thin the justifications of biometrics in EU law are.

The Court engaged only briefly with the second question concerning whether there was an obligation set by the legislator for an impact assessment to be conducted prior to the enactment of the regulation. It concluded that there was no obligation to conduct an impact assessment, but the reasoning the Court provides is quite original. Namely, the Court states that Regulation 2019/1157 does not itself process personal data, but "merely" provides for Member States to carry out the processing when an application for an identity card is made.[546] It is unclear how a piece of legislation could process personal data in the sense of the reasoning of the Court. A law is not the data controller or data processor. It is always the natural or legal person that carries out the processing determined by Member State or EU law.[547] From the fact that the law itself does not process personal data, but only mandates the processing, the Court concludes that an impact assessment was not required for Regulation 2019/1157.[548]

3.2.6.3. The Third Act: Reaffirming the Legitimacy of the Processing of Biometric Data

The third ground for the invalidity of Regulation 2019/1157 advanced by the referring court is whether the obligation to include two fingerprints in the storage medium of identity cards, as laid down by Article 3(5) of that Regulation, entails an unjustified limitation of rights under Articles 7 and 8 CFR. This question is broad in scope because it implies that biometric data processing is contrary to fundamental rights. One could say that the stakes were high, but also that the game was rigged, since it should not be expected of the CJEU to effectively prohibit biometrics, which have become an essential tool of public authorities in all Member States. It was clearly important for the CJEU to answer the third question, even though it had already established that Regulation 2019/1157 was invalidated. The CJEU wanted to make sure that the

[546] ibid, paras 65-66.
[547] Regulation (EU) 2016/679, Article 4(7)-(8).
[548] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, paras 66-68.

legitimacy of biometrics is not questioned even after the invalidation of the Regulation. The Court thus proceeded with a familiar fundamental rights analysis of the processing of fingerprints.

Firstly, recalling *Schwarz*, the CJEU stated that Articles 7 and 8 CFR should be read jointly to mean that the processing of personal data is a threat to these fundamental rights.[549] The processing of two fingerprints and storing them in the medium of the ID, as in this case, represents the processing of particularly sensitive personal data, and therefore constitutes a limitation of both the right to private life and the right to the protection of personal data.[550] The Court also distinguished two operations, namely the collection of fingerprints and their temporary storage while the card is being made, for the purposes of personalisation of identity cards.[551] This shows the value of analysing a biometric system via its parameters, such as storage, collection access, and so on, that will be applied further in this chapter using the example of Eurodac. However, it is surprising that the Court distinguishes collection and the temporary storage by public authorities and does not mention here long-term local storage as an additional operation on personal data. Even if biometric data are stored under the physical control of the person involved, this still represents a limitation of privacy. After all, citizens are forced to have their biometric data stored locally, which is not a matter of choice, so this operation of storage on a chip should also be taken into account. As it stands, the Court focused at this point on the short-term storage that lasts until the card is made, after which the fingerprint data are erased from this central storage and rest solely on the card itself.

The Court examined the justification for the limitation of privacy and data protection through Article 52(1) of the Charter. It considered whether these limitations are provided by law, whether they respect the essence of those rights and whether the principle of proportionality is complied with, meaning that limitations are necessary and genuinely meet the objective of general interest recognised by the EU or the need to protect the rights and freedoms of others. In this last regard, Article 8(2) of the Charter states that personal data must be processed for specified purposes and based on the consent of the person or some other legitimate basis laid down by law.[552]

[549] ibid, para 70.
[550] ibid, paras 72-73.
[551] ibid, para 74.
[552] ibid, para 76

The Court first stated that concerning the principle of legality (being based on law), limitations are defined clearly and precisely by the (invalidated) Regulation. Secondly, the information contained in fingerprints is not such as to adversely affect the essence of fundamental rights in Articles 7 and 8.[553] One could argue that the legal provisions requiring fingerprinting are quite general and lack precision, especially since the procedure as well as the exact technology used are left to the public authorities of a Member State. The argument concerning "essence" is very rarely successfully applied. The Court claimed that the conclusions from the case *Ligue de Droits Humains* can be applied in *RL v Wiesbaden* analogously.[554] In *Ligue de Droits Humains*, the Court concluded that the processing of the Passenger Name Record (PNR) does not infringe the essence of fundamental rights in question.[555] PNR data reveal the name and nationality of the passenger as well as information relating to the flight, including the travel date and itinerary.[556] PNR data are completely different from biometric data. The Court in *Ligue de Droits Humains* relied on the fact that the PNR Directive expressly stated that PNR data may not include sensitive data. On that basis, the Court in *Ligue de Droits Humains* concluded that the processing of PNR data does not adversely affect the essence of fundamental rights in question.[557] The Court thus engaged in a game of Chinese whispers, transplanting the conclusions from *Ligue de Droits Humains* to the completely different factual situation in *RL v Wiesbaden*, where it stated that biometric data are sensitive. Simply put, the Court stated that the processing of sensitive, biometric data does not infringe the essence of fundamental rights because the processing of non-sensitive personal data also does not infringe the essence of fundamental rights. Both arguments concerning legality and essence are for the Court as the final arbiter to decide. The true weighing of the arguments lies in the proportionality assessment part of the judgment.

The Court determined that combating document fraud, including falsification of identity cards and identity theft, constitutes an objective of general interest recognised by the EU. The objective of interoperability of identity documents is also of general interest, according to the Court, because it contributes to facilitating the exercise of free movement of EU citizens.[558] Mentioning interoperability as a general objective of the EU should be criticised. Interoperability should be seen as a tool for achieving certain other objectives that are in the

[553] ibid, paras 77-81.
[554] ibid, para 81.
[555] Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* ECLI:EU:C: 2022:491, para 120.
[556] ibid, para 31.
[557] ibid, para 120.
[558] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, paras 86-88.

general interest of the EU and its population. But, in itself, the interoperability of documents is not in the interest of the EU population. The Court failed to make this distinction between the means and the objectives. This point will be further elaborated when discussing interoperability later in this chapter.

As a second step of the proportionality analysis, the Court determined that the inclusion of two fingerprints in the storage medium of identity cards is appropriate for meeting the objectives of general interest.[559] The reasons are that the inclusion of fingerprints makes is more difficult to falsify identity cards and, secondly, makes it easier to verify the identity of the holder. Including complete fingerprints is appropriate because only complete fingerprints allow interoperability, claimed the Court. These observations can be criticised. It is true that biometric data make the verification of identity much more reliable. But there may be other methods, as mentioned by the German court, such as holograms, that can make identity cards safer. Secondly, the inclusion of whole fingerprints instead of only parts of fingerprints or *minutiae* (parts of distinctive whorls of the fingertip) does make it easier to make the fingerprint data compatible with different fingerprint recognition systems. This is because different fingerprint algorithms may look at different parts of the fingerprint to make the verification, so having the whole fingerprint stored makes it possible to use a number of different systems. However, it is also the opinion of this author that including the whole or only key parts of a fingerprint does not have any effect in terms of the infringement of privacy, making the debate on *minutiae* redundant. As will be explained in the part concerning biometric templates, it does not make much substantive difference whether a part of biometric data was removed if the part that remained equally serves the purpose of identification or verification. In this case, it is doubtful whether it would be beneficial to the privacy and data protection of individuals if certain parts of the fingerprints were omitted. The privacy of the person is equally limited in either case.

In the process of determining that the measure of including two fingerprints is necessary for the purpose of achieving objective of general interest, the Court included two interesting arguments. First of all, the Court stated that including two fingerprints in addition to a facial image is more effective since ageing, lifestyle, illness, plastic or reconstructive surgery may alter the face.[560] If this argument is true, then one can raise the question of whether there is any need to include the facial image, in addition to fingerprints, especially since a facial image

[559] ibid, para 89.
[560] ibid, para 99.

reveals a lot even to the naked eye, unlike fingerprints which are not understandable without technical tools. However, this case cleverly avoided an analysis of the proportionality of facial images, focusing only on fingerprint data.

The second interesting argument is that the Court considered the impact assessment of the Commission which accompanied the proposal for the regulation which would give rise to Regulation 2019/1157 (which is a separate matter from the hypothetical data protection impact assessment of Article 35(10) GDPR). Contrary to the Court's line of reasoning, this impact assessment concluded that there should not be a requirement to include two fingerprints.[561] The Court stated that the impact assessment's conclusion does not prove that the inclusion of two fingerprints is not necessary in the present case. But the Court failed to provide reasons to counter the conclusion of the Commission's impact assessment, besides the claim that this impact assessment of the Commission is not obligatory.

The Court in the final step conducted a balancing exercise between the seriousness of the interference of including two fingerprints and the objectives for which this is pursued. The seriousness of the interference is high in the present case, because it affected a large number of persons (most of the EU population are required to have identity cards) and because fingerprint data, as biometric data, are particularly sensitive.[562] On the other hand, the Court stressed that the storage of fingerprints is only local on the cards and that there are safeguards to limit the risks for personal data. These safeguards are not particularly reassuring, in the opinion of this author. These include that only duly authorised staff should have access, and further that the storage will be highly secure.[563] The significance of the objective lies in facilitating free movement, the Court reiterated at this point.[564] Finally, the Court balanced the interference with the objectives and concluded that the limitation of privacy and data protection is justified. The Court could be criticised for reusing similar arguments at different points in its analysis, but the result seems never to have been in question. The most important message of the Court is that limitations of fundamental rights caused by the processing of fingerprint data are justified, even if Regulation 2019/1157 is invalid. The message was that there can be no doubt that biometrics are here to stay, even if adopted under a wrong legal basis.

[561] ibid, para 100.
[562] ibid, para 107.
[563] ibid, paras 111 and 118.
[564] ibid, paras 119-120.

3.3. Biometric Parameters: Case Study of Eurodac as a Biometric System

3.3.1. The Methodology for the Analysis of Biometric Parameters

Any biometric system has a certain minimal number of elements, here called (biometric) parameters, which need to be set for a biometric system to operate. A biometric system means any system that uses biometric technologies for biometric identification or verification. Examples of biometric systems include systems for the verification of identity of passport holders, or any of the biometric information systems of the EU, including Eurodac, which may be used for both biometric verification and identification. From a technical point of view, any biometric system must likewise define rules for collection, storage, transfer of (biometric) data, the overall infrastructure but also be guided by the purpose for which the biometric system is built. This is why the adopted approach in this section is to analyse the biometric parameters of a biometric system using the example of Eurodac.

Thus, most important cases concerning biometrics can be presented in view of these biometric parameters. Processing involves any operation performed on personal data.[565] Any operation conducted upon personal and biometric data, such as collection or storage, represents a separate limitation of fundamental rights (*RL v Wiesbaden, Schwarz)* and similarly any interference with the human right to private life must be justified (*Marper, Gaughran*).[566] The CJEU has found that the collection and storage of fingerprints and facial images of third-country nationals in a database must satisfy all the requirements imposed on the processing of personal data.[567]

This part of the thesis will provide a case study of the Eurodac information system by analysing the biometric parameters by which this biometric system is defined. The processing of biometric data should be understood in chronological steps, as a sequence representing different biometric parameters. First is the act of collecting biometric data by the taking of fingerprints or of a facial image. These data are transmitted to Eurodac. Transmission is the second, separate operation of the processing of biometric data. It is followed by an automatic comparison. All the biometric data in Eurodac are automatically compared against the collected and transmitted dataset. Comparison entails biometric identification. But biometric identification may or may not result

[565] Regulation (EU) 2016/679, Article 4(2).
[566] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022), 354; Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, paras 23-25.
[567] Opinion 1/15 EU-Canada PNR Agreement ECLI:EU:C:2017:592, para 123.

in the storage of biometric data, because such biometric data may already be in the database. In any case, the operation of storage is a separate, subsequent action or a biometric parameter.

There are many advantages to the approach based on the examination of parameters of a biometric system. It will allow a better understanding of how biometrics work, as a synthesis of the technical and legal basics of biometrics. The analysis will show that the difference between verification and identification, as it currently stands in legislation and in case law, is not definitive. Further, the approach will reveal that there are more operations of processing of biometric data than one might expect from judgments or legislation, particularly in view of the transfer of and access to biometric data, as will be explained in the analysis of the so-called no-hit. The parameters approach further allows a toolbox to be envisaged for assessing any biometric system, with parameters that can help assess the legality of a biometric system in view of EU law. The biometric parameters may also allow technical experts greater understanding of the legal effects of biometrics.

Finally, this methodology has constraints. First, it is the CJEU, as well as national courts, which provide the relevant interpretation of law, even if their interpretation may not be completely coherent. Therefore, an unusually long storage period might be justified by the courts, or an objective of general interest might be interpreted in a novel and unusual manner by the judicial authorities. Secondly, any approach is very unlikely to affect the general position of the CJEU that biometrics are justified in terms of fundamental rights. This is even though the parameters of biometric systems are becoming more restrictive towards the privacy of individuals. This is seen from the ever longer periods for the storage of biometric data, the expansion of databases and the stretching of the purposes of existing biometric databases. The CJEU may always find how to interpret the biometric parameters in a way to justify the use of biometrics. With this in mind, the focus in this part is not on a fundamental rights analysis, but on many of the parameters that feature prominently in such an analysis. The fundamental rights analysis of biometrics will be the subject of the Chapter 4.

The layout of this part is to explain Eurodac as a biometric system, then to note how Eurodac implies a different understanding of biometric data compared to the meaning of the concept in the GDPR. A discussion of the accuracy of the Eurodac biometric system will follow. Then the parameters related to the operation of Eurodac will be critically examined. These are the biometric parameters of collection, comparison, transmission, storage, access to, purpose and personal scope of Eurodac.

3.3.2. Eurodac as a Case Study of a Biometric System

Eurodac is a database established in 2003 that uses biometric data to determine in which EU State the migrant first applied for asylum. Broadly, Eurodac stores biometric data of asylum seekers (Category 1), of persons apprehended in relation to irregular border crossing (Category 2), and of persons who were found illegally staying in one of the EU Member States (Category 3). Eurodac is one of the EU's large-scale information systems in what is called the area of Freedom, Security and Justice. Eurodac serves both administrative and law enforcement purposes. Other such systems which process biometric data are the SIS, VIS, while soon to become operational are the EES and ECRIS-TCN. Biometric systems of the EU have radically changed in the recent period, particularly concerning the way in which biometric data are transmitted between them, which mostly concerns so-called interoperability.

As previously mentioned, Eurodac is one of the EU information systems established in the Area of Freedom, Security and Justice (AFSJ).[568] The specific chapters of the AFSJ correspond to the purposes for which these information systems were established: policies on border checks, asylum and immigration; judicial cooperation in civil matters; judicial cooperation in criminal matters; and police cooperation. Concerning Eurodac, this system serves the policies on border checks, asylum, and immigration as well as police cooperation.[569] Some of the other biometric information systems include the Schengen Information System (SIS), the Visa Information System (VIS) and ECRIS-TCN. The SIS includes biometrics such as palm prints, fingerprints, but also DNA records in the case of missing persons.[570] The EES, which is not yet operational, will collect fingerprints and facial images of visa-free travellers to the EU.[571] The ETIAS is another new information system, but it will not process biometric data.

The main purpose of Eurodac is to serve Regulation (EU) No 604/2013 which determines the Member State responsible for examining an application for international protection.[572] In order

[568] Article 3(2) of the Consolidated version of the Treaty on European Union [2012] OJ C326/1 (TEU); Title V of the Treaty on the Functioning of the European Union (TFEU), Articles 67 to 89.
[569] Regulation (EU) 2024/1358, TFEU, and in particular Article 78(2), points (c), (d), (e) and (g), Article 79(2), point (c), Article 87(2), point (a), and Article 88(2), point (a).
[570] Regulation (EU) 2018/1862; Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals; Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks PE/35/2018/REV/1 [2018] OJ L312/14.
[571] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes [2017] OJ L327/20.
[572] Regulation (EU) 603/2013, Recital 4.

to establish the responsible state, it is vital to determine the identity of the person. The identity of a person is determined by the biometric identification of fingerprints. In this way, biometrics are the key for the functioning of the EU asylum system. Biometric identification is also vital in relation to irregular migrants. Irregular migrants can be differentiated from seekers of international protection by the fact that they have not lodged a claim for international protection or that their claim has been rejected.

The Eurodac biometric information system is composed of a Central System, a Communication Infrastructure, and the Common Identity Repository (CIR). There is also a Secure Communication Infrastructure used for the transfer of data between the Central System and the European search portal (ESP) and between the Central System and the CIR.[573] The ESP and CIR are elements of interoperability which are shared by all biometric EU large-scale information systems. The CIR contains fingerprints, facial images, and biographical data.[574] In addition, there are national Eurodac systems.

The currently applicable Eurodac regulation[575] from mid-2026 will be replaced by the 2024 Eurodac Regulation.[576] The subject of this analysis will primarily be the new 2024 Eurodac Regulation. This is done to make the discussion here applicable even after the imminent changes take place in 2026. In the newer legislation, Eurodac is envisaged as part of a larger, interoperable EU system of biometric and personal data. The 2024 Eurodac is centred on the notion of biometric data (mentioned 160 times) while the 2013 Eurodac regulation did not mention biometric data at all, instead only referencing fingerprint data. The new Eurodac regulation is also more pertinent to the analysis because it prescribes the biometric parameters, analysed here, in more detail, stipulating separately the conditions for collection, transmission and storage for each category of persons whose biometric data it processes. The 2024 Eurodac will also process facial images, in addition to existing fingerprint data. Vavoula considers rightly that it is surprising that an additional type of biometric data was added while existing rules requiring a full set of fingerprints were not changed.[577] The storage period for biometric data has been increased in the 2024 Eurodac Regulation. Most importantly, access to biometric data for the purpose of law enforcement has been made easier in the 2024 Eurodac Regulation

[573] Eurodac 2024, Article 3.
[574] Regulation (EU) 2024/1358, Article 3(2).
[575] Regulation (EU) No 603/2013.
[576] Regulation (EU) 2024/1358.
[577] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022) 384.

in comparison with the 2013 Regulation. Another momentous change is that the age of enrolment of persons into Eurodac has been lowered from fourteen to six years. This means that biometric data of children as young as six years will be processed, and with force if necessary. There are also changes concerning the linking of the datasets of a single person together in more effective ways and making biometric data interoperable. Finally, in the 2024 Eurodac Regulation, Eurodac is envisaged as part of a broader migration and asylum system, together with the Screening Regulation and the Asylum and Migration Management Regulation.[578] Since the automatic comparison of facial images means the existence of facial recognition, one can say that Eurodac is without doubt an AI system as well.

3.3.2.1 Definition of Biometric Data in Eurodac 2024 Regulation

There is a semantic change from the Eurodac 2013 to Eurodac 2024 regulation. The older version is titled "Eurodac for the comparison of fingerprints(...)" while the new regulation is called "Eurodac for the comparison of biometric data". One reason is that the new Eurodac includes facial images besides fingerprints. But more important is the realisation (of the legislator) that biometric data is the more appropriate term that does not refer to a narrow notion for the purpose of a single regulation but is the same overarching concept with many applications in EU law.

Eurodac defines biometric data differently from the GDPR. Eurodac envisages biometric data in comparison to alphanumeric data. Biometric data are fingerprint and facial image data, while alphanumeric data are all other data such as biographic data.[579] The GDPR views biometric data in relation to personal data, with biometric data being a particular subset of personal data.[580] These two understandings of biometric data are not contradictory. Eurodac acknowledges that the GDPR (or the LED, in the context of law enforcement) legal framework regulates the processing of biometric data.[581] But there is a certain difference in what biometric data mean in Eurodac compared to the GDPR. In Eurodac, biometric data are opposed to alphanumeric data, with biometric data meaning fingerprint and facial image data that are distinguished from alphanumeric data (such as letters or digits) by being more precise and thus better suited for

[578] Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders PE/20/2024/REV/1 [2024] OJ L 2024/1356; Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management PE/21/2024/REV/1 [2024] OJ L 2024/1351.
[579] Regulation (EU) 2024/1358, Article 3(q) to 3(t).
[580] Regulation (EU) 2016/679, Article 4(14).
[581] Regulation (EU) 2024/1358, Recitals 13, 77, 80, and others.

identification In terms of the GDPR, the emphasis is on the notion that biometric data are more sensitive than personal data in general. Recital nine of Recast Eurodac states that biometric data are processed on the basis of substantial public interest under Article 9(2)(g) GDPR, which the author of this thesis considers to be the most important legal basis for the biometrics used by public authorities (as discussed in the previous chapter). The processing of Eurodac's biometric data for law enforcement purposes (accessing already store biometric data for comparison) is regulated by LED rules.[582]

Biometric data in the Eurodac Recast are defined as fingerprint data or facial image data.[583] Fingerprint data mean the plain and rolled impression of all ten fingers, including latent fingerprints. Facial image data mean digital images of the face with sufficient image resolution and quality to be used in automatic biometric matching.

Other important concepts in Eurodac (which clearly shows how technical jargon is creeping into legislation) are dataset and sequence. A dataset is linked into one sequence and represents the whole personal data recorded in connection to one person, which includes biometric and alphanumeric data.[584] If one of the fingerprints returns a match when compared to biometric data in the Eurodac database, all data linked to that fingerprint is retrieved.[585] Eurodac 2013 did not mention the concept of dataset. Dataset is composed of biometric data, alphanumeric data, and a scanned colour copy of an ID, where available.[586] All these can of course be viewed as personal data. Considering the way the Eurodac regulation is structured, it is the concept of biometric data that is crucial for understanding how the system operates. Biometric data are the key element of interoperability. They are used for the actual identification of persons, they are stored, compared, and protected – it all begins and ends with biometric data.

3.3.2.2. Accuracy, Quality and Multimodality in Respect of Biometric Data.

Using multiple biometric technologies in parallel increases accuracy. It is a matter of simple mathematics. If a certain algorithm operated by fingerprint recognition produces false positives once in ten thousand comparisons, and if facial recognition, used on its own, produces a false positive result also once in ten thousand comparisons, when used together, the chance of a false

[582] Regulation (EU) 2024/1358, Article 2(4); Regulation (EU) 2024/1358, Article 47.
[583] Regulation (EU) 2024/1358, Article 2(s).
[584] "Alphanumeric data" means data represented by letters, digits, special characters, space, or punctuation marks, Article 2(t) Regulation (EU) 2024/1358.
[585] Regulation (EU) 2024/1358, Article 3(6).
[586] ibid, Article 2(y).

positive is reduced to10 000 x 10 000, or once in one hundred million. Biometric multimodality, as it is known, has been recognised by EBCG (Frontex) as a tool to increase accuracy and reduce the possibility of fraud.[587] However, a similarly negative cumulative effect on privacy should also be recognised in the case of using multiple biometric technologies in parallel. Most importantly, adding another biometric technology must be necessary for achieving a certain objective of general interest. Eurodac, along with some other EU biometric systems, has taken the step of introducing facial images alongside fingerprints. These images are not merely photographs but must be capable of being used for automatic biometric comparison.

Accuracy is thus increased when both fingerprint and facial recognition are used. But this multimodality in Eurodac further limits privacy. Accuracy, however, is important because only a sufficiently accurate method can be considered as appropriate for achieving an objective of general interest of the EU. In *Schwarz*, the Court stated that the biometric verification method which uses two fingers is sufficiently accurate.[588] It is an open question why ten fingerprints are needed for Eurodac, and with the new addition of facial images as a failsafe. This shows the limits of approaching the proportionality analysis of the Court objectively.

The issue of quality has been problematic when it comes to Eurodac and other biometric systems.[589] Low quality fingerprints lead to fingerprints which are rejected by the Central System. Moreover, quality issues may lead to mistakes, including false positives and negatives. The European Court of Auditors has concluded that references to data quality in legislation is lacking, and that neither eu-Lisa nor the Commission are effectively able to evaluate, control or enforce quality issues.[590] Data quality standards for Eurodac and certain other biometric information systems, such as the VIS, are not the same. The quality of fingerprints for Eurodac, unlike the VIS, is controlled by eu-Lisa centrally.[591] The EU's Fundamental Rights Agency has expressed this concern by looking at the negative effects of the quality problems of biometric

[587] Frontex, "Technology Foresight on Biometrics for the Future of Travel" (European Border and Coast Guard Agency, 2022) www.frontex.europa.eu.
[588] Case C-291/12 *Schwarz* ECLI:EU:C: 2013:670.
[589] Fundamental Rights Agency (FRA), "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018), 17.
[590] European Court of Auditors, "Special Report No 20/2019: EU Information Systems Supporting Border Control – A Strong Tool, but More Focus Needed on Timely and Complete Data" 6 <https://www.eca.europa.eu/en/publications?did=51952> accessed March 26, 2025.
[591] Fundamental Rights Agency (FRA), "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 15.

data on data accuracy, leading to flawed administrative decisions, the possibilities of identity fraud and other issues in a report published in 2018.[592]

Eurodac defines facial image data as the digital image of a face with sufficient quality for automatic comparison.[593] This would imply that a photograph of insufficient quality would not be biometric data. Whether a photograph is biometric data or not depends on the technical nature of processing, as discussed in the previous chapter.[594] Quality sufficiency is determined by technical standards. In the case of the Eurodac system, eu-LISA sets the standards by which biometric data of insufficient quality is rejected.

3.3.2.3. The Parameter of the Collection of Biometric Data

The parameter of the collection of biometric data involves practical, technical, and legal aspects of the first gathering of biometric data. ISO terminology refers to biometric enrolment as creating and storing the biometric enrolment data record, which usually, but not always, involves the storage of such data.[595] From a technical perspective, the enrolment of fingerprints may be understood in many ways. Any number of fingerprints may be collected. In the case of Eurodac, it is ten fingerprints. In the case of biometric passports and IDs in the EU, it is two fingerprints.[596] The position of the CJEU is that the smaller the number of fingers involved in the collection of biometric data, the lesser the limitation of fundamental right of privacy (and data protection).[597] But this position, on further reflection, could be disputed. Natural persons may feel their privacy is equally infringed (and their human dignity) whether they press two or, for example, four fingers (four fingers in the case of the Entry Exit System)[598] against a scanner. This is irrespective of the fact that most EU citizens could recall that their fingerprints were being collected for the purpose of being issued with an ID or a passport. It is not necessarily true that EU citizens would perceive that their privacy was infringed to a lesser degree because of the number of fingers involved. The second problem that may be raised in relation to the number of fingers is related to the proportionality of the biometric system. Some systems, such

[592] Fundamental Rights Agency (FRA) "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018), 81-99.
[593] Regulation (EU) 2024/1358, 2(1)(r) 2024.
[594] See 2.4.2 of the thesis.
[595] International Organization for Standardization, ISO/IEC 2382-37:2022(en) Information Technology — Vocabulary — Part 37: Biometrics www.iso.org.
[596] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670; Regulation (EC) No 444/2009, Article 1(2).
[597] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C:2024:251.
[598] Regulation (EU) 2017/2226, Article 3(1)(16).

as Eurodac, necessitate all ten fingerprints, while other biometric systems, such as is the case with biometric passports or biometric IDs, consider it necessary to enrol only two index fingers. The reason for requiring a complete set of fingerprints for Eurodac was never adequately explained by the legislator.[599] In terms of Eurodac, the lawfulness of processing personal data is supervised by national supervisory authorities and the EDPS.[600]

Differences in the collection stage of fingerprinting among different operators can arise from the use of different software or hardware. There are many methods of fingerprint comparison, or what could be called algorithms for the comparison of fingerprints. Discrepancy in fingerprinting operations among Member States for the purpose of enrolment in Eurodac or another information system is also caused by the different types of hardware used to collect fingerprints, even within the Member States. The cause of diversity in equipment is that there are many suppliers of biometric systems and there is no single procurement procedure at the level of the EU. This diversity may cause problems in achieving the same standards in the collection of biometric data, although the diversity may have some benefits. There is competition among developers of biometric systems and consequently this important equipment is not sourced from a single private supplier.[601]

A distinction can be made between inked fingerprints and live-scanned fingerprints; in the first case, the fingertips are dabbed in ink which are then pressed against paper and may subsequently be transferred to digital form, while the live-scanned fingers are directly pressed against a digital scanner and processed as digital data. From a technical standpoint, fingerprints can be collected either plain or rolled. In the second case, the fingertip is rolled from side to side to create a broader image. Eurodac accepts fingerprint data as plain and rolled fingerprints of all ten fingers, or even a latent fingerprint.[602] A latent fingerprint represents a trace of grease, sweat or similar that is usually not visible by the naked eye and is collected by special equipment, e.g. from a crime scene. Latent fingerprints may present most problems in terms of quality, since only a portion of the fingerprint may be legible, which might cause incorrect matching or rejection of the fingerprint by the algorithm used by the biometric system.

---

[599] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022), 362
[600] Regulation (EU) 2024/1358, Articles 44-45 and 47.
[601] Interviews between the author and the representative of the Croatian Ministry of Interior held in 2024 and 2025 concerning Croatian police practice and the use of EU information systems.
[602] Regulation (EU) 2024/1358, Article 2 (q).

Procedures for fingerprinting, including for ensuring compliance of the data subject, are set in national administrative laws. Eurodac acknowledges fundamental rights when it comes to collecting biometric data.[603] The procedure of taking biometric data must comply with the CFR, ECHR and the UN Convention on Rights of Children, as was recalled in *RL v Wiesbaden*.[604] The CJEU has recently stated that fingerprint data are biometric data which is particularly sensitive.[605] As an example of national implementation, Croatian rules on data collection by the border police state that the police may collect fingerprints, palmprints as well as other biometric data and other data concerning the properties of physical identification.[606] Croatian law on the surveillance of the national border prescribes that the border police may use video recording or photography, take fingerprints, palm prints as well as other biometric data by using appropriate technical equipment.[607] The Croatian law on international protection, in the Article titled Expression of Intent, states that persons over 14 years of age are required to submit to fingerprinting and to being photographed.[608] Likewise, the same Article further states that police officers also have the duty to take photographs and fingerprints,[609] and that persons who do not submit to fingerprinting without a justified reason will be fingerprinted without their consent.[610]

Eurodac expressly admits that coercion can be used, as a last resort.[611] Resorting to coercion without giving a person the opportunity to comply willingly is very likely a breach of fundamental rights.[612] The issue of coercion is paradoxical: a person can willingly submit to fingerprinting, but if the person does not, they may be coerced. In this way, persons do not have a genuine choice of refusing to be fingerprinted. The rules of Eurodac also envisage the linking of the refusal to have fingerprints taken with a negative outcome of the request for international protection, except in cases where there are objective reasons for a person being unable to provide biometric data (where the person did not intentionally bring about the condition).[613]

---

[603] Regulation (EU) 2024/1358, Articles 1(2) and 13(2).
[604] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251.
[605] ibid, para 107.
[606] Pravilnik o načinu prikupljanja podataka, tehničkim uređajima za prikupljanje podataka, sadržaju i korisnicima operativnih zbirki podataka koje vodi granična policija te rokovima čuvanja NN 102/2018 (Rulebook on the method of data collection, technical devices for data collection, content and users of operational data collections maintained by the border police and on the retention periods), Article 4.
[607] Zakon o nadzoru državne granice NN 83/18, 27/16, 114/22, 151/22 (Act on State Border Control) Article 39.
[608] Zakon o međunarodnoj i privremenoj zaštiti NN 70/15, 127/17, 33/23, 17/25 (Act on International and Temporary Protection), Article 33(5).
[609] ibid, Article 33(8).
[610] ibid, Article 33(7).
[611] Regulation (EU) 2024/1358, Article 13(2)-(3).
[612] FRA, "Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac" (2015) 4.
[613] Regulation (EU) 2024/1358, Article 13(5).

The other exception to the obligation to provide biometric data are for reasons of the health of the data subject or of public health.[614] Otherwise, the refusal to give biometric data can be considered an implicit withdrawal of the request for international protection.[615]

Processing the biometric data of children or, more concretely, fingerprinting and taking facial images, is regulated under specific rules in Eurodac.[616] This is of particular concern since the threshold by which persons are enrolled in Eurodac has been lowered from 14 to 6 years of age in the new Eurodac Regulation. The treatment of minors in relation to the processing of personal and biometric data is an important and complex problem.[617] It can be argued that the fingerprinting of minors may contribute to their fundamental rights by limiting the risks of child smuggling and by increasing the possibility to reunite them with parents. On the other hand, one could argue that if the processing of biometric data of children is beneficial to children, then it should not be limited at all. Should not five-year-old children also have a better chance of reuniting with their parents? However, the issue of the processing of biometric data of children deserves detailed and separate treatment and thus is beyond the scope of this thesis.[618] One obvious problem in relation to Eurodac is that it is often unknown how old a person is, that is, whether the person is a child. Biometric technologies may be crucial in the future in determining the exact biological age of a migrant or an asylum seeker. Since there is no certain way of determining the exact age of a child, taking fingerprints and facial image of every applicant above the age of six in practice means that there will be many cases where children below that age are fingerprinted.[619]

Eurodac is under reform as part of the so-called Pact on Migration and Asylum. The Screening Regulation sets general conditions for registering TCNs at external border.[620] This registration includes the processing of biometric data, which is sent to the CIR's logically separated part for Eurodac. The changes that the Screening Regulation brings in terms of shifting the purpose of

[614] See Regulation (EU) 2024/1358, Articles 15, 18, 20, 22.
[615] Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU PE/16/2024/REV/1 [2024] OJ L 2024/1348, Article 41.
[616] Regulation (EU) 2024/1358, Article 14.
[617] See, on biometric data and children in the EU migration context, Mona Alexandra Riedl, "Notes Biometric Borders and Minors' Rights: A Critical Analysis of European Migration Management under the New Eurodac Regulation" (2024) University of Twente Student Thesis.
[618] See I Goldner Lang, "'Laws of Fear' in the EU: The Precautionary Principle and Public Health Restrictions to Free Movement of Persons in the Time of COVID-19" (2021) 14 European Journal of Risk Regulation, 141 https://doi.org/10.1007/978-3-031-71598-3_4.
[619] Regulation (EU) 2024/1358.
[620] Regulation (EU) 2024/1356.

the asylum system from a humanitarian perspective towards a security perspective will not be analysed here.[621] What is important is that the Screening Regulation, together with the Eurodac Regulation and the Interoperability Regulations,[622] affects the conditions for the processing of biometric data. The Screening Regulation determines that biometric data are collected from two categories of persons: persons apprehended in relation to irregular crossing and persons who were found illegally staying in the EU.[623] The procedure envisaged consists of multiple steps, but it is important that the registration of biometric data is conducted in accordance with the rules set out in the Eurodac Regulation.[624]

3.3.2.4. The Parameter of Comparison of Biometric Data

A biometric comparison is an estimation of the similarities between, in ISO terminology, a biometric probe and a biometric reference.[625] It can be noted that it is an estimation, meaning that the result is measured in probability and therefore there is never absolute certainty. An algorithm can be set to return the result as positive if a certain set level of likeness between the two compared sets of data has been achieved. For the sake of simplicity, comparison is the act of comparing two biometric templates, which may, in legal terms, be equated to comparing two sets of biometric data.

Comparison entails either biometric verification or identification.[626] Verification means a comparison of the biometric data of one persons (in the case of a positive comparison or in the case where biometric data were compared against fraudulent data). Biometric verification means the limitation of privacy of the one person whose data are compared (e.g. the facial image of a person taken at a border crossing compared with the facial image of the same natural person contained in the passport). A comparison of the biometric data collected with the biometric data in a database is done automatically, with only a few exceptions.[627] Automatic comparison may be conducted with both biometric and alphanumeric data.[628] A comparison based on

[621] See European Council on Refugees and Exiles (ECRE), "Reforming EU Asylum Law: The Final Stage" (2023) https://ecre.org/wp-content/uploads/2023/08/Policy-Parper-Reforming-EU-Asylum-Law-the-Final-Stage-August-2023.pdf
[622] Regulation (EU) 2019/818; Regulation (EU) 2019/817.
[623] Regulation (EU) 2024/1356, Article 1 a and b
[624] Regulation (EU) 2024/1356, Article 8(5)(d).
[625] International Organization for Standardization, ISO/IEC 2382-37:2022(en) Information Technology — Vocabulary — Part 37: Biometrics, www.iso.org.
[626] See more in 1.7.2.1 of the thesis.
[627] In the case of Eurodac, an exception to automatic comparison is when an applicant for international protection arrives in a Member State following a take charge transfer (Article 16(2)(a) 2024 Regulation (EU) 2024/1358). See also Articles 9 and 10 of the same regulation.
[628] Regulation (EU) 2024/1358, Articles 32-33.

alphanumeric data is not as precise as a comparison of biometric data. One can imagine that there are many persons sharing the same or similar biographical data, not to mention the possibilities of misspelling, transcription, and other errors to which alphanumeric data are prone. Concerning Eurodac in particular, if the designated authorities or Europol have already consulted the CIR which has shown that there is indeed data relating to a certain person in Eurodac, prior consultation of national databases is not required.[629] A biometric comparison in the sense of Eurodac means comparing biometric data belonging to one person against the biometric data of all persons in the database. In terms of processing biometric data, biometric identification thus represents the processing of biometric data of many persons (the biometric data of the person being compared plus the biometric data of all the persons in the database).

Here, then, is an important revelation. The difference between biometric verification and identification is not (only) that identification limits the privacy of one person more than verification, but identification also means the limitation of the privacy of many persons. Since biometric identification can be expressed as comparison of 1:n, in the case of a biometric database containing a million samples, biometric identification means a comparison of 1:1,000,000. Crucially, this necessarily means that biometric identification involves the infringement of the privacy of as many persons as there are biometric templates in a database. This line of thought can be extended further. The privacy of the one person that is being identified is infringed to a greater extent than that of all the persons whose biometric data are being compared but does not result in a positive comparison. The limitation of privacy of such persons exists but is minimal. On the other hand, the biometric data of the one person submitted for comparison against Eurodac is compared numerous times against all the templates in Eurodac, and then possibly transferred and stored. Nevertheless, when the effects on privacy caused by biometric identification are examined, such action should be understood as involving the limitation of privacy of all persons whose data are in the database, not just the one that is being identified. This is not considered in the legal analysis either of the courts, legal scholars or the legislation concerning the effects of biometric data processing.

Thus, the intensity and amount of infringement of privacy in each comparison of biometric data in the case of biometric identification can be distinguished. It is interesting to note that from this perspective of biometric parameters, there is not so much difference between biometric identification and verification in terms of the limitation of privacy suffered by the person whose

[629] ibid, Articles 33(2) and 34(2).

data are being submitted for comparison against Eurodac or against another template of their own biometric data, even though this person is primarily who the courts or the legislator have in mind when assessing the effects of biometrics. The usual understanding of biometric identification being more burdensome to privacy and thus under a stricter legal regime might thus be incorrect, as far as the one person is concerned.[630] Biometric identification should consequently be more burdensome to privacy and data protection because it involves more persons and also because of the intensity of the limitation of privacy of the one person, whose biometric data are being compared not once, but as many times as needed until there is a "match" or until all the biometric templates in a database have been exhausted. Furthermore, biometric identification is usually thought of as being connected to remote storage, as was discussed in the context of the AI Act and its definitions of biometric terms.[631] Finally, biometric identification can be understood not only as a higher intensity of comparison, but also as implicitly involving other biometric parameters, such as transmission and storage of biometric data after a positive or negative comparison, unlike verification.[632] Thus, one should be careful to understand that biometric identification is both different in terms of the biometric parameter of comparison but also in that it involves more parameters (potentially) than is the case with biometric verification.

3.3.2.5. The Parameter of Transmission of Biometric Data, Including to Third Countries

Every biometric system must determine the technical way in which data are transferred within the system. As a legal phenomenon, transmission is the operation of processing biometric data whereby biometric data are moved to be stored, compared, or accessed. The manner of transfer is determined by the technical capacities but also by legal constraints, as care must be given to transfer data in the way stipulated by law, and which hinders privacy and data protection in the least degree. It is the Member State's responsibility to collect biometric data and transmit them to Eurodac. With the exception of the cases of persons admitted according to resettlement schemes, biometric data transmitted by the Member States are compared automatically.[633] The collection and transmission of biometric data are the duty of the Member State of origin, which

[630] Case law, for example Case C-291/12 *Schwarz*, considers biometric verification (authentication) as less intrusive to privacy than identification. Likewise, the GDPR and the AI Act distinguish between verification and identification (see GDPR Article 4(14) and 9(1) and AI Act Annex 1(1)(a) which states that biometric identification is a high-risk system, but verification is not).
[631] See 2.7.4 of the thesis.
[632] See 1.7.2 concerning the meaning of biometric identification in general for a better understanding of the position of this author that there might be an unclear dividing line between biometric verification and identification despite the fact that the current legal framework depends on this distinction.
[633] Regulation (EU) 2024/1358, Article 27(1).

is the one that originally collected the biometric data (the Member State where the person was found illegally or where the migrant crossed the border in an irregular manner). This Member State has a deadline of 72 hours to transmit biometric data to Eurodac, starting from the registration of the claim for international protection or the taking of the biometric data.[634] The same Member State has the duty to amend or erase the data when appropriate.[635] It is important to note that the Member State of origin transmits the biometric data to Eurodac but it also immediately receives the results of the comparison of personal (and biometric) data, except for persons involved in resettlement schemes, where it only transmits the data.[636]

Concerning Eurodac, biometric data are transmitted in a data format as agreed in the Interface Control Document, which is a technical document that allows for communication between national access points and Eurodac.[637] This document should have been agreed by eu-LISA and the Member States by December 2024.[638] It is very difficult to assess how transmission affects fundamental rights and data protection without considering the technical aspects. However, a serious effect on privacy, but also possibly on other fundamental rights, is raised by the possibility to transfer biometric and other personal data to third countries for law enforcement purposes, following a positive match (hit) unless there is a "real risk that, as a result of such a transfer, the data subject might be subjected to torture, inhuman and degrading treatment or punishment or any other violation of his or her fundamental rights".[639] In 2023, Member States transmitted more than 1.7 million sets of fingerprint data to Eurodac, for either storage or for search (comparison) purposes.[640]

The revisited 2024 Eurodac Regulation allows the transfer of personal data from its database to third countries for the purposes of return of a person.[641] The consequences of a mistaken transfer of biometric data can be extremely grave. Therefore, a proportionality assessment of such processing of personal data should be carried out rigorously in the case of transferring data to third countries. On the other hand, the issue may concern national security which may suppress a detailed examination. It should be noted that all processing actions in Eurodac are documented

[634] Regulation (EU) 2024/1358, Articles 18.1, 20.1, and 15.1 Recital 4
[635] ibid, Article 40.
[636] ibid, Article 36.
[637] ibid, Article 37 and Article 2(v).
[638] ibid, Article 63(4).
[639] ibid, Article 49(2)-(3).
[640] eu-LISA, "Eurodac 2023 Annual Report December 2024" www.eulisa.europa.eu/Publications/Reports/Eurodac%20Statistics%20Report%202023.pdf.
[641] Regulation (EU) 2024/1358, Article 50.

(logged)[642] which is a simple but important security measure that reduces abuse and allows for an analysis of previous actions.

The transfer of personal data to third countries has been a prominent topic in the judgments of the CJEU in the last decade. This topic goes well beyond the scope of this thesis. Suffice it to say that the CJEU found that access to personal data on a general basis by public authorities, in the context of a case concerning the transfer of personal data to third countries, may be regarded as contrary to the essence of the fundamental right to respect for private life of Article 7 CFR.[643] Particularly relevant is that the Court, in the same case, went on to say that if legislation provides no remedies to enable access to or rectification of personal data for the data subject, that is also contrary to the essence of the fundamental right to effective judicial protection.[644] It could be argued that such considerations apply to Eurodac in particular, since data subjects, given their precarious position as irregular migrants, are not in a position to effectively obtain judicial protection, particularly in the context of the transfer of their personal data to third countries. The extremely low effectiveness of judicial protection afforded to data subject in the context of Eurodac is attested by the fact that there have been no complaints, requests or inquiries of data subjects concerning their biometric data processed in the context of Eurodac in Croatia.[645] The situation is likely to be similar in other Member States, despite the fact that Eurodac processes millions of fingerprints each year. Similarly, there has been no case before the CJEU with respect to Eurodac. In these circumstances, the possibility of the transfer of personal data to third countries is highly problematic. As a biometric parameter, the transfer to third countries of biometric data of migrants should be heavily restricted or prohibited.

3.3.2.6. Storage Parameters: The Place and Duration of the Storage of Biometric Data

The storage (of biometric data) is one of the most important parameters in assessing a biometric system. From a legal standpoint, the mere storing of fingerprints, DNA and cellular samples is an interference with the right to private life under Article 8 ECHR.[646] In *RL v Wiesbaden,* the CJEU identifies that the processing in question consists of at least two operations; the first is

[642] ibid, Article 51.
[643] Case C-362/14 *Schrems I* ECLI:EU:C: 2015:650, para 94. See also Case C-311/18 *Schrems II* ECLI:EU:C: 2020:559.
[644] Case C-362/14 *Schrems I* ECLI:EU:C: 2015:650, para 95.
[645] The source of this information is an interview with Anamarija Mladinić, an expert from the Croatian data protection authorities - AZOP. There has not been such an inquiry or request by a migrant towards the authorities or the Ministry of the Interior, which processes biometric data and is competent to receive complaints. The author is grateful for the interview and kindly thanks Anamarija Mladinić.
[646] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC 4 December 2008) para 67.

the act of collecting the biometric data, and the second is the storage of those data.[647] Closer inspection shows that storage actually consists of two distinct parameters. The first is regarding where the data are stored and the second aspect is for how long the data are stored. Both these elements are recognised as playing a role in the proportionality assessment of the CJEU.[648]

Local storage means that the biometric data are stored on the document that is in the physical possession of the person that is the subject of the data processing. Such is the case for identification cards and passports, as well as for residence permits for third-country nationals in the EU, which store the biometric data locally.[649] This was the factual situation in a number of biometric cases before the CJEU, namely *Schwarz, Willems and RL v Wiesbaden* and to a certain extent in *Willems* and *A, B and P*.[650] Biometric data that are processed when EU citizens apply for passports or IDs are stored only locally on the documents in their possession and it is accessed by public authorities when the identity of the person is being verified (for example, at a border crossing). Biometric data require technical processing, otherwise a photograph inspected by a border guard represents the processing of personal data, not biometric data. As has been discussed, even though one could equate local storage with biometric verification and remote storage with biometric identification, the issue is more complex. Biometric identification does not necessarily involve the action of storage of biometric data.

In Eurodac, biometric data are recorded together with alphanumeric personal data and other data that relate to the administrative procedure in question, such the status of the application for international protection or whether the person is considered to present a threat to internal security.[651] What is stored in Eurodac in terms of biometric data are ten fingerprints and a facial image. It should be noted that the national biometric database may contain more biometric data, not all of which is transmitted to Eurodac.

3.3.2.6.1. The Place of Storage

The storage of Eurodac biometric data is in two places: the Eurodac Central System and the CIR.[652] Therefore, the case of Eurodac represents the remote storage of biometric data.

[647] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, para 74. Concretely, the collection of the facial image and two fingerprints is mandated by Article 3(5) Regulation 201971157 on a "highly secure storage medium" on the card itself.
[648] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, 61-22.
[649] See 3.2 of the thesis.
[650] See 3.2 of the thesis.
[651] Regulation (EU) 2024/1358, Article 17, Article 16(1) and Recital 30.
[652] ibid, Article 33(2).

Generally, remote storage is seen as a greater limitation of the fundamental right to privacy than local storage, because the biometric data are outside the control of the person.[653] The EDPS likewise concluded that storage on a local chip is more friendly to privacy than storage in a central database.[654] However, remote storage is necessary for a system such as Eurodac. Migrants could easily discard their identification documents containing biometric data, and law enforcement bodies would not be able to access them to conduct biometric recognition. On the other hand, even though stored locally, the processing of biometric data for the purpose of issuing IDs concerns a vastly greater number of people, considered to be about 370 million persons or 85% of the EU population,[655] so in the sense of number of persons whose biometric data are processed by being stored, local storage may be linked to a greater limitation of fundamental rights than in the case of isometric databases such as Eurodac. This is why it is hard to imagine how one could supplant remote storage with local storage, since these systems serve different purposes. The use of local storage was a convenient argument that the Court used in *Schwarz* to stress the low and proportionate impact on privacy and data protection that the EU passport scheme presents. The problem was that the Court invoked *Schwarz* in subsequent cases which also involved addressing the possibility of remote storage in a database, as has been discussed.[656]

More importantly, EU biometric law, when it comes to the issue of storage, has a blind spot. The way national biometric databases process biometric data is not considered by the CJEU when analysing the effects of biometrics on fundamental rights. That was a key point in *Willems*, where the issue was whether EU law allows biometric data collected for the purpose of its regulations to be used in *national* biometric databases.[657] However, the CJEU evaded directly answering this question by stating that Regulation 2252/2004 does not require Member States to guarantee that biometric data would not be used in national databases. The CJEU in *Willems* and also more recently in *RL v Wiesbaden* avoided considering the effects of processing biometric data by national databases by claiming that the question of national databases was outside EU law.[658] In other words, the Court will analyse the biometric systems of passports

[653] Case C-291/12 *Schwarz* ECLI:EU:C: 2013:670..
[654] EDPS, "Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)" (2011) para 53 https://www.edps.europa.eu/sites/default/files/publication/11-02-01_fp7_en.pdf.
[655] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, para 35.
[656] See 3.2.2 and 3.2.3 of the thesis.
[657] Case C-446/12 *Willems* ECLI:EU:C: 2015:238.
[658] ibid.

and IDs on the basis of a legal fiction: that those biometric systems only process biometric data locally, despite the fact that there are national biometric databases that collect the same biometric data and store them remotely. This fiction is not particularly convincing since it is clear that national databases affect privacy and data protection as much as EU-wide databases do. But this is a pragmatic political choice by the Court framed in a legal analysis that eschews the glaring fact that the same fingerprints are also stored in national biometric databases, subject to national laws.

3.3.2.6.2. The Duration of Storage

The parameter of the duration of the storage of biometric data is also sometimes called the retention period. The retention period is counted from the date of the transmission of biometric and personal data to Eurodac.[659] The personal data of persons who have applied for international protection is stored for ten years from the date of transmission of the data. Biometric data of persons registered for the purpose of conducting an admission procedure under the union resettlement and humanitarian admission framework are stored for different periods, ranging from no storage to five years of storage.[660]

The storage period of biometric (and other) data has been revised for Eurodac 2024.[661] Storage lasts for five years for the biometric data of a number of categories of persons: for irregular migrants, that is persons apprehended in connection with an irregular crossing of an EU external border,[662] for persons admitted in accordance with a national resettlement scheme,[663] for TCNs or stateless persons illegally staying in a Member State,[664] and TCNs or stateless persons disembarked following a search and rescue operation.[665] For persons registered for the temporary protection scheme, the duration of the storage of biometric data is one year from the entry into force of the relevant Council Implementing Decision, and it is renewable yearly.[666] The storage period of biometric data (fingerprint data) in the still applicable Eurodac 2013 is

[659] Regulation (EU) 2024/1358, Article 29.
[660] ibid, Article 29(2).
[661] ibid, Article 29.
[662] ibid, Article 29(6).
[663] ibid, Article 29(5).
[664] ibid, Article 29(7).
[665] ibid, Article 29(8).
[666] ibid, Article 29(9).

18 months for irregular migrants.[667] Biometric data of applicants for international protection is stored for ten years.[668]

Setting the biometric parameter of the length of storage is no easy task. On one hand, numbers should allow for a simple assessment, with a longer period representing a more negative impact on the rights of migrants. A longer storage period would require adjustment by other biometric parameters, so that then data are stored locally, or the long storage period is justified in view of the persons concerned (e.g. persons convicted of serious crimes) or the purpose of the biometric system is particularly important (e.g. prevention of terrorism). Nevertheless, it is not possible to objectively determine what length of storage is too long, and the precise number of years that is perfectly suitable in view of the other biometric parameters. The justified length of the storage period for the biometric data of persons applying for international protection could be ten years, but it is impossible to objectively determine that the period of storage in such a case could not be eight or twelve years. The length of storage can be justified either way, which means that the number of years is mostly pulled out of a hat and then justified according to needs.

The ECtHR's *Marper* case determined that the indefinite retention of biometric data is contrary to the human right to privacy.[669] The retention period for personal data was also examined in the CJEU's judgment in *Tele2 Sverige v Watson* as a factor in the proportionality assessment.[670] The existence of a limited period for which the data are stored is thus crucial for the legality of processing biometric data. Similarly, Eurodac has also determined how long biometric data can be kept in its database for certain categories of persons. There can hardly be objective circumstances to associate the parameters of a biometric system with a certain allowed fixed period for the storage of biometric data. On the other hand, the length of the retention period cannot be completely "made up" and unsubstantiated. There must be a genuine attempt to justify a certain retention period as the absolute minimum necessary, whether in the case of a proportionality exercise preceding a legislative act or in a judgment of a court which interprets whether a certain restrictive measure is justified.

One final aspect of the parameter of storage is erasure. In the case of Eurodac, stored (biometric) data must be erased before the elapsed time if the person has acquired citizenship of an EU

[667] Regulation (EU) 603/2013, Article 16.1.
[668] Regulation (EU) 2024/1358, Article 29(1).
[669] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008).
[670] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C: 2016:970, paras 86-108.

Member State.[671] The erasure, as for other changes to the data, is done by the Member State of origin, so that if the person acquired citizenship of another Member State, the data are erased only when the Member State of origin learns of the acquisition of citizenship.[672] Otherwise, the biometric data are erased automatically from Eurodac upon the expiry of the storage period.[673] The principle of automatic erasure is the only approach that can be considered proportionate in a biometric system. To be dependent on the manual erasure of biometric data would in practice certainly lead to storage periods lasting over the stipulated legal limits. The conditions of erasure are thus important in the fundamental rights calculus.

3.3.2.7. The Parameter of Access to Biometric Data

Access to biometric data should be understood as the action of being able to see, read or amend biometric data that is already in the database. Access could thus be distinguished from either the initial collection of biometric data, storage, or the action of comparison of biometric data (biometric identification). First is access for the purpose of migration, asylum, and border control (in short, migration access). Accessing Eurodac's biometric data for migration purposes means that public authorities can see whether the person in question has applied for asylum previously or has been apprehended in association with illegal stay in the past.

The other broad category of access is access for the purpose of law enforcement. Law enforcement access is regulated in Eurodac. The legal framework for the processing of biometric data for the purposes of law enforcement is found in the LED and not in the GDPR (in addition to the provisions of Eurodac which also regulate the processing of personal and biometric data for such purposes). As explained in 2.6.2 of the thesis, the LED provides a less restrictive framework for the processing of biometric data than the GDPR, the reason being that law enforcement is considered a justified reason for the restriction of the rights to data protection and privacy. Recital 30 of the Eurodac 2024 Regulation states that Eurodac can be consulted only by authorities responsible for internal security if the act is so reprehensible that it "justifies querying a database that registers persons with a clean criminal record", which means that Eurodac should not be as easily accessible as criminal databases. The threshold for

[671] Regulation (EU) 2024/1358, Article 30(1).
[672] ibid, Articles 30(1) and 40(3).
[673] ibid, Article 29(10).

the proportionality assessment of law enforcement access to Eurodac should be particularly high.[674]

Access to biometric data is in fact composed of a number of distinct processing activities. For example, if law enforcement authorities access Eurodac, this means that personal data were transmitted to Eurodac, they were compared with the personal data in Eurodac and then the results were transmitted back to the authorities. If there is a match, there is also the transfer of the matching personal data in the database to the authorities. With that in mind, it becomes clear that the conditions for access to Eurodac protect the biometric data (of migrants) that are already in Eurodac, and not the biometric data that law enforcement authorities have submitted for comparison.

In terms of the access conditions, there are different roles for the designated and the verifying authorities. In the case of Eurodac, the designated authorities for law enforcement purposes are those asking for access to Eurodac data, while the verifying authorities are the authorities of the same Member State that check the conditions for access to Eurodac.[675] The verifying authorities forward the request to National Access Points. The verifying authorities may forward the request to access before checking the conditions for access. This is in "exceptional cases of urgency, when there is imminent danger from terrorist or other serious offence (...)".[676] This possibility further opens up Eurodac to law enforcement. It is understandable in the ever-present dialectics of necessity and proportionality that there is also the possibility of a more immediate approach to data in Eurodac in the case of serious circumstances for national security. But the consequence prescribed by Eurodac for unjustified access prior to verification is simply that all data accessed without proper authorisation will be erased by the designated authorities.[677]

As well as in the case of the collection and comparison of biometric data for migration and asylum purposes, facial recognition is only used if fingerprint recognition is not available.[678] It should be noted that the parameter of access entails biometric identification: a comparison of one set of biometric data against all biometric data in the database. This is also made clear by the wording "A comparison of a facial image with other facial image data in Eurodac for law

[674] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022), 369.
[675] Regulation (EU) 2024/1358, Article 32.
[676] ibid, Article 32(4).
[677] ibid, Article 32(5).
[678] ibid, Article 32(3).

enforcement purposes may be carried out(...)".[679] This is important to note because the Eurodac Regulation does not make the dichotomy of verification and identification explicitly clear.

It may be considered unusual, or even problematic in terms of the proportionality assessment, that the 2024 Eurodac Regulation stipulates that facial recognition is used only when fingerprint recognition is not possible. Contrary to this, in *RL v Wiesbaden*, the Court examined the biometric ID scheme which had the opposite order of biometric technologies to those in Eurodac. In the case of the biometric verification of IDs, the first used is facial recognition, and then, only when necessary, fingerprint recognition.[680] The Court overall found such an application to be proportionate in its balancing exercise, but it raises the question of the priority of biometric technologies. In *Marper*, the ECtHR concluded that fingerprints do not contain as much information as DNA samples and that fingerprints, unlike photographs, are unintelligible to untutored eye.[681] In *Schwarz*, the CJEU was not clear when it stated that the combination of fingerprints and a facial image "may not *a priori* be regarded as giving rise in itself to a greater threat to the rights recognised by Articles 7 and 8 of the Charter than if each of those two operations were to be considered in isolation".[682] In the opinion of this author, the logic of biometrics and its effects on privacy should demand that first only fingerprint recognition be used if it sufficient, because it infringes privacy the least in comparison with DNA profiling or facial recognition. If fingerprint recognition is not enough to effectively achieve certain goals, facial recognition should be used in reserve, but such use should be justified. This is mostly the position of Eurodac, except that it is not exactly clear what event or reason makes facial images a requirement in addition to fingerprinting, which was added in the 2024 Eurodac Regulation. If the case law that is examined here shows one thing, it is that the debate on the hierarchy of biometric technologies can be justified either way.

There are four conditions that designated authorities must satisfy to gain access to Eurodac for the purpose of law enforcement. Designated authorities must conduct a prior check in the available national database and in the automated fingerprinting identification systems (AFIS) of all other Member States available under Decision 2008/615/JHA.[683] However, Eurodac may

[679] Regulation (EU) 2024/1358, Article 32(3).
[680] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C:2024:251, para 117; Recital 19 of Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement PE/70/2019/REV/1 [2019] OJ L188/67.
[681] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008), paras 78 and 84.
[682] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, para 49.
[683] Regulation (EU) 2024/1358, Article 33(1)(a).

allow access to its data without a prior check in national databases or the AFIS of other Member States. This is the case if the designated law enforcement authorities consulted the Common Identity Repository (CIR) in accordance with Interoperability Regulation 2019/818 which indicated that data relating to a person is indeed in Eurodac.[684] In addition, designated authorities *may* consult the VIS database, provided that the conditions in Decision 2008/615/JHA are met.[685]

The second condition for law enforcement access is that the comparison requested must be "necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database proportionate to the objective pursued".[686] The third condition is that the comparison is necessary for specific persons concerning a specific case (which should prohibit fishing expeditions of law enforcement bodies). The final condition is that there are reasonable grounds that it will substantially contribute to the prevention, detection or investigation of terrorist offences or serious criminal offences, and in particular if there is a substantiated suspicion that the person connected to such offences is in the Eurodac database.[687] Similar conditions are envisaged for law enforcement access to Eurodac by Europol.[688]

These condition reflect the analysis of courts in cases concerning biometrics, which takes into account how different factors which limit the processing of biometric data contribute to the proportionality analysis in accordance with Article 52(1) CFR. These conditions give weight to the requirement that the limitation of the privacy and data protection of an individual must be proportionate and necessary and meet an objective of general interest recognised by the EU and can be considered to effectively reduce the possibility to abuse Eurodac for the purposes of law enforcement. Nevertheless, statistics show a low amount of law enforcement access to Eurodac in comparison to overall access numbers.[689]

However, it is true that this low amount may have significantly contributed to crime reduction and prevention (though it is also true that it is impossible to determine exactly how this has effectively been achieved by allowing law enforcement authorities access to Eurodac). For

[684] ibid, Article 33(2).
[685] ibid, Article 33(1) last paragraph.
[686] ibid, Article 33(1)(b).
[687] ibid, Article 33(1).
[688] ibid, Article 34.
[689] eu-LISA, "Eurodac 2023 Annual Report December 2024".

example, in the ECtHR's *Marper* case, statistics were produced to demonstrate that access to biometric data helps solve serious crimes. However, the extent to which biometric data actually contributed to the resolution of such crimes was misleading.[690] It should be admitted that the conditions for law enforcement access are restrictive and detailed, as far as Eurodac is concerned. In terms of proportionality, particularly important is the requirement that Eurodac may be used only as an ancillary source for the identification of persons, not on equal grounds with law enforcement databases. But this favourable analysis of how the current conditions of law enforcement access for Eurodac is aligned with fundamental rights might be undermined if interoperability is taken into consideration.

3.3.2.8. No-hit as Processing of Personal Data

The assessment of a biometric system in terms of its parameters has raised a valuable question. Related to the parameter of access to biometric data, but also to the parameters of comparison and transmission, is the concept of hit and no-hit as defined in Eurodac. The authorities can conduct a search for data on a certain person in any of the systems. This search is carried out via the European Search Portal, an element of interoperability designed for this purpose.[691] Persons can be identified with alphanumeric or biometric data contained in the Common Identity Repository (CIR).[692] A hit represents a match between the biometric data recorded in Eurodac and the data transmitted by a Member State.[693] A no-hit means that there was no match in a comparison of biometric data between one biometric template submitted for comparison and all the biometric templates in the (Eurodac) database. Because of a no-hit, law enforcement authorities will not be able to read any of the biometric data in the database.

Upon closer inspection, however, a no-hit itself should be regarded as the processing of biometric data, and composed of multiple parameters as examined in this section. In the case of a no-hit, the biometric data would have been automatically compared, and in addition, the law enforcement authority would have received the information that no biometric data in the database were a match for the biometric data submitted. The information that a person is not in

[690] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008) paras 115-116.
[691] See 3.4 of this thesis.
[692] eu-LISA, "Single Programming Document 2022–2024", European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice Single Programming Document 2022–2024 2020-323 Rev 2 (2021) 67.
[693] Regulation (EU) 2024/1358, Article 2(1)(j).

the Eurodac system may itself represent personal data.[694] A no-hit might rise to personal data when considered with other information.[695] If a no-hit represents the processing of personal data, then a no-hit must be justified in terms of data protection and fundamental rights. A related question is whether the action of the storage of biometric data already subsumes the subsequent comparisons (millions, in the case of Eurodac) that will be conducted on the biometric data stored. Probably not, because, as previously explained, the CJEU clearly distinguishes different operations of processing personal data as separate limitations, though it is true that neither the Court nor the legislator has considered the processing of biometric data at this level of detail. Should it be taken into account in the proportionality assessment (when drafting the rules or assessing the limitation before the court) that the privacy of a person is more seriously infringed if the biometric data are in a database, since there they are not only stored but constantly compared (even if the result is a no-hit)? However, a no-hit could also be interpreted as the absence of processing in the (Eurodac) database.

A hit, on the other hand, signals that the biometric data of the person are already in the database. This is biometric identification. A hit proves that the biometric data that the authorities submitted for comparison have found their match in the stored biometric data in Eurodac. Thus, a hit does not reveal the identity of a new person but instead associates additional biometric and other alphanumeric data with the person whose biometric data are already stored. If there is a hit following an automatic comparison, Eurodac transmits the personal data, including fingerprint and facial image data, name, nationality, and other biographic (and alphanumeric) data associated with a person (linked in a dataset).[696] A hit which resolves which State is responsible for the asylum claim takes precedence over other hits.[697] Of course, if there is no hit, the personal data are not transmitted. Overall, much more personal data are collected and stored in Eurodac following the Eurodac 2024 Regulation. The currently applicable Eurodac does not record the name of the person, nationality, date and place of birth and some other biographic data that the new Eurodac does store.

[694] Also, the position of EDPS, "Consequently, a user who is not allowed to access data stored in a specific system is similarly not allowed to get access to "hit/no hit" information, since even this limited information constitutes personal data". Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice, 17 November 2017.
[695] See Regulation (EU) 2016/679, Recital 26, on what personal data are by an assessment of the concept of identifiability.
[696] Regulation (EU) 2024/1358, Article 27(4).
[697] ibid, Article 27(5).

Regarding what has been analysed so far in the thesis in the synthesis of biometric law, the hit or no-hit system is proportionate, because it blocks access in the case of a no-hit. It thus greatly strengthens the privacy and data protection of individuals whose biometric data it concerns. This system allows an incremental, step-by-step system of processing biometric data in accordance with how the hurdles are cleared. The more the conditions are satisfied, the greater the processing of biometric data is allowed. Related to this discussion is the marking of personal data. The Member State which grants international protection marks the data of that person in Eurodac.[698]

3.3.2.9. The Purpose of a Biometric System

Every biometric system is built for a certain purpose. This purpose might be to register the biometric data of persons who have committed serious crimes so that these persons can be readily identified. The purpose of Eurodac might be seen as to identify migrants who are associated with the irregular crossing of borders, many of whom apply for asylum in the EU. From a broader perspective, the purpose of Eurodac is to increase the sense of security among EU citizens, and this it achieves by registering, counting, and identifying those who came uninvited from outside. In any case, the purpose of a biometric system is an important parameter which determines other parameters. A biometric system serving purposes of law enforcement usually has longer storage periods and uses more biometric technologies, including DNA profiling. Therefore, the purpose of a biometric system influences other parameters such as the length and place of storage, the nature of the collection of biometric data, and the parameter of (the ease of) access to biometric data.

A second point that must be clarified in relation to its purpose is that it should not be viewed narrowly in legal terms. Purpose is not necessarily the same as the aims of a biometric system, as listed in the Eurodac Regulation, nor is purpose quite the same as the objectives of general interest that are the focus of a fundamental rights analysis. Despite this line of thought, it is hard to disentangle the parameter of purpose from the objectives examined by the Court or the aims listed in a regulation. The fact that no clear line can be drawn between legal or political purpose, or the technical purpose of a biometric system should not prevent the examination of the purpose of a biometric system. This is because purpose is paramount in the designing of a biometric system, and the examination of purpose reveals the nature of a biometric system.

[698] ibid, Article 31.

Purpose, in the form of the objective of general interest of the EU, or in the form of reasons of substantial public interest (which justify the processing of sensitive data such as biometric data under Article 9.2.g. GDPR) is also a key element in the proportionality analysis of biometrics.

Purpose has many sides and guises as interpreted in EU biometric law. First, purpose appears in the context of the EU data protection legal framework, which looks at the purpose of the processing of personal data, something that was analysed in Chapter 2. This includes consideration of the purpose of the limitation principle (Article 5(1)(b) GDPR) as well as the lawfulness of processing under Article 6 GDPR. One can also look at many layers of the purpose of a concrete biometric application. Collecting fingerprints of asylum seekers could be understood as having the purpose of determining whether the person in question has applied for asylum before, or more generally fingerprinting could be for the purpose of achieving the goals of Article 1(1) of the Eurodac Regulation, or having the purpose of contributing to the Area of Freedom, Security and Justice, as defined in the TFEU, to which Eurodac is an integral contributor. The purpose of Eurodac is to help determine which Member State is responsible for examining an application for international protection.[699]

Seminal scholarly articles recognise that the purpose of Eurodac is to assign identity to a person. Guild stated that Eurodac is a solution to how to assign identity to a person.[700] Van der Ploeg stressed that the purpose of fingerprinting is about establishing identity rather than examining a pre-existing one.[701]

In other words, the main purpose of Eurodac is (biometric) identification. Article 1 of the 2024 Eurodac Regulation that will soon come into force lists ten purposes. These include supporting the VIS and ETIAS, and assisting interoperability by storing biometric data in the CIR, but also for purposes which are less well-defined policy goals, such as controlling irregular migration, protecting children, and supporting evidence-based policies. There are specific purposes for the processing of biometric and personal data. The 2024 Eurodac Regulation specifies that specifically processing biometric and personal data may be done as one of its purposes but also for the purposes of a number of other regulations concerning the VIS, ETIAS, interoperability,

[699] ibid, Article 1; Regulation (EU) 2024/1351, Article 1(3).
[700] Elspeth Guild, "Unreadable Papers? The EU's First Experiences with Biometrics: Examining Eurodac and the EU's Borders" in Juliet Lodge (ed), *Are You Who You Say You Are? The EU and Biometric Borders* (Wolf Legal Publishers, 2007).
[701] I Van der Ploeg, "The Illegal Body: `Eurodac' and the Politics of Biometric Identification". Ethics and Information Technology (1999) 1, 295–302, 300, https://doi.org/10.1023/A:1010064613240.

temporary protection, the asylum system and resettlement.[702] Eurodac also states that the processing of biometric data by Member States for the purpose of their national biometric databases is not covered by the rules in Eurodac.[703]

In terms of justifying the limitation of the fundamental rights of privacy and data protection, an investigation of purpose forms an important element of the analysis. Any processing of biometric data is a limitation of fundamental rights and must genuinely meet the objectives of general interest recognised by EU law in order to be justified.[704] For example, in *Schwarz*, the Court's logic was that persons need passports for the purpose of travel, that passports need to contain biometric data to check their authenticity, thus preventing falsification and fraudulent use, which then prevent illegal entry into the Union. Preventing illegal entry into the EU is an objective of general interest recognised by the EU.[705] Therefore, to tie the ends of the syllogism together, the purpose of fingerprinting EU citizens is to prevent illegal entry into the EU. The Court's approach can be criticised for creating tenuous syllogisms for establishing an objective of general interest of the EU. The biometric parameter of purpose can thus be interpreted widely by the CJEU in its analysis of objectives of general interest.

Purpose can be approached from another side, as in the novel judgment in *RL v Wiesbaden.*[706] The objective of general interest determined there is the free movement of persons. The Court stated that to achieve the free movement of persons, there have to be documents containing both a facial image and fingerprints which are also interoperable.[707] The logic here is to defend the restriction by framing it as a freedom. Freedom of movement for EU citizens is stipulated by Directive 2004/38 (Citizens' Directive) and Article 45 CFR. Freedom of movement means the right to exit and enter Member States with a valid ID or passport. A valid ID or passport is one that includes biometric data. Therefore, freedom of movement means the obligation to submit to the processing of biometric data.[708] In every other circumstance, one would interpret the obligation to store fingerprints as an additional restriction, not a facilitator of free movement. Whether one accepts the logic of the Court as coherent or not, it remains true that determining

[702] Regulation (EU) 2024/135, Article 1(2).
[703] ibid, Article 1(2) first sentence.
[704] Article 52(1) CFR.
[705] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, paras 37-38.
[706] See 3.2.6 of the thesis.
[707] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, paras 87-88.
[708] ibid, para 120: "(...) the inclusion of two fingerprints in the storage medium of identity cards, are of particular importance not only for the European Union and the Member States, but also for EU citizens".

the parameter of purpose of a biometric system is essential for understanding its technical or legal logic.

The purpose of a biometric system thus may be to identify or verify the identity of incoming travellers, whether those that need a visa (as is the case with the VIS) or those that can enter visa-free (EES). Many biometric systems, particularly those of national States, are built for the purposes of prevention and suppression of crimes. The purpose of other systems might be to secure the borders or control irregular migration, focusing on different groups of persons. The parameter of purpose is tightly connected to the parameter of the personal scope of a biometric system.

3.3.2.10. The Personal Scope of Biometric Systems: Whose Biometric Data are Being Processed?

Any biometric system must define the parameter of which persons it applies to. This personal scope should be defined precisely and as narrowly as possible and yet still achieve the purpose of the biometric system. The broader the group of persons in the scope of a biometric system, the greater the justification that is required for such processing. In this way, the parameter of personal scope may affect other parameters. For example, since the processing of biometric data for the purpose of issuing an ID covers hundreds of millions of EU citizens, it is required that such biometric data be stored only locally on the chip, and not in remote storage.[709]

Eurodac currently processes biometric data of three main groups of persons. These are the persons who applied for international protection, third-country nationals or stateless persons apprehended in connection with the irregular crossing of an external border, and third-country nationals or stateless persons found illegally staying in a Member State.[710] In addition, the Eurodac Regulation prescribes that the data of those recognised as beneficiaries of international protection be marked and then blocked after a certain period.[711]

The 2024 Eurodac Regulation, which, as stated, applies from 2026, contains the same three main categories. In addition, the 2024 Eurodac Regulation entails the processing of biometric data for persons registered for the purpose of conducting an admission procedure and persons admitted in accordance with a national resettlement scheme, and third-country nationals or

[709] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251.
[710] Regulation (EU) 603/2013.
[711] ibid, Article 18.

stateless persons disembarked following a search and rescue operation.[712] The collection and transmission of biometric data are regulated separately in the 2024 Eurodac Regulation, though in many key regards the collection and the scope of the recorded biometric data are similar for each of the personal groups. Eurodac is not designed to be a criminal database. In fact, Eurodac states that persons in the database have a "clean criminal record".[713] This is why the processing of biometric data in Eurodac, in terms of access for law enforcement, should be regulated more stringently than for databases that concern persons associated with crimes.[714]

Any biometric scheme should be one that processes the biometric data of as small and as precisely a defined group of persons as possible. The broader the group of persons, the stronger are the justifications that are needed, which may be done by changing other biometric parameters. For example, a biometric system which concerns every EU citizen, such as biometric IDs, may require the local storage of biometric data and biometric verification,[715] instead of a remote database and biometric identification. The parameters that make the assessment should be observed together, not in isolation. In a recent judgment concerning the processing of biometric data for law enforcement purposes, the CJEU determined that there must be a differentiation between those convicted of crimes and those merely suspected of crimes when it comes to interference with their fundamental rights.[716] The parameter of personal scope thus represents one item in a checklist of both technical and legal assessments of a biometric system.

3.3.3 Concluding Remarks

This part has analysed the building blocks of any biometric system, known as biometric parameters. These biometric parameters appear in legislation, since a legislative act must define the manner of access to biometric data, the length of storage, and other parameters. Even more importantly, these same biometric parameters appear in case law. When the CJEU assesses whether the processing of biometric data is a justified limitation of fundamental rights, it takes into account biometric parameters such as the purpose of the biometric system in the context of the objective of general interest and in the justification of the limitation of fundamental rights to privacy and data protection.

[712] Regulation (EU) 2024/1358, Chapters III and VI.
[713] ibid, Recital 30.
[714] ibid.
[715] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, para 60.
[716] Case C-205/21 *Ministerstvo na vatreshnite raboti* ECLI:EU:C:2023:49.

In this section, the analysis of parameters has yielded further insight into the rightful legal perception of biometric identification and the more complex nature of every operation of the processing of biometric data than might have appeared before. The approach to biometric parameters, exemplified by thinking of a biometric system as a series of steps from collection to comparison to storage has allowed for a new understanding of the nature of so-called hits and no-hits. In the final part of this chapter, the discussion turns to the legal consequences of interoperability and biometric templates, crucial terms in EU biometric law, particularly in the context of migration and asylum.

3.4. Interoperability and Biometric Templates as EU Biometric Law Phenomena

The interoperability of EU information systems is a significant new phenomenon that affects the processing of biometric data because it concerns access, storage, and protection of biometric data. Rules concerning interoperability must be considered part of EU biometric law with effects on migrants and asylum seekers. Overall, this section will provide an essential insight into how different EU *biometric* systems are connected and how interoperability affects the data protection and privacy rights of migrants.

This section of the thesis will first explain interoperability in view of biometrics, that is, how interoperability represents the actions of processing biometric data. This will include an analysis of the individual components of interoperability. The critical analysis of one component of interoperability, the shared Biometric Matching Service (sBMS) and the legal nature of biometric templates stored in it will constitute the second part of this section. Whether biometric templates stored in the sBMS are biometric data is a vital debate for the purpose of this thesis. If biometric templates are biometric data, which is the position of this author, then such biometric templates must be processed and protected more strictly, including a stricter proportionality assessment and more stringent rules that apply to the processing of sensitive personal data. Interoperability and the question of biometric templates are closely related. This is because the sBMS, the database that stores biometric templates for all interoperable EU information systems, is one of four elements of interoperability.

This analysis is important in two ways. First, because it provides an answer to the legal aspects of biometric interoperable systems that process the biometric data of migrants. Secondly, the analysis of biometric templates is crucial for the last substantive chapter of this thesis which will investigate methods of protecting biometric data to eliminate the negative effects on

privacy and data protection during the processing of biometric data. The biometric template is what in most cases is being protected or encrypted, so it is vital to understand what the biometric template is, especially in the context of EU law.

3.4.1. The Interoperability of EU Information Systems: The Impact on EU Biometric Law

Interoperability is a concept that signifies the connection between EU information systems, namely Eurodac, the VIS, SIS, ETIAS (which does not process biometric data), ECRIS-TCN and EES. Interoperability is the ability of different operation systems to communicate.[717] Interoperability is set up in EU law by two regulations. One concerns the interoperability of EU systems in the field of police and judicial cooperation, asylum and migration, covering Eurodac, the SIS and ECRIS-TCN.[718] The other concerns the interoperability of information systems in the field of borders and visa, covering interoperability concerning the EES, VIS, ETIAS, and again the SIS.[719] The provisions of both regulations are similar, so one can consider them jointly as Interoperability Regulations.

Interoperability redefines the purposes for processing biometric data, the conditions of storage, and the conditions of access to biometric data. Interoperability makes access easier for public authorities. The Interoperability Regulations do not change the fact that the processing of personal and biometric data is regulated either by the GDPR, the LED,[720] or if it concerns the processing of personal data of EU bodies, the EUDPR.[721] An analysis of how the processing of biometric data is regulated in general in EU law was presented in Chapter 2.

Interoperability represents new operations in the processing of personal and biometric data because it entails storage and access. EU information systems were developed at different times and for different purposes, and the way that data are organised in these systems differed. But that will remain only a historical fact once interoperability comes fully into force. The reality is that there are nominally different information systems, but which now share a common

[717] EDPS, "Reflection Paper on the Interoperability of Information Systems in the Area of Freedom, Security and Justice" (2017).
[718] 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 PE/31/2019/REV/1 [2019] OJ L 135/85 (Regulation 2019/818 of the Interoperability Regulations), Article 3.
[719] Regulation (EU) 2019/817 on establishing a framework for interoperability between EU information systems in the field of borders and visa PE/30/2019/REV/1 OJ L 135 (Regulation 2019/817 of the Interoperability Regulations), Article 3
[720] Recital 54 of both Interoperability Regulations.
[721] Recital 69 of Regulation (EU) 2019/818; Recital 73 of Regulation (EU) 2019/817.

infrastructure that makes it possible to search data simultaneously. The CJEU has recently weighed in on the importance of interoperability in the context of processing biometric data, by stating that the interoperability of document verification systems, in particular of facial images and fingerprints, is an objective of general interest to the EU.[722] Consequently, fundamental rights and freedoms could be restricted as a result of interoperability by relying on this objective, provided that the action is proportionate.

Interoperability allows public authorities to check whether there are personal data, including biometric data, of a person in any of the connected databases. This can be done without fulfilling further access conditions.[723] An important consequence of interoperability is that it relieves Member States of the obligation to consult national databases or automated fingerprint identification systems of other Member States before consulting simultaneously all the interconnected EU databases.[724] Interoperability in general allows law enforcement authorities to check whether personal data exist in any of the connected information systems. Overall, law enforcement access is facilitated.[725] In relation to simultaneous access, the basic safeguard is what is known as the two-step consultation approach.[726] Simply put, authorities may in the first step receive information on whether there are queried personal data in one of the databases, and will need in the second step to satisfy the requirements to access the data. Interoperability may provide visa authorities, border guards, the police and other authorities access to all six databases even if these authorities are not specified in a particular database as having access as competent authorities.[727] There are many other possible breaches of fundamental rights that stem from interoperability, as identified by Blasi Casagran, who listed the potential violation of multiple data processing principles as well as fundamental rights, particularly in relation to the processing of biometric data.[728]

[722] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251., para 88.
[723] N Vavoula, "Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?" (2020) 26 European Public Law 131.
[724] Regulation (EU) 2024/1358, Article 33(2).
[725] N Vavoula, "Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?" (2020) 26 European Public Law 131, 140.
[726] eu-LISA, "Single Programming Document 2022–2024 European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice Single Programming Document 2022–2024 2020-323 Rev 2 (2021), 67; Recital 35 of the Interoperability Regulations.
[727] C Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21 Human Rights Law Review 433, 443.
[728] ibid, 443-456.

Interoperability is treated as an end in itself, as noted by Vavoula.[729] The purpose of interoperability is to contribute to the objectives underlying information systems by, *inter alia*, supporting the purposes of these information systems.[730] The purposes and the means to achieve them are not clearly distinguished in the Interoperability Regulations. The EDPS raised criticism that the purposes of interoperability are not well defined and that there is no clear distinction between the objectives of interoperability which serve legal and those which serve technical ends.[731] Technology should be used to achieve the legally recognised objectives of general interest, and that technological improvement should not be an end in itself. The Interoperability Regulations state that all new processing actions on personal data are limitations of the rights under Articles 7 and 8 CFR but that this is justified by the objectives of these systems, namely the effective management of the Union's borders, the internal security of the Union and the effective implementation of the Union's asylum and visa policies.[732] These should be viewed as the objectives of interoperability. The Court in *RL v Wiesbaden*, in the context of the interoperability of identity documents and passports, stated that such interoperability is an objective of general interest.[733] The opinion of this author is that interoperability should be recognised as a means to achieve certain objectives of general interest, not as an interest in itself. It can hardly be imagined that the EU population has an interest in documents or biometric systems being interoperable. Interoperability only serves as a tool to achieve the greater security of the EU or to prevent document or identity fraud. Thus, the legislator and the CJEU are mistaken when they interpret interoperability as an end in itself.

3.4.2. Components of Interoperability

There are four components of interoperability. These are the European Search Portal (ESP), the sBMS (shared Biometric Matching Service), the Common Identity Repository (CIR), and the Multiple Identity Detector (MID). Not all are equally important from the perspective of biometrics and EU biometric law, but all influence the processing of biometric data of migrants contained in the interoperable EU biometric systems. The sBMS raises particularly interesting questions in relation to the nature of the biometric template, so this will be dealt with in a separate section. Naming the ESP, sBMS, CIR and MID as "components" does not properly

[729] N Vavoula, "Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?" (2020) 26 European Public Law 131, 636.
[730] Interoperability Regulations, Article 2(1) and Article 2(2)(g).
[731] EDPS, "Reflection Paper on the Interoperability of Information Systems in the Area of Freedom, Security and Justice" (2017), 19.
[732] Interoperability Regulations, Recital 40.
[733] Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251, para 88.

reflect reality. In terms of their function as places of processing personal data, they should be considered to be (new) databases, not mere components.[734] What is more, some of these components not only store, but process biometric data through other operations.

3.4.2.1. Multiple Identity Detector (MID): Links as New Types of Biometric Data?

The stated dual purposes of the MID are facilitating identity checks for genuine travellers and combating identity fraud.[735] The MID is necessary in order to correct inaccurate, incomplete or fraudulent data across multiple systems, as there is currently no way to do this, if the Interoperability Regulations are to be believed.[736] The MID is a database of what the Interoperability Regulations call links. Links can be viewed as personal data that signify that there is a connection between personal data in multiple databases (effectively that the same person may be enrolled in more than one database). The processing of links represents an action of processing personal data because the link is new information relating to a person – that the person's data are present in multiple EU information systems. Since these links did not exist before the MID was set up, the Interoperability Regulations correctly recognised that it is necessary to stipulate the right of access to, rectification and erasure of personal data (links) stored in the MID.[737]

MID links are defined as yellow, green, red and white.[738] Any link means that the MID has indicated that (possibly) the same person's data are enrolled in multiple databases.[739] A yellow link means that manual verification of personal data (including possibly manual verification of biometric data) has not yet taken place.[740] A green link signifies that the linked data actually concern different persons, which has been verified by a comparison of biometric data or by manual verification of identity data by the authorities.[741] A red link signifies that the authorities have checked the multiple identities and established that it refers to one or more persons in an unjustified manner, which may indicate fraud.[742]

---

[734] C Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21 Human Rights Law Review 433, 439-440.
[735] Regulation (EU) 2019/818, Recital 24; Interoperability Regulations, Article 25(1).
[736] Regulation (EU) 2019/818, Recital 38.
[737] Interoperability Regulations, Article 48
[738] ibid, Articles 30-33.
[739] For a simple graphical explanation of links, see Figure 3 in C Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21 Human Rights Law Review 433.
[740] Interoperability Regulations, Article 30.
[741] ibid, Article 31.
[742] ibid, Article 32(1).

The manual verification of biometric data which is triggered by certain links presents a conundrum in terms of the definition of biometric data. According to the EU law definition, technical processing is a constituent part of biometric data. Therefore, if the same fingerprint is processed manually rather than technically, the manual processing of the fingerprint for the purpose of biometric recognition would be the processing of personal and not biometric data. The limits of the current definition of biometric data (from the GDPR and LED, but also the AI Act)[743] can be seen in this case. The manual processing of a fingerprint does not change the nature of the fingerprint nor the purpose of the procedure. It can be argued that the manual processing of a fingerprint is even more stringent than automatic processing – it is done to check the results of automatic comparison. After all, biometrics existed before the automatic comparisons of fingerprints by machines, but in the sense of the EU definition, pre-automatic biometrics (not processed by technical means, but manually) does not concern the processing of biometric data. Thus, the requirement of technical processing shows its downsides in the example of the manual verification of biometric data following a link in the MID.

The Interoperability Regulations invoke the data minimisation principle of Article 5(1)(c) GDPR, by which the processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[744] One of the Interoperability Regulations claims that interoperability components do not store any new personal data besides the links in the MID.[745] This is not true, if only because the sBMS contains its own copies of biometric data, in parallel to biometric data held in the CIR (only in a different format). Since the Interoperability Regulations are justified on the premise that only the MID stores new data and that any other storing of personal data would go against the data minimisation principle, one can conclude that by its own criteria, interoperability infringes the data minimisation principle.

3.4.2.2. The European Search Portal: More Than a Gateway

Public authorities use the ESP to search data related to persons in the information systems of the EU, including Eurodac, according to their access rights in that legal instrument. In essence, the ESP is used so that authorities of Member States as well as EU agencies can simultaneously access the EES, VIS, ETIAS, Eurodac, SIS and ECRIS-TCN as well as Europol data and

[743] See 2.5, 2.6 and 2.7 of the thesis.
[744] Regulation (EU) 2019/818, Recital 70; Regulation (EU) 2019/817, Recital 74.
[745] Regulation (EU) 2019/818, Recital 70.

Interpol databases in accordance with their rights of access.[746] The ESP can thus be understood as a window through which public authorities can view personal data stored in interoperable information systems.[747] The ESP and the sBMS are used to automatically find links between the same or similar data stored in the CIR and SIS. While the sBMS is used in relation to biometric data, the ESP should establish links between alphanumeric data from interconnected databases.[748]

Member State authorities will have a dedicated profile for each category of user created by eu-LISA. Each profile will have listed access rights, which is what data each profile may search for, and what data the profile has the right to receive.[749] Each query to the ESP will be made with either alphanumeric or biometric data. The ESP simultaneously searches for the data in Eurodac, the EES, ETIAS (which cannot be queried with biometric data), SIS, VIS, ECRIS-TCN, Europol data, Interpol databases as well as the CIR.[750] The user, such as the immigration authority of a Member State, will then receive all the data that is held in these systems and also in the MID (this then signifies that the person queried is in multiples databases) unless it does not have the right to access these data.[751] Vavoula summarises that the ESP is used in two principal ways. It is used for automated queries for the purpose of examining applications for travel authorisations under the ETIAS and for visas and residence permits under the VIS. Secondly, national authorities or an EU agency use the ESP to search all databases at once. For example, border guards can use the ESP instead of going through different information systems one by one.[752]

On the one hand, the purpose of the ESP seems simple and reasonable, in that the ESP presents a portal for accessing data. But, on the other hand, the ESP is hard to pin down as simply a portal. It can only be understood in relation to the sBMS because both are used to search different types of personal data for similarities, the ESP for so-called alphanumeric and the sBMS for biometric data similarities in connected databases, as two pieces of a puzzle. In viewing the effects of interoperability on the privacy and data protection rights of migrants, it is difficult to conduct a proportionality analysis because of the problem of determining whether

[746] Interoperability Regulations, Article 6(1)
[747] ibid, Article 6.
[748] ibid, Recital 41.
[749] ibid, Article 8.
[750] ibid, Article 9(1).
[751] ibid, Article 9(4)-9(6).
[752] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022) 613.

the ESP, and its interaction with the sBMS, is truly the least restrictive and most effective way of achieving the goals of interoperability.

Could there have been fewer components and function overlaps? For example, the role of the ESP is its toll for accessing data in other components of interoperability, but the ESP also serves the MID in finding links between personal data in multiple databases. The ESP further interacts with the sBMS in this task but also accesses the biometric data in all the databases in the CIR as well as in the SIS. The elements of interoperability are not separated from each other in terms of their purpose. Finally, one could imagine the radical idea of only one ESP-like system, which could suffice to achieve the basic intention of interoperability. All the databases would be connected only by the ability to search multiple databases at once, setting aside other interoperability aspects. The ESP would have to be set up in such a way as to compare biometric or alphanumeric data against each database instead of public authorities having to do so manually. This would lead to a drastic reduction in the scope of processing personal data. But this approach would not yield what is achieved by interoperability: the unification of information systems. In such a vision of interoperability, the reduced ESP would truly only represent a portal. This, of course would change the whole meaning of interoperability as well.

3.4.2.3. The Common Identity Repository (CIR): Storage of Biometric Data in Its Original Form

The CIR contains travel document data, identity data and biometric data for persons who are registered in Eurodac, the EES, ECRIS-TCN and VIS.[753] The Interoperability Regulations state that the CIR itself represents a new processing of personal data.[754] Nevertheless, the personal data in the CIR must be logically separated in accordance with the EU information system to which it originally belongs.[755] Logical separation does not mean it is physically separated (stored in a different place or on different hardware). The CIR creates an individual file for each person in the EES, VIS, ETIAS, Eurodac and ECRIS-TCN.[756] Data, including biometric data, are stored in the CIR instead of in each individual information system.[757] Vavoula calls the CIR a major design shift since the data are stored in the CIR instead of in each separate system.[758]

[753] Regulation (EU) 2019/818, Recital 26.
[754] Interoperability Regulations, Recital 23.
[755] ibid, Recital 27 and Article 18(1).
[756] ibid, Article 17.
[757] ibid, Recitals 22 and 23.
[758] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022) 620.

The CIR stores the biometric data of underlying information systems in the same form as the data are recorded for each system, and thus biometric data of a fingerprint image may be stored in a different form for Eurodac than for the VIS. Taking the example of fingerprint data, the EES stores fingerprint data as four fingerprints of the right hand,[759] while Eurodac stores "plain and rolled impressions of the fingerprints of all ten fingers".[760] The SIS stores what can more broadly be described as dactyloscopic data, which includes fingerprints and palm prints, which *may* consist of from one to ten fingerprints and up to two palmprints.[761]

As with the sBMS, the CIR will automatically add, amend or delete files as they are changed in corresponding systems.[762] The purpose of the CIR is to make access easier for law enforcement authorities to those databases that are not established exclusively for the purposes of law enforcement.[763] Broadly speaking, the CIR can be accessed for three purposes. The first is for police authorities to identify a person.[764] The second purpose is to resolve a multiple identity when it is detected in association with the MID.[765] Thirdly, the CIR is accessed for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, in specific cases and when there are reasonable grounds to believe that consultation with the CIR will contribute to the stated purposes. In particular, where there is a suspicion that a person connected with these crimes is in one of the databases.[766] The practical use case for the CIR is straightforward: if there is a person that the police of a Member State cannot identify, they can take fingerprints of that person and with those biometric data request a comparison with the CIR.[767] The CIR conveys whether there are matching data in any of the connected systems. The police can conduct a query with other personal data (which means identity data or travel document data, in the parlance of the Interoperability Regulations).

For criminal investigation, the police authorities can query the CIR. The conduct of processing (a collection) of biometric data for the purpose of consulting the CIR is determined by national laws.[768] Access to biometric data is conditioned on there being reasonable grounds to believe that consulting the CIR will contribute to the prevention, detection or investigation of the

[759] EES Regulation 2017/2226, Article 3(16).
[760] Regulation (EU) 2024/1358, Article 2(1)(q)
[761] Regulation (EU) 2018/1862, Article 42
[762] Interoperability Regulations, Article 19(1).
[763] ibid, Recital 25.
[764] ibid, Article 20.
[765] ibid, Article 21.
[766] ibid, Article 22.
[767] Regulation (EU) 2019/818, Recital 28.
[768] ibid, Recital 30.

terrorist offences or other serious criminal offences, in particular where there is a suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence is a person whose data are stored in the EES, VIS, ETIAS or Eurodac.[769] If any of the information systems contain matching data (that is, if the biometric data in the CIR are logically separated as belonging to any of these information systems), then the authorities must request full access, which is granted if the access conditions of the underlying system are satisfied.[770] The answer to the query that there are personal data in a particular information system is called match-flag. The match-flag itself is a form of personal data in that it indicates that the personal data of a specific individual are in the interoperable systems. Nevertheless, match-flag is interpreted to "constitute a very limited interference with the right to protection of personal data of the individual concerned (...)".[771] The information that a person is already in a database is valuable information for public authorities in their effort to identify an individual. Such information leads necessarily to further investigation and has significant consequences for the individual. Accessing such personal data can thus hardly be considered as limited interference.

3.4.3. Biometric Templates in the sBMS: Storage of Biometric Data in Interoperable Form

The sBMS stores biometric templates, which are defined as distinct from biometric data in the Interoperability Regulations.[772] Biometric templates are derived biometric data from underlying information systems, including biometric data from the SIS,[773] and, unlike the CIR, they do not contain biometric data from the SIS. The SIS, in addition to facial images and fingerprints, stores DNA profiles and palm prints as biometric data.[774] Since DNA profiles and palm prints are not in other interoperable information systems, the sBMS does not store them.[775] The action of storage implies that the sBMS is a database, as noted by Vavoula.[776] Storage also means that there is the processing of biometric data, since storage involves one operation of processing. The stated main purpose of the sBMS is to prevent one person having different (biometric) identities in multiple EU information systems by using one biometric template for all the interoperable systems.[777] Biometric templates are defined as mathematical representations

[769] Interoperability Regulations, Recital 31 and Article 22.
[770] ibid, Article 22.
[771] ibid, Recital 36.
[772] ibid, Article 4(12).
[773] ibid, Recital 18.
[774] Regulation (EU) 2018/1862, Articles 42-43.
[775] Interoperability Regulations, Recital 18.
[776] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022) 637.
[777] See similarly explained in Regulation (EU) 2019/818, Recital 22.

which are obtained by feature extraction from biometric data limited to the characteristics necessary to perform identifications and verifications.[778] This definition attempts to ensure that the information stored in the sBMS is not treated as biometric data, which would greatly relax the legal requirements for processing data contained in biometric templates.

The legal nature of biometric templates is disputed. The Interoperability Regulations imply that biometric templates are not biometric data. The position of this author is that considering their nature, and considering the concept of biometric data, biometric templates are biometric data. In the analysis, it will be clarified that it is important to properly designate biometric templates as biometric data and that the debate concerning biometric templates is of utmost importance for understanding EU biometric law concerning migrants and asylum seekers. All biometric systems currently use biometric templates, as the Interoperability Regulations themselves state.[779] Therefore, biometric templates are used in all existing EU biometric systems and are defined for those systems as biometric data.[780] The novelty of the legislator is the attempt to define the biometric templates of the sBMS as not being biometric data themselves.

Two implied arguments can be distinguished in the claim that biometric templates are not biometric data. The first is that biometric templates are a reduced form, a mathematical representation of the "original" biometric data and are thus not biometric data themselves. The second argument is that biometric templates cannot be reversed to reveal the image (the personal data) they were derived from and thus are likewise not personal data themselves. Therefore, biometric templates represent one of three possibilities: as biometric, personal, or not even personal data. Biometric templates, stored in the sBMS, could be considered to qualify as biometric data, in which case biometric templates should be processed under the strict legal regime for sensitive personal data. The second option is to consider biometric templates to be personal data, in which case biometric templates should be stored, used for comparison, accessed, and protected under the rules applying to non-sensitive personal data. Finally, biometric templates may be anonymous data, which is supported by the claim that biometric templates cannot lead to the identity of any person. In its impact assessment, the Commission referred to biometric templates as non-sensitive, dubiously claiming that biometric templates

[778] Interoperability Regulations, Article 4(12).
[779] ibid, Recital 18.
[780] For example, Regulation (EU) 2024/1358, Article 2(1)(s), defines biometric data as fingerprint and facial image data.

are mere "mathematic representations and not actual data",[781] (as if all digital data are anything else but a mathematical representation). Such a qualification of biometric templates as data that cannot identify a person benefits national authorities, eu-LISA, and other EU bodies because they are less restricted when processing what is effectively biometric data. The two arguments concerning the nature of biometric templates in the sBMS will now be critically examined.

3.4.3.1. Biometric Templates are Biometric Data Because They Function as Such

Biometric template is not a novel term in biometrics. It has been defined in ISO terminology as a set of stored biometric features comparable directly to a biometric probe.[782] This means that a biometric template is biometric data that are actually used for comparison. ISO vocabulary states that a biometric template is a type of biometric data.[783] An unaltered photograph is a biometric template if it is used for comparison. These reflections hold true in EU law, where a photograph is biometric data if it is processed technically for biometric recognition. Article 29 of the Working Party (A29WP, the predecessor of EDPB) document on biometrics recognised biometric templates as the data actually used for storage and comparison.[784] The paper states that templates should not be qualified as personal data only in cases where no reasonable means can be used to identify the data subject.[785]

One way of proving that biometric templates are biometric data is to show that biometric template have the functional elements of biometric data. The definition of a biometric template in the Interoperability Regulations already hints that templates are actually biometric data because the Regulations define them as containing characteristics necessary to perform identification and verification.[786] In addition, the Interoperability Regulations state that in order to search biometric data in the CIR and SIS, these databases use the biometric templates stored in the sBMS.[787] In other words, biometric data in the CIR or SIS are compared against "biometric templates" in the sBMS. That would not work if biometric templates were not actually themselves biometric data. The Interoperability Regulations define biometric template as a term distinct from biometric data. Biometric templates are defined in the Interoperability

[781] EU Commission, "Commission Staff Working Document Impact Assessment on establishing a framework for interoperability between EU information systems" SWD/2017/0473 final - 2017/0351 (COD), 5.1.2 and 6.1.8.2.
[782] ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics.
[783] ibid.
[784] A29WP, 'Working Document on Biometrics' (2003) WP 80, 4-5.
[785] ibid, footnote 11.
[786] Interoperability Regulations, Article 4(12).
[787] ibid, Article 14.

Regulations as "mathematical representations" and as distinct from biometric data, which are defined separately.[788] All biometric systems of the EU use biometric templates to conduct biometric comparisons, as also stated in the Interoperability Regulations.[789] Apart from making an artificial distinction between biometric templates and biometric data, the Interoperability Regulations recognise that biometric data constitute sensitive data.[790]

In its impact assessment, the Commission considers the sBMS to be an enabler of interoperability, but states that the sBMS is not a system, which can be interpreted as meaning that it is not a database that processes biometric data.[791] The same document states that the sBMS contains "non-sensitive" biometric templates.[792] The Commission, in its analysis of the objective of general interest, necessity and proportionality of the sBMS, seems to twist the truth when it states that biometric templates do not represent biometric data as taken from individuals but only a mathematical representation of these data.[793] This is incorrect because biometric data are not merely the data in the form of a photograph of a face or an image of the captured fingerprint. Instead, biometric data are defined functionally as data used for biometric recognition (verification and identification). The Commission's accompanying impact assessment concerning interoperability is lacking because it is based on this misleading assumption that biometric templates are not biometric data. In fact, the sBMS represents another place where biometric data are stored in addition to the CIR, so it should be justified with the understanding that storing biometric templates means the processing of biometric data. Biometric templates should be properly understood as biometric data in the meaning of the EU data protection legal framework or EU biometric law (as systematised in this thesis). Furthermore, any biometric data are necessarily a mathematical representation since all biometric data are always expressed as mathematical figures so that the computer algorithm can process it. Any digitally stored photograph is likewise a mathematical expression because what is actually stored as a digital photograph is a mathematical expression, and not a hand-painted picture stored in a vault.

A biometric template may represent a reduction of all the data that was captured (called a biometric sample) when a fingerprint was taken, or likewise a facial image. But this reduction

[788] ibid, Article 4(12) and Article 4(11).
[789] ibid, Recital 18.
[790] ibid, Recital 20.
[791] EU Commission, "Commission Staff Working Document Impact Assessment on establishing a framework for interoperability between EU information systems, 5.1.2.
[792] ibid.
[793] ibid, 6.1.8.2.

does not affect the function of biometric data, since what was discarded was only the data that was not necessary for biometric recognition. A biometric template keeps only that part of the captured biometric data that is important for an algorithm to conduct biometric verification or identification. As a hypothetical example, a facial image algorithm may need only the data concerning a small number of facial points measured from a facial image. These data points could be the distances between the eyes or the ratio of the length and width of the face.[794] In other words, the data that are stored, the biometric template, necessarily fits the definition of biometric data in EU law. The fact that not all the data that were captured end up stored as a biometric template does not affect this conclusion.

Furthermore, any photograph or an image of a fingerprint itself does not represent all the details of a face or a finger, down to the atomic level. Instead, any photograph is already a reduction of the physical world that is captured by a machine, constrained by its technical capabilities in recording reality. There are technical standards for collecting fingerprints and facial images that regulate how detailed in terms of pixels (dots) a fingerprint image or facial image needs to be in order for most used biometric systems to work.[795] A biometric template is thus nothing more than a reduction of data to the level necessary to conduct a biometric comparison, because there is no need to store more biometric data than is necessary for the purpose of biometric recognition.

A further argument goes that biometric templates are not personal data because biometric templates are merely strings of numbers, which are themselves meaningless.[796] The author of this thesis is reminded by a similar argument used in *Marper v UK*, where the UK government argued that DNA profiles are nothing more than a sequence of numbers that contains no intrusive information on the individual,[797] and that, being in coded form, computer technology is required to render the information intelligible.[798] The ECtHR disagree with those arguments and stated that DNA profiles are of a highly sensitive nature, and that this conclusion is not

[794] See EU Commission, "Commission Staff Working Document Impact Assessment on establishing a framework for interoperability between EU information systems" SWD/2017/0473 final - 2017/0351 (COD), Figure 6.
[795] For example, eu-LISA is involved in the development of software tools for the assessment of fingerprint quality (NFIQ2), facial image quality (OFIQ). See eu-LISA, "Technology Brief, Biometric Technology, Part 2. What Added Value Does Eu-Lisa Bring Through Biometrics?" (2024).
[796] Compare EU Commission, "Commission Staff Working Document Impact Assessment on establishing a framework for interoperability between EU information systems" SWD/2017/0473 final - 2017/0351 (COD), 5.1.2, with the definition of biometric data as in Article 4(11) of the Interoperability Regulations. The arguments of both sides are presented in N Vavoula N, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022), 638.
[797] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008) para 65.
[798] ibid, paras 74-75.

affected by the fact that the information is in coded form.[799] Similarly, it is clear that biometric templates, despite being in a certain form that is not intelligible by itself, are still highly sensitive personal data. First of all, personal data which need additional elements to identify a person are still personal data (only pseudonymised).[800] Secondly, there are no biometric data that by themselves reveal a person's identity – there is always the need for hardware and algorithms (other data) to make the identification. Thus, biometric templates are biometric data even though they are unreadable without the proper hardware and software (not to mention that processing biometric data requires electricity as well).

The whole debate on biometric templates should recall the unusual nature of biometric data in the sense that what biometric data are depends on how the data are processed and for what purpose, as follows from Article 4(14) GDPR.[801] If a photograph is technically processed for the purpose of biometric recognition, then the photograph is biometric data. Similarly, since a biometric template is automatically processed for the purpose of identification or verification, then the biometric template is biometric data.

Without the sBMS, it is not possible to compare biometric data in the CIR, as Blasi Casagran notes.[802] Vavoula also reaches the conclusion that biometric templates should be considered not only personal data, but biometric data.[803] It is debatable whether biometric templates should be considered even to be a reduced form of the original biometric data, since the only information that they reduce from the original data is the information that does not serve the purpose of biometric recognition. It is like claiming that images of the face printed in a passport are not photographs because a part of the actual image taken has not been reproduced. Biometric templates are biometric data without the parts which do not serve for the purpose of biometric recognition. Calling biometric templates anything but biometric data is a legal ruse that should be recognised as such.

---

[799] ibid, para 75.
[800] Regulation (EU) 2016/679, Recital 26 and Article 4(5). As argued also in this context by N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022) 638.
[801] See Chapter 2.2.2 of this thesis.
[802] C Blasi Casagran, "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21 Human Rights Law Review 433, 449.
[803] N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022) 639.

3.4.3.2. Biometric Templates Are Biometric Data Regardless of Irreversibility

The irreversibility of a biometric template essentially means that it is not possible to reverse the biometric template so that it reveals the facial image it originated from.[804] Irreversibility is thus a useful feature of biometric data, which may reduce the impact on privacy and data protection caused by the processing of biometric data. However, irreversible or not, a biometric template remains biometric data. The Interoperability Regulations in Recital 19 require that biometric templates must not be reversible to the data they were extracted from. This is a beneficial feature of biometric templates as stored in the sBMS. It may even be considered a necessary feature, since any protection that can be applied to personal data must be applied, as follows from Article 32 GDPR and from the principle of integrity and confidentiality of Article 5(1)(f) GDPR. The proportionality principle contained in Article 52(1) CFR likewise requires that a method which limits fundamental rights to the least degree must be used, which, applied in this context, would mean that if the irreversibility of a biometric template can be applied, it must be applied.

Irreversibility does not change the legal qualification of biometric data, something that the Interoperability Regulations in Recital 18 seem to imply by referring to biometric templates as an irreversible derivate of biometric data. Legal literature on biometrics has associated biometric templates with irreversibility. This line of thought holds that if biometric templates cannot be reversed to reveal the image they were derived from, they are not personal data since they do not reveal the image of the face.[805] But this argumentation is faulty. Biometric data do not need to show a face or a fingerprint to the naked human eye to qualify as biometric data. An essential element of biometric data is their ability to identify people by technical means. The mistake in the reasoning is that it takes a characteristic – reversibility – as a constituent element of biometric data, which it is not. To put it another way, biometric data do not need to reveal how a person looks to be biometric data. Irreversibility may be a beneficial characteristic that enhances the privacy and data protection rights of an individual and will be explored in the final substantive chapter of this thesis concerning the methods to protect biometric data.

[804] For a more technical explanation of methods of protecting biometric templates, see M Gomez-Barrero and others, "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters" (2016) 18 Information Sciences, 370–371.

[805] For an overview of the debate, see C Jasserand, "Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data" (2016) European Data Protection Law, 297–311.

The existence of biometric templates also shows a more fundamental problem with the processing of biometric data and its justifications.[806] If biometric templates as reduced versions of biometric data are sufficient to conduct a biometric comparison, then the biometric data as stored for Eurodac and other EU biometric systems in the CIR fail the proportionality test in view of fundamental rights. It is not justified to store biometric data in an unaltered form since the purpose of a biometric comparison can be achieved with biometric templates which are irreversible (e.g. do not directly show the face of a person). The storage of biometric data in a form that contains more information than is necessary to conduct biometric recognition is also contrary to the GDPR's data minimisation principle. The justification is that it is technically and politically complicated to force a single format on all the involved EU biometric information systems.

3.4.4. Concluding Remarks on Interoperability and Biometric Templates

A legal assessment of interoperability from the perspective of biometrics can be summed up in four critiques. First, the overall architecture of interoperability is complicated, and it is extremely hard to determine whether the current constellation of four components that overlap in their function and purposes is the least intrusive possible for the fundamental rights of migrants and other natural persons. The technical architecture of interoperability is extraordinarily complex, and it is hard even for an expert to make a claim about what is the best or the least complicated way of executing the purposes that are to be achieved with interoperability. This complexity is also likely the reason that the implementation of all systems concerning interoperability has been constantly postponed.[807] Understanding interoperability is a difficult task, because it requires a combination of legal and technical expertise. It is even more difficult to assess whether any alternative interoperability architecture might exist to limit the fundamental rights of migrants less than the solution adopted. As a principle in dealing with modern technologies, one solution would be to limit the complexity of any system to the level

[806] Kindt provides a nuanced discussion of the legal meaning of biometric template, but similarly concludes that the biometric template is (at least) personal data. See EJ Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Science & Business Media, 2013) 270.

[807] Neither all the information systems nor the elements of interoperability are yet ready for deployment and have been repeatedly delayed. See EU Commission, "Report from the Commission to the European Parliament and the Council on the State of Play of Preparations for the Full Implementation of the Interoperability Regulations in Accordance with Article 78(5) of Regulation (EU) 2019/817 and Article 74(5) of Regulation (EU) 2019/818" COM(2024) 293 final. In relation to the EES, after a series of missed deadlines, in December 2024 the Commission proposed an imminent "progressive" start of the EES. See EU Commission, "Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Regulation (EU) 2017/2226 and Regulation (EU) 2016/399 as regards a progressive start of operations of the Entry/Exit System" 567 final 2024/0315(COD).

at which legal scrutiny by legal experts is still feasible. It could make sense to prohibit "black box" algorithms and technologies whose results are difficult or impossible to legally assess or explain, even if this would limit the tools available for public authorities. It would share a similar logic to the precautionary principle,[808] in the sense that a technology should be prohibited if its future effects cannot be fully appraised or if there is doubt whether the effects on fundamental rights can be mitigated after its deployment.

The second point is that the purposes of interoperability as a whole and of individual components are not clear, or are not rooted in the objectives of general interest of the EU, but instead often refer to technical aspects of interoperability. Hence, interoperability is justified as an end in itself, which should not be the case. In the view of this author, the consequence of this incorrect view of interoperability as an objective instead of a means is that a genuine proportionality analysis cannot be conducted. This should lead to the conclusion that as things stand interoperability is an unjustified restriction of the privacy and data protection rights of migrants and asylum seekers.

The third critique of interoperability in view of biometric law is that there are more actions of processing biometric data than the legislator has accounted for. This means that actions which represent the processing of biometric data but are not recognised as such are not properly justified. It is not just that the MID creates new links, which lead to the processing of personal and biometric data, but also that the CIR and sBMS also represent actions of processing biometric data which are not properly justified.

The final and most consequential problem detected in relation to biometrics and interoperability concerns the biometric templates in the sBMS, which are disguised as not being biometric data, with significant consequences for the way such data are processed and protected. Ultimately, this leads to unjustified limitations of the fundamental rights of migrants and other persons whose biometric data, in the form of so-called biometric templates, are processed in the sBMS as part of an interoperability scheme. In essence, biometric data are protected by methods that protect biometric templates, as also noted by eu-LISA.[809] It is important to understand that biometric templates are indeed biometric data not only because any biometric recognition

[808] On the application of the precautionary principle to the free movement of persons in the EU, see I Goldner Lang, "'Laws of Fear' in the EU: The Precautionary Principle and Public Health Restrictions to Free Movement of Persons in the Time of COVID-19" (2021) 14 European Journal of Risk Regulation 141.
[809] See eu-LISA, "Technology Brief, Biometric Technology, Part 2. What Added Value Does eu-Lisa Bring Through Biometrics? (2024) https://www.eulisa.europa.eu/our-publications/eu-lisa-tech-brief-biometric-technology-part-2.

system uses biometric templates, but also because biometric templates are a form of biometric data upon which encryption and other privacy methods can be applied, as will be discussed in the last substantive chapter of this thesis.

Chapter 4: Fundamental Rights Analysis of Biometrics Applied in Migration and Asylum

4.1. Aims, Methods, and Structure.

The goal of this chapter is to analyse biometrics in the framework of fundamental rights. It is undisputed that the processing of biometric data is a limitation of privacy and data protection, as has been examined in the previous chapter. Privacy and data protection are the most important fundamental rights to frame the use of biometrics because the CJEU uses these to interpret the effects of such use by public authorities. The chapter is divided into three parts, corresponding to three groups of fundamental rights that may be affected by biometrics: privacy and data protection; the right to dignity (with a view to the way biometrics affect the right to asylum); and the right to non-discrimination in view of biometrics. In the first of the three parts, the examination will turn to the issues of why the right to privacy is important in view of biometric data processing and whether privacy can be distinguished from data protection. For the largest part, however, the first part of this chapter is a critical analysis of the way fundamental rights of privacy and data protection are used to justify and legitimise the use of biometrics.

There are also other fundamental rights and freedoms, as defined in the EU's Charter of Fundamental Rights, which are relevant when it comes to the use of biometrics by public authorities, particularly concerning migrants, and refugees. The main purpose of this chapter is to answer how rights are affected by the use of biometrics. This is the prerequisite for answering the main research question of this thesis, namely what tools can be used to limit the negative impact of biometrics on fundamental rights. Therefore, the second part of this chapter will analyse biometrics through the lens of the right to human dignity. This will include a view of how fingerprinting has developed from its eugenic origins and how human dignity as a legal concept was conceived precisely having in mind eugenic practices. The crucial issue in the second part of this chapter is the analysis of whether human dignity should prevent the forced fingerprinting of certain vulnerable groups and the effects that fingerprinting has on the right to asylum itself.

Facial recognition, a much more recent technology, is a particularly suitable study to examine whether the fundamental right to non-discrimination can be effectively used to challenge biometrics. This will be done in the last, third part of this chapter. In particular, algorithmic bias is a phenomenon that is usually associated precisely with facial recognition. Examining non-discrimination in relation to biometric algorithms opens up a discussion of the distinction

between bias and discrimination in the technical and legal sense, and of fairness, a value important to understand the dichotomy between the bias and accuracy of algorithms. The examination presented here shows the limits of technical solutions and the primacy of law grounded in policy and ethics when it comes to modern technologies such as facial recognition.

Not every fundamental right that can be brought into connection with biometrics will be analysed here. The focus is on fundamental rights and freedoms which are primarily important in the sense that the relation to biometrics is clear. Secondly, the focus will be on substantive rights since procedural aspects are rather more determined by the national legislation of Member States. Finally, the fundamental rights and freedoms chosen for analysis here make excellent studies of a particular problem within biometrics. The analysis of human dignity shines a light on the origins of biometrics and the issue of forced fingerprinting, while non-discrimination represents a solid legal background for examining problems raised by facial recognition.

4.2. Privacy (and Data Protection) as the Main Arena of EU Biometric Law

4.2.1. Introduction

Privacy and data protection are fundamental rights found in Articles 7 and 8 CFR. A specific trait of the EU legal order is that it contains separate rights to privacy and to data protection. The rights in the ECHR are closely related to those in the CFR, and the case law of ECtHR is particularly relevant for the development of EU biometric law, starting from the *Marper* case. The use of biometrics in EU law is regulated by a dual legal framework. One is the mentioned fundamental rights framework by which CJEU has examined whether the processing of biometric data is a justified limitation of the privacy and data protection rights of the CFR. The second legal framework applied in parallel to the fundamental rights framework is the data protection framework of secondary EU legislation. This concerns the application of the GDPR and LED (and in rarer cases the EUDPR) when it concerns the processing of personal data and of biometric data. The two legal frameworks cannot be strictly disentangled, but the GDPR and LED introduce specific rights of the data subject in the event of the processing of their personal data and principles that govern such processing. This was demonstrated particularly using the examples of the DPA's decisions in the cases concerning Clearview AI and Worldcoin.[810] The

[810] See 2.9 and 2.10 of the thesis.

provisions on biometrics in the AI Act should also be considered to affect the fundamental rights legal framework.[811]

This section will explain and analyse the privacy and data protection legal framework as it relates to biometrics, from a theoretical background to, most importantly, a critical assessment of how biometrics are framed as a justified limitation of the fundamental rights of privacy and data protection, as developed in the practice of the CJEU.

4.2.2. Privacy and Data Protection: Theory, Development and the Distinction Between the Two Rights

The legal interpretation of the right to data protection is contentious, with some scholars arguing for a separation of this right from the right to privacy, while others argue for the interdependence of the two fundamental rights.[812] In the analysis of this relationship, Tzanou concludes that data protection is a separate right, even if the separation is not clear, and that data protection is a relative newcomer as a right.[813] Privacy itself is a broader concept than personal data and, on the other hand, not all personal data are necessarily private.[814] The theories behind data protection and privacy can be described as being held by two broad camps of either instrumentalists or separatists, names that reveal the inclination towards the position that data protection is in the service of privacy or that it is a fully separate right.[815]

The development of the right to privacy is tied to technological development from its beginning in the realm of law. The legal concept of privacy was developed in the 19th century as a response to the launch of new technologies, such as mass (paper) media and photography. The right to property or certain moral rights were not enough to cover the intrusion into the private life of a person that can be caused, for example, by the reading of private letters. Photographs

[811] See 2.7 of the thesis.

[812] M Tzanou, *The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance* (Hart, 2017) 21-24.

[813] ibid, 22. The fault that this author finds with either approach is the implicit view that legal reasoning can be completely and rationally explained by an overarching theory that is grounded in law. This author considers, after examining the case law of the CJEU on biometrics in particular that the reasoning behind privacy and data protection, in relation to biometrics, can be explained only post hoc, that is, after a decision is made. Whether the CJEU will understand privacy and data protection as fully separate, somewhat detached or indistinguishable does not depend on the theory that the judges have on the issue of the duality of privacy and data protection but depends on the end goal they are trying to reach. Every scholar is aware of this reality, yet falls under the spell of trying to calculate the parameters of legal "science", which includes this author as well.

[814] ibid, 22; Case T-194/04 *Bavarian Lager* ECLI:EU:T:2007:334, paras 118-119.

[815] M Tzanou *The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance* (Hart, 2017) 31-46.

allow fleeting moments to be captured permanently and then possibly distributed in newspapers to millions of people. Modern technologies allowed this to happen. For example, a journalist might capture a photograph of a theatre actress caught in a less appropriate moment and then dispatch it far and wide as news.[816] Warren and Brandeis grasped the issue well by stating that "Gossip is no longer the resource of the idle and of the vicious, but has become a trade (...)".[817] Similarly, private letters of no particular public interest should nevertheless be protected from prying eyes. The home of a person and domestic life should likewise be protected from the interference of others, or of the state. Almost a hundred years later, in the second half of the twentieth century, there slowly appeared a similar need to protect personal data. This issue was raised with the rise of computers and the digitalisation of information.

The approach to the protection of personal data can be either to protect this by interpreting the right to privacy, or to establish specific laws on data protection. It can be argued that the use of biometric technologies raises new legal challenges in relation to privacy (and data protection). The reason is that biometric data, which are derived from unique human features, are particularly sensitive and vulnerable because of their intimate connection to the human individual. Biometric data are a digital representation of some part of the essence of an individual and which makes the individual different from any other. Another aspect of the particular value of biometric data is that they can reveal much more about a person than other personal data, such as an address or social security number. For example, DNA can reveal the health, life expectancy, and the physical and mental traits of an individual.

As will be further discussed, biometric data are not revocable in many circumstances. This means that if fingerprint data are stolen, or compromised in another manner, new fingerprint data might not be possible, since a person has only ten fingers. For the same reasons, biometric data, if in the wrong hands, can lead to the persecution of persons which the victim may find hard to avoid, since an iris scan, unlike a name, cannot be changed. For these, and certain other reasons, it can be argued that biometric data deserve particularly strict rules, a more consistent

[816] SD Warren and LD Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193, footnote 13.
[817] ibid, 196.

interpretation of existing rules,[818] or certain new rules in order to achieve a satisfactory level of protection of privacy and data protection.[819]

Thus, the pattern is that technological change causes new modes of invading the moral or physical aspects of a person, and rights are simply there to respond to these new kinds of interference. It will also be argued that there is a need to recognise or adopt the definitions related to biometrics, such as biometric data, revocability of the biometric template or the encryption of the biometric template, so that in the new technological landscape human and fundamental rights can keep up.

From the analysis of the development of privacy in lockstep with technologies, it emerges that there are two basic motivations for processing biometric data, or personal data in general. First, the motivation is economic, or for the pursuit of profit by (other) private individuals, in what is a horizontal relationship. This was true from the observations of Warren and Brandeis on using gossip as a resource which will sell newspapers. It is equally applicable today in the logic in which social media use private data to sell as a commodity, mostly for advertising purposes (or in the case of Clearview AI, selling AI processed biometric data to public authorities as an economic activity). The other mechanism for processing biometric data is that of public authorities, which are motivated to acquire information on private individuals, domestic or foreign. This second, vertical biometric relationship between public authorities and the individual is the more important one in the context of this thesis. Privacy and data protection apply, if differently, in both vertical and horizontal relationships related to using biometrics.

Biometric technologies, coupled with AI, disturb the precarious balance of rights and obligations between the individual and the State. Persons do not expect, as has already been mentioned in this thesis, their family photo, which was uploaded online, to be used against them without their consent. Showing one's face in public means something different from what it meant a decade ago, since biometric recognition allows, without the knowledge of the person concerned, to be identified and for their biometric data to be stored for future use. As was shown in the example of the ECtHR case *Glukhin*, individuals may change their behaviour in public

[818] Such as a consistent interpretation of the meaning of biometric data as sensitive personal data, as was argued in this thesis in 2.4.6 and 2.4.7. It is likewise important to understand that the biometric template is itself biometric data, which is argued in this thesis in 3.4.3.

[819] The need for certain new rules primarily relates to introducing new legal concepts relating to biometrics into EU legislation, such as defining the biometric template and concepts such as the revocability of the biometric template, in order to achieve a higher protection of biometric data that would limit the negative effects of biometrics on fundamental rights.

in fear that they can be identified and persecuted which causes a *chilling effect* on their civil rights.[820] In a similar manner, applying for international protection, or for an ID, which implies processing biometric data, may have new, unforeseen consequences for the rights of a person for many years following such an event.

The CJEU has interpreted privacy and data protection without distinguishing between the two, at least until more recently. Both in the context of the CFR and ECHR, the right to data protection has not been used as a right in itself, but as serving other rights and freedoms, and most notably serving the right to privacy.[821] The judgment in *Schwarz* is recognised in this thesis as a key judgment for EU biometric law, but it is also notable for representing the approach of the Court to delineating between the fundamental rights of privacy and data protection in general. In a nutshell, the CJEU examined both the right to privacy and to data protection in *Schwarz*, without making a distinction between them, by asserting that any processing of biometric data is a threat to both rights, examining at the same time justifications for the limitation of both those fundamental rights together.[822] In *Digital Rights Ireland*, the CJEU held that the retention of personal data constitutes interference with the fundamental right to private life under Article 7 CFR, while access to these personal data by national authorities constitutes an interference with both the right to privacy and to data protection (Article 7 and 8 CFR).[823] Fuster interprets this as an attempt by the CJEU to make a genuine distinction between the right to privacy and to data protection, but that the CJEU has not shown any clear perception of the essential difference between the two rights.[824]

4.2.3. Justifying Limitations of Privacy in Four Steps: A Biometric Checklist That Failed

Biometric technologies are fingerprint recognition, facial recognition and many others which use unique human features to determine identity. Since the use of biometric technologies requires an inspection of intimate, unique or essential human characteristics, it is understandable that it should be regulated strictly, particularly since these data are in digital form, which allows it to be stored for any period and to be accessed by numerous parties. In legal terms, therefore, biometrics may be considered to raise abundant legal challenges to

[820] See the analysis of the case in 2.8.2.2 of the thesis.
[821] Gloria Gonzàlez Fuster, "Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" (2014) 2, Birkbeck L. Rev., 265.
[822] ibid, 270.
[823] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238, paras 34-35.
[824] Gloria Gonzàlez Fuster, "Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" (2014) 2, Birkbeck L. Rev., 272-275.

human dignity, the right to be treated equally, access to asylum and also privacy and data protection. These topics are explored in this chapter.

Biometrics as technical phenomena mean the processing of biometric data that should be justified under the conditions of Article 52(1) CFR (and the requirements of secondary law legislation, such as the GDPR). Thus, the technical complexity of biometrics is in legal terms simplified to an exercise in justifying the limitation of privacy and data protection. This is the main lesson of the case law of the CJEU. This chapter will further explore other legal avenues by which biometrics can be interpreted, but the privacy and data protection legal framework remains the most important one. Biometric case law was critically analysed in Chapter 3 of the thesis, by exploring relevant judgments. All the cases were decided within the framework of privacy and data protection. There is no need to reiterate the analysis here. Instead, the key common elements of the fundamental rights analysis will be succinctly constructed and examined to answer the question of how privacy and data protection fundamental rights are applied in the case of biometrics.

The right to privacy is stated in Article 7, while the right to data protection is contained in Article 8 CFR. Article 8 CFR prescribes that everyone has the right to the protection of their personal data. The Article adds that personal data must be processed fairly, for a specific purpose, based on either consent or another legitimate purpose laid down by law. Further, everyone has the right to access data that concern them and the right to rectification. Finally, compliance with this right to data protection is assured by the control of an independent authority.[825] These aspects of data protection mirror the rights and principles of the GDPR and other secondary EU legislation on data protection, which was previously analysed in this thesis.[826] Contrary to the more fully elaborated right to data protection, the fundamental right to privacy under Article 7 is defined in succinct terms, even though it is mostly understood as the "big brother" of the right to data protection. Regarding the right to privacy, the CFR states that everyone has the right to respect for his or her private and family life, home and communications.[827]

[825] CFR, Article 8(2)-8(3).
[826] See particularly 2.3.2 and 2.3.3 of this thesis.
[827] CFR, Article 7.

The ECHR and its right to privacy has been highly influential in the development of EU biometric law.[828] The ECHR defines privacy as the right to respect for private and family life, which includes home and correspondence. The second paragraph of Article 8 ECHR defines the conditions for interference: that it is done according to the law, that it is necessary in a democratic society in the interest of either national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. Unlike the objectives of general interest of the CFR, the right to privacy in the ECHR contains a list of reasons that can serve as justifications for interference with privacy.

The rights to privacy and to data protection are not absolute fundamental rights. This means their limitation can be justified. Justification is possible under the terms of Article 52(1) CFR. The conditions for the justification of the limitations of privacy and data protection are that limitation is provided by law and that it respects the essence of those rights and freedoms. Limitations are further subject to the principle of proportionality, which means that they must be necessary and must genuinely meet the objectives of general interest recognised by the EU, or these limitations must be needed to protect the rights and freedoms of others. This is the blueprint for the analysis that the Court makes in biometric cases, most notably in *Schwarz* and in *RL v Wiesbaden*.[829]

Fuster notes that the Court in *Schwarz* took several "alarming" shortcuts in its analysis, most notably by equating the conditions of Article 8(2) CFR, which requires consent of the person or another legitimate basis laid down by law, to the condition of Article 52(1), by which a limitation of a fundamental right must be provided by law.[830] Foster continues that Article 52(1) is supposed to echo this criterion as developed in the case law of the ECtHR, where the legality requirement is understood as the foreseeability of the law, legal protection against arbitrariness, limited scope of discretion of public authorities and certain further criteria of the legality requirement.[831] However, the CJEU wrongly simplifies this substantive analysis of the qualities of the law on which the limitation is based by replacing it with the criterion that it is sufficient for the limitation to be based on a provision of Regulation 2252/2004.[832] On the other hand,

[828] See 2.8.2 of the thesis.

[829] See 3.2. of the thesis, particularly 3.2.1 and 3.2.6.

[830] Gloria Gonzàlez Fuster, "Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" (2014) 2, Birkbeck L. Rev., 270-271.

[831] ibid, 271.

[832] ibid, 271.

Vavoula concludes that the CJEU devotes more of the analysis to the proportionality principle, while the ECtHR focuses more on the legality principle.[833]

The CJEU examines the application of biometrics in four basic steps which broadly correspond to the requirements of Article 52(1) CFR for the justification of the limitations of fundamental rights, in the cases of rights to privacy and data protection, which are examined together. Similarly to the CJEU, the ECtHR has established that the systematic collection and storage of personal information on a certain individual by the State falls within the scope of Article 8(1) ECHR (which concerns the right to privacy, or more precisely the right to respect for private and family life).[834]

There has been a substantial amount of cases concerning biometrics, which were analysed as biometric case law.[835] However, in all of the cases, whether these concerned the processing of biometric data for the purpose of an identity card, a passport, or the storage of biometric data of migrants in a remote database, the Court affirmed these different actions of processing biometric data as justified, given their factual circumstances and considering the objectives of general interests that these uses of biometrics nominally promoted. The approach of the Court, where fundamental rights are always subservient to the interest of security and where the framework of fundamental rights always bends to meet security needs, was critically examined in that section on biometric case law.

4.2.3.1. The Blueprint for the Justification of Biometrics: The First Iteration.

The use of biometric technologies by public authorities in the EU is legally interpreted as the processing of personal (biometric) data which infringes privacy and data protection. Fingerprint data are regularly interpreted to mean personal or biometric data. Processing is any activity such as storage of fingerprint data or its collection. Each of these actions is a separate infringement of privacy and data protection. This has been established in *Schwarz*, and has been held consistently, most recently in *RL v Wiesbaden*, in which the Court again engaged in the exercise of examining biometrics as a justified interference with fundamental rights. Further, the legal basis for processing cannot be deemed to be the consent of the data subject, but rather has to be based on a law. The Court further established that Articles 7 and 8 CFR, which are examined

[833] N Vavoula, "Consultation of EU Immigration Databases for Law Enforcement Purposes: A Privacy and Data Protection Assessment" (2020) 22 European Journal of Migration and Law 139; N Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill, 2022), Chapter 1.
[834] *Rotaru v Romania*, App. no. 28341/95 (ECtHR 4 May 2000) para 44.
[835] See 3.2 of the thesis.

together, are not absolute rights, which means that their limitation can be justified by the conditions under Article 52(1) CFR. In *Schwarz*, the Court proceeded to a fundamental rights analysis in four steps, considering the facts concerning the use of biometrics.

The first condition is that the limitation of fundamental rights caused by biometric processing is provided for by law. This legality condition is the easiest hurdle to clear, since the only aspect that the Court examines is whether a law exits that requires the processing of biometric data, such as a passport or ID card regulation to that effect. In comparison, as was noted, the ECtHR devotes greater attention to whether the law on which interference of privacy is based satisfies certain qualities, such as limited scope of discretion and protection against arbitrariness.[836]

The second step in biometric case law is to determine the existence of an objective of general interest which justifies the limitation of fundamental rights. The CJEU devotes much more attention to this than to the previous step concerning legality.[837] However, the problem is that objectives of general interest can be deduced in various ways, meaning that there is always an opportunity for the Court to construct an objective of general interest that can serve as a justification of a biometric scheme. For example, the Court deemed that the purpose of having fingerprint data in the passports of EU citizens is to prevent illegal entry into the EU.[838] This is not convincing, since restricting the fundamental rights of hundreds of millions of EU citizens will not prevent illegal migrants coming into the EU. In cases concerning biometrics, the objectives of general interest are to combat document fraud or to prevent illegal entry. An even less convincing example of an objective of general interest which the Court has raised in cases concerning biometrics is the objective of the interoperability of the verification systems of identity documents.[839] As was noted in the case law analysis, interoperability can be considered as a means to achieve a certain objective of general interest, but in itself there is no public interest in documents being interoperable.

The third step in the fundamental rights analysis of biometrics is the requirement that the essence of fundamental rights be respected even in the case of limitation. This criterion does not represent a significant point of interest in any of the judgments concerning biometric technologies reached by the CJEU. The Court does not consider that the processing of

[836] See 2.8.2.1 of the thesis.
[837] See the *Schwarz* case analysis in 3.2.1 of the thesis.
[838] Case C-61/22 *RL v Landeshauptstadt Wiesbaden*, para 87.
[839] ibid.

fingerprint data infringes the essence of privacy or data protection.[840] In *Schwarz* it simply stated that there are no indications that processing fingerprint data does not respect the essence of fundamental rights. In *RL v Wiesbaden*, the Court held that the processing of biometric data does not have an impact on the essence of fundamental rights to privacy and data protection by referring to the conclusion in *Ligue de Droits Humains* and PNR data. As was noted, this is entirely incorrect, because the Court itself considered biometric data to be sensitive, while in *Ligue de Droits Humains*, it considered PNR data not to affect the essence of fundamental rights because it is not sensitive by nature.[841]

In the last step, the Court considers whether the objective of general interest is suitable (appropriate) and necessary. This part of the fundamental rights analysis incorporates most facts relevant to biometrics, such as the number of fingers involved in fingerprinting, the question of the reliability of fingerprint recognition, and the question of alternative methods of identification. The Court in *Schwarz* drew some debatable conclusions, such as that fingerprinting is not of an intimate nature and that the collection of facial images in addition to the collection of fingerprints does not represent a greater "discomfort" in comparison to only collecting fingerprints.[842] By responding that the moment of fingerprinting is not particularly intimate or discomforting, the Court concluded that the processing of biometric data as a whole is a justified infringement of privacy and data protection. This is a (subtle) logical fallacy, of the kind that claims the Sun is not hot because it does not shine brightly at night. Furthermore, it can be seen as contradictory to the claim that fingerprinting is not of an intimate nature since the Court in the same judgment also stated that biometric data are particularly sensitive personal data.[843]

4.2.3.2. Fundamental Rights Analysis of Biometrics 2.0: Layout and Argumentation.

RL v Wiesbaden represents the Court's analysis in more carefully devised steps than in *Schwarz*, slightly changing the layout of the fundamental rights analysis of biometrics. In the first step in *RL v Wiesbaden*, the Court separated two questions: what is the objective of general interest at stake, and whether the measure (collection and storage of fingerprint data) is appropriate for achieving the objective of general interest.[844] In the second step, the Court examined whether

[840] Case C-291/12 *Schwarz*; Case C-61/22 *RL v Landeshauptstadt Wiesbaden*.
[841] See 3.2.6.3 of the thesis.
[842] Case C-291/12 *Schwarz*, para 48.
[843] Case C-61/22 *RL v Landeshauptstadt Wiesbaden*, para 107.
[844] ibid, paras 85-97.

the measure is necessary for attaining the objective of general interest.[845] In examining necessity, the Court considered the arguments concerning the reliability of fingerprinting, compared to other identification methods, and how much of a fingerprint image is required to achieve identification.[846]

In the third step, the Court considered two questions. The first concerns the seriousness of the limitations of the rights to privacy and data protection. Here, the Court concluded that processing the biometric data in question is a serious limitation of fundamental rights, given the nature of the personal data and the huge number of persons involved in the biometric scheme.[847] To counter these arguments which speak in favour of prohibiting biometrics, the Court mentioned that biometric data are stored only locally on the document and not in remote databases, as well as the guarantees provided by the law. These include that only qualified staff would process the data and that there are special rules for vulnerable groups and that the data have to be stored on a highly secure storage medium. The Court transcribed these legal provisions without examining whether they have true substance. The Court proceeded to examine the significance of the objectives of preventing identity fraud and the production of false identity cards. The Court was not discouraged by statistics which pointed to a marginal amount of ID fraud, coupled with a trend towards a further decrease in such occurrences.[848] It found that there is a fair balance between the objective pursued and the limitation of fundamental rights.

This conclusion of the Court exemplifies the problematic nature of the proportionality analysis in cases concerning biometrics. The number of persons involved in the biometric scheme may be in the millions, and the extent of the limitation of their privacy and data protection may be determined to be significant, yet this is somehow offset by a marginal amount of ID fraud, which may not even correspond to the objective of general interest. A genuine proportionality exercise would first acknowledge the conflict that is being resolved between security and privacy. The objective of general interest does not prevent fraud or illegal entry, but it is the acquisition of knowledge on the identity of citizens, foreigners, migrants or any group of persons which contributes to the security of a political entity. The possibilities opened with the use of modern technologies and the mass harvesting of biometric and other sensitive data are

[845] ibid, paras 98-105.
[846] ibid.
[847] ibid.
[848] ibid, para 41.

too important to ignore, and if good actors are not doing it, malevolent ones certainly are. The story of biometrics is certainly not about false IDs. In order to predict how future cases concerning biometrics as an AI phenomenon will be resolved before the Court, it is more useful to grasp the importance of new technologies for identification to understand, first, the motivation of public authorities to use biometrics, and secondly the motivation of the Court not to enter into conflict with national authorities on issues possibly concerning national security and sovereignty but instead to provide a more or less convincing justification of biometrics within the framework of fundamental rights. The fundamental rights analysis of biometric law can always appear to be made on sound grounds and be consistent with past rulings.

4.2.3.3. A Blind Spot in the Biometric Fundamental Rights Analysis: Remote Databases

The biometric case law that was decided between *Schwarz* and *RL v Wiesbaden* reveals another structural weakness in the fundamental rights analysis of EU biometric law.

Among the crucial questions of the relationship between EU law and biometrics is whether the storage of biometric data in remote databases is contrary to the fundamental rights of privacy and data protection. This is the key issue in the cases that chronologically fit between *Schwarz* and *RL v Wiesbaden*. In both *Willems* and *A, B and P,* the Court refused to directly answer the question whether the creation of national biometric databases is contrary to fundamental rights. The Court relied on its conclusion from *Schwarz*[849] that the processing of biometric data is a justified limitation of privacy and data protection, even though the Court in *Schwarz* examined the biometric system only as the storing of biometric data on documents, not in remote databases, as facts concerning both *Willems* and *A, B and P*.

This sets the stage for two particularly inconsistent moments in the fundamental rights analysis in *A, B and P*. First of all, the biometric scheme in *A, B and P* concerned ten fingerprints, not merely two. In *Schwarz*, the biometric scheme was judged not to go beyond what is necessary since it only involved two fingers.[850] The Court in *A, B and P* is aware that the biometric scheme in this case involves not two, but ten fingers, yet it does not take it into account in the proportionality analysis, which is contrary to *Schwarz*. The second inconsistency in the analysis of the Court is that, in *A, B and P*, the Court concludes that that the fingerprint processing does not go beyond what is necessary because it is limited to third-country nationals.[851] Yet, in

[849] Case C-446/12 *Willems*, paras 46-48.

[850] Case C-291/12 *Schwarz*, para 48.

[851] Case C-70/18 *A, B and P*, para 61.

Schwarz, the fingerprinting involves a much broader group of EU citizens that apply for passports even though the objective of general interest is the prevention of *illegal entry* into the EU.[852] Applying the reasonable logic of *A, B and P* would mean that *Schwarz's* objective of general interest is either inapplicable or that the measure in *Schwarz* goes much beyond what is necessary, since it should target third-country nationals, as the measure does in *A, B and P*, and not EU citizens.

Therefore, predicting the outcome based on facts relating to the operation of a biometric system is not possible. If one studied *Schwarz* and concluded that the rule is that more than two fingers applied to collect fingerprints go beyond what is necessary and thus a fingerprint biometric system using ten fingerprints would be contrary to fundamental rights, one would be wrong. A fingerprint system is deemed justified on the basis that it collects and stores only two fingerprints from each person, and a fingerprints system that uses ten fingerprints is justified by relying on some other fact and ignoring the problematic ones. A checklist of facts that the Court considers important can only be made after the Court makes a certain judgment, but they have no predictive value. The ability to make verifiable predictions is a characteristic that separates scientific theories from pseudoscience. Thus, what in one judgment is a key element of analysis which justifies the limitation of privacy and data protection, in another is not deemed relevant. These arguments alone should break the illusion of the consistent and logical nature of biometric case law. The facts, expressed as parameters, can serve as guidance, but primarily as guidance for the Court to frame the decision, not as a genuine fundamental rights exercise.

4.2.4. Conclusion on Privacy and Data Protection Analysis of Biometrics

Privacy and data protection are the most useful and important framework for assessing the effects of biometrics, as far as EU law is concerned. Unfortunately, in the steadily increasing number of judgments reached before the CJEU the end result is always that the processing of biometric data is a justified limitation of fundamental rights, even if the facts change and contradict previous reasoning. Therefore, there is consistency of the Court in terms of the outcome which favours the use of biometrics, but that is less than can be said of the consistency of the legal analysis of the factors. There are recognised important biometric factors (that have been analysed in this thesis).[853] These include which biometric technology is used or how many fingers are required for fingerprinting, as well as accounting for the place and the duration of

[852] Case C-291/12 *Schwarz* para 47.
[853] See 3.3 of the thesis.

the storage of biometric data, the objectives for which the limitation of privacy and data protection is imposed, and the number of persons in the scope of a biometric system. But the problem is that there is no consistency in how these factors are accounted for by the Court. The layout of the fundamental rights analysis follows the contours of Article 52(1) CFR, but the facts relating to the biometric system can be used at different steps in this analysis (for example, the fact that only two fingerprints are processed was used in examining proportionality strictly in *Schwarz*, while the same fact was also used as evidence by the Court of the measure being appropriate in *RL v Wiesbaden*).[854] It now remains to be explored what other fundamental rights can offer in limiting at least certain uses of biometrics.

[854] Case C-61/22 *RL v Landeshauptstadt Wiesbaden*, para 89; Case C-291/12 *Schwarz*, para 48.

4.3. Human Dignity and the Rule of the Thumb

The hypothesis of this part of the thesis is that human dignity, a fundamental right, is infringed by the coerced fingerprinting of migrants. The assessment of this question will contain three parts, from the general to specific analysis of human dignity. First, the history of fingerprinting will show that there was a deeply troubling relationship between the use of human fingerprints and human dignity. The second part will show the problems of applying human dignity as a legal tool. In third part of this section, the analysis focuses on the fundamental right of human dignity and the problem of coercive fingerprinting of migrants, particularly in the context of Eurodac.

4.3.1. The Eugenic History of Fingerprinting

In his book *On the Origin of Species*, Charles Darwin uses the example of pigeon breeding to explain how deliberate selection of animal traits can result in a single species developing diverse traits in a very short time period, evolutionary speaking.[855] The most incredible example of human intervention are likely dogs, a single species with incredible variety in a single species. Humans selectively breed many animals. Popular dog shows consist of measuring how uniform the ears are, how curly the hair is, or if the eye colour is as prescribed by the standards for a certain 'noble' dog breed. What prevents such a way of thinking to be applied to humans as well? The question posed by some scientists following Darwin was whether the same methods of purposefully promoting good traits could be applied to the human species. Further, some may argue that such a eugenic policy might be even necessary, since with technological development, humans are no longer bound by evolutionary pressures. It was necessary to measure the biological properties of human beings in a scientific manner in order to be able to separate the "wheat from the chaff".

Eugenics was the pseudoscience tasked with improving the human population through nursing desirable traits. Biometry was the complementary science of measuring the biological characteristics of living organisms, so that there would be a scientific foundation in differentiating among humans.[856] Francis Galton was a polymath and a cousin of Charles Darwin who devoted much of his energies to determining the qualities of what he considered

[855] Charles Darwin, *On the Origin of Species* (general editor David Quammen, Sterling, 2008) 26.
[856] Biometry is still taught as a science of measuring biological properties of domesticated animals in agricultural studies (Croatian: biometrika).

to be human races. Galton thought that Darwinism, the process of natural selection under environmental pressure, no longer properly functions in relation to humans. To supplement natural selection, there needs to be, according to Galton, a deliberate effort to suppress the bad and promote the good traits of the human population.[857] Galton stated that eugenics, a term he coined, would make society function at a higher level.

"The general tone of domestic, social, and political life would be higher. The race as a whole would be less foolish, less frivolous, less excitable, and politically more provident than now. Its demagogues who *"played* to the gallery" would play to a more sensible gallery than at present".[858]

There are, however, more than a few fundamental problems with eugenics. Galton was very subjective in defining good human qualities, who possessed them, and how these qualities propagate.[859] The second problem was that at that time genetics were not properly understood. Mendel would author a paper in 1865 in an obscure scientific journal in Brno about the inheritance of traits in peas, but the paper remained misunderstood until it was "rediscovered" in 1900.[860] Galton never achieved his goal of scientifically proving the biological differences between "races" of humans. But in his research Galton discovered that certain human traits can be used to uniquely identify individuals. Galton published the book *Finger Prints* in 1892, with ample statistical evidence that fingerprints can be used to uniquely identify a person. Contrary to his assumptions, races cannot be identified from fingerprints, as he concluded by studying the fingerprints of "totally distinct races such as the Welsh and the Negro".[861] The sinister background of fingerprint recognition in Galton's book is shown by Galton's approach to studying the fingerprints of different classes and races of people, as he understood it.[862]

In the same year that Galton's book was published, in Argentina the first criminal case was resolved by using fingerprints. This was the start of the development of storing and comparing

---

[857] F Galton, "Eugenics: Its Definition, Scope, And Aims", (July 1904) 10(1) The American Journal of Sociology https://galton.org/essays/1900-1911/galton-1904-am-journ-soc-eugenics-scope-aims.htm
[858] ibid.
[859] As can be seen in his views expressed in his book, F Galton, *Hereditary Genius: An Inquiry Into Its Laws and Consequences* (1869).
[860] S Mukharjee, *The Gene: An Intimate History* (Penguin, 2016) 54.
[861] F Galton *Finger Prints* (MacMillan, 1892) 195 https://galton.org/books/finger-prints/galton-1892-fingerprints-1up.pdf.
[862] "The races whose fingerprints I have studied in considerable number are English, pure Welsh, Hebrew, and Negro; also, some Basques from the Cambo in the French Pyrenees, twenty miles south-east of Bayonne". ibid, 192.

fingerprints for the purpose of law enforcement, based on the scientific theory of Galton, and applied in this first case by Juan Vucetich, who was born in today's Croatia as Ivan Vučetić.

Fingerprint databases in the following decades grew exponentially. Some databases contained millions of fingerprints sets. The crucial further step was the electronic, or computer, revolution from the mid-20th century. Computers allow the automatic search and comparison of fingerprints. The thread connecting the origins of biometrics to its modern applications is unbroken. Thales is an immense European defence and security company that produces military equipment, but which is also a provider of biometric systems that form the technical side of Eurodac and other identification systems. Thales's website devoted to their fingerprinting solutions still mentions that "according to Sir Francis Galton (Charles Darwin's cousin), the probability of finding two identical prints is one in 64 billion, even with twins".[863]

During the Second World War, Nazi Germany used what could be considered a radical simplification of biometric identification by imprinting permanent numbers on the skin of a person instead of using fingerprint recognition. Eugenics remained an acceptable science until the end of the war, after which eugenics were slowly abandoned, though not all the ideas behind it.[864] Societies and journals which used the term "eugenic" were renamed in the later part of the 20th century with the terms "genetic" or "biosocial".[865] Governmental policies of forced sterilisation and separation of children from their families for the purpose of raising the children in a "civilised" manner continued to be practised in second part of the 20th century in the West. The most enduring and widespread offshoot of eugenics is biometrics, and, in particular, fingerprint recognition. Biometrics, unlike eugenics, have evolved, survived, and thrived.

Human dignity is a counterargument for racism, eugenics, and the exclusion of those who are different. Human dignity is not merely a philosophical term, but a legal one as well. The question then is whether biometrics, given their origins, inherently collide with the principles contained in human dignity.

---

[863] Thales's website, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history.

[864] A Rutherford, *Control: The Dark History and Troubling Present of Eugenics* (WW Norton & Company, 2022).

[865] The scientific journal Annals of Eugenics was renamed Annals of Human Genetics, the Eugenics Education Society became the Galton Institute in 1989 and then renamed in 2021 as the Adelphi Genetics Forum. The Eugenics Review, which used to be published by the Galton Institute, was renamed Journal of Biosocial Science and is now published by Cambridge University Press. Francis Galton himself founded the journal Biometrika, which principally convers statistics, and is still known under the same name since being established in 1901.

4.3.2. The Concept of Human Dignity: A Link Between Morality and Law.

In his widely regarded paper on the concept of human dignity, McCrudden states that human dignity provides an interpretation for human rights more than it provides content.[866] McCrudden explores the question of whether human dignity is a basis for human rights, a human right itself, or just another name for human rights.[867] He argues mostly for the first position, that human dignity is the basis of human rights (one could say, the justification) by recalling that the United Nations Charter, the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights (ICESCR) and the International Covenant on Civil and Political Rights all start with the mention of dignity.[868]

McCrudden identifies three aspects of the content of human dignity. The first is that every human being has intrinsic worth by being human.[869] The second is that this intrinsic worth should be respected by others. The third element of human dignity is the relationship between the State and the individual in connection with human dignity. The State is obliged to respect the human dignity of individuals in its actions. The question that arises from the content of human dignity is what forms of treatment are inconsistent with the worth of every human being, with their dignity? McCrudden states that human dignity has meaning beyond this core of three elements. Dignity may be viewed as a synonym for human rights, or as something slightly more substantial, as a unique value, upon which human rights are built.[870] This view of human dignity as a value, or a tool for the interpretation of other human rights, might be considered the dominant view in the EU legal order, as will be explained below. The strongest interpretation of dignity is that it is a right in itself, which is true of some jurisdictions where it can be enforced before courts.[871]

Given its unclear meaning, it is understandable that there is considerable critique of the concept of human dignity. For example, Rosen cites Schopenhauer who claims that dignity is just a façade for a lack of any real basis of morals, and Nietzsche who stated that dignity is a phantom developed to hide the brutal truth that people are actually slaves.[872] Rosen also reiterates the

---

[866] C McCrudden, "Human Dignity and Judicial Interpretation of Human Rights" (2008) 19 European Journal of International Law, 655.
[867] ibid, 656.
[868] ibid.
[869] ibid, 679.
[870] ibid, 680-681.
[871] ibid, 681.
[872] M Rosen, "Dignity: The Case Against". In C McCrudden (ed.), *Understanding Human Dignity* (British Academy, 2013) 144, https://doi.org/10.5871/bacad/9780197265642.003.0007&#62.

more nuanced view, known at least since the times of Plato, that dignity is an illusion which is nevertheless essential to the political order.[873] Rosen raises a number of arguments against the usefulness of human dignity as a concept. He states that since everyone has human dignity, it signifies nothing.[874] This could be considered the weakest argument against dignity. The strength of the concept is that every human is endowed with dignity, no matter what the status is of the person (in pre-modern period, *dignitas* represented the elevated status of a certain person, meaning that it was something that belonged to the few). That human dignity has a meaning can be seen from the way humans treat animals that they cultivate for food. Treating other human beings in such a way would be obviously against human dignity, yet human dignity is not extended to livestock.

Returning to Rosen's arguments, he attacks the work of Kant as unclear and transcendental. Kant is the originator of the concept of dignity in the modern sense, as something that every human possesses and that should never be compromised.[875] Rosen further states that dignity is the Trojan horse for religiously inspired attacks on equality, meaning that dignity is a term that was "smuggled" into law and morality by Christian thinkers to propagate their values.[876] Rosen thus positions dignity as a reactive, anti-liberal notion. He mentions that both the Universal Declaration of Human Rights (1948) and the German Basic Law or Grundgesetz (1949) give human dignity a central position, which to the mind of Rosen seems to signify a reconciliation, or a compromise, between liberal and social-democratic (Christian) values.[877] Rosen can be countered by raising the point that these documents mention human dignity precisely as a reaction to the cynical and ultimately horrific ways in which humans were treated in the period before they were enacted. Human dignity is vague and broad, but it was also important to the generation that experienced the atrocities of the Second World War. It is the way the law is applied that determines the effectiveness and meaning of human dignity. But, contrary to the position of Rosen, this does not mean that human dignity is useless.

Rosen makes two further engaging arguments against dignity. He states that dignity reduces individual autonomy.[878] The case repeated multiple times in the discourses on dignity is of a

[873] ibid, 144.
[874] ibid, 144.
[875] Hill Jr responds to Rosen by arguing for a better understanding of what Kant meant. TE Hill, Jr., "In Defence of Human Dignity: Comments on Kant and Rosen", Understanding Human Dignity (British Academy 2013) 313, https://doi.org/10.5871/bacad/9780197265642.003.0017&#62.
[876] Rosen, 147.
[877] ibid, 149.
[878] ibid, 149-152.

French dwarf who was prohibited from participating in a dwarf-tossing contest on the grounds that such activity violated his human dignity, despite the fact that he wanted to engage in the activity.[879] However, such an understanding of dignity as something that cannot be relinquished is not contrary to the current understanding in law, which prevents persons, for example, from willingly selling themselves into servitude.

The point about autonomy is moot in the context of this thesis. Biometric applications considered here are not based on the consent of the person. The action of processing biometric data (which may be detrimental to human dignity) is based on a legal obligation or a public interest that (supposedly) prevails over the individual interest. Nobody is asked whether they wish to be enrolled in a database of DNA for persons convicted of serious crimes or whether they want to provide their biometrics for crossing the border or for applying for asylum. Rosen (and the thinkers he reflected upon, such as Macklin[880] and Pinker[881]) imagine a world where people can always say no to biometrics if they feel uneasy about the procedure. In the world explored by this thesis, however, individuals are not "self-sovereign" in the way Rosen imagines.[882]

In the opinion of the author of this thesis, the more appropriate philosophical framework to analyse dignity and autonomy in the context of biometrics would be to consider Isaiah Berlin's two concepts of liberty.[883] Negative liberty is the absence of coercion, and it is the liberty that classical liberal philosophers usually have in mind. Coercion is something that is produced by others, such as forcing a hand to give fingerprints. It is negative liberty that Rosen seems to have in mind when considering human dignity. Positive liberty, as devised by Berlin, is a more sophisticated liberty, which entails being one's own master. Positive liberty means being able to choose freely, without being bound by norms or implicit pressures. This would mean choosing whether to be fingerprinted without the implicit coercion that refusal might jeopardise the asylum application, even if there is no physical coercion.

With that in mind, it is clear that a person who is forced to give fingerprints lacks either negative or positive liberty. However, even providing a choice of whether a person wants to

---

[879] ibid, 151.

[880] R Macklin, "Dignity Is a Useless Concept" (2003) 327 BMJ 1419.

[881] S Pinker, "The Stupidity of Dignity" (The New Republic, May 28, 2008) https://newrepublic.com/article/64674/the-stupidity-dignity&#62.

[882] Rosen, 150.

[883] I Berlin, "Two Concepts of Liberty". In I Berlin (ed.), *Four Essays On Liberty* (Oxford University Press, 1969) 118-172.

give fingerprints does not grant the individual positive liberty. If the person refuses to give fingerprints, they may lose the right to asylum, the right to stay in a country or may face grave consequences as a result of being returned to their country of origin. Even if there is no coercion, there is no real choice. This is why it is pointless to consider fingerprinting in the context of human dignity based on autonomy. As his final argument, Rosen shrewdly detects that European courts refuse to invoke the grounds of human dignity when it would be contrary to the actions of the State, such as in cases of mass surveillance.[884] With this argument, Rosen finally identifies the Achilles heel of human dignity as it is conceived in EU law. Human dignity is absolute, as long as it does not interfere with the power of the State.

Human dignity can be viewed as an essentially contested concept in EU law, according to Rodriguez, since it satisfies the seven criteria for such concepts.[885] Gallie, according to Rodriguez, developed the framework of essential contestability which should be understood as applying to concepts which at the same time raise strong opinions in their favour while also generating endless disputes.[886] It seems that describing human dignity as a contested concept is itself a negative normative claim related to the value and meaning of human dignity.

4.3.3. Human Dignity in EU Law: A Right and a Value under Threat.

This part of the thesis will explain what human dignity is as a legal concept in EU law in its multiple facets. First, the section will examine human dignity in EU law, and then in the second part, human dignity in the particular context of EU migration law. The crucial part of the analysis is to examine whether the practice of forced fingerprinting infringes human dignity, and what boundaries can be imposed on coercive biometrics by the concept of human dignity.

Human dignity features prominently in the European Union Charter of Fundamental Rights (CFR). The preamble mentions it first among the "universal values" of human dignity, freedom, equality, and solidarity. The first chapter of the CFR is named 'Dignity' and consists of five Articles. Human dignity is mentioned first among the rights. The CFR states in unequivocal terms that human dignity is inviolable and that it must be respected and protected.[887] From this wording it is clear that the legislator calls for the right of human dignity to be enforced, by stating that it must be protected. The text does not suggest that human

[884] Rosen, 153.
[885] P-A Rodriguez, "Human Dignity as an Essentially Contested Concept" (2015) 28 Cambridge Review of International Affairs 743.
[886] ibid.
[887] CFR, Article 1.

dignity is merely an (unenforceable) value. Human dignity has dual character under the CFR, as a right and a principle, according to Dupré.[888] It could be argued that the concept of (human) dignity actually appears in three forms, as identified above: as a value, as a foundation of the (first five absolute) rights in the CFR, and as a right in itself.

The CFR mentions eugenics in the right to the integrity of a person, one of the first five "dignity" rights in the Charter. It states that in the fields of medicine and biology, there must be free and informed consent of the person concerned and that there is a prohibition of eugenic practices.[889] From this, it is clear that the legislator was informed and influenced by the debate on the history of eugenics, the matter of consent, and its overall framing within the issue of (human) dignity when it drafted Article 3 CFR. However, the right to the integrity of a person (as a derivation of the concept of human dignity) from this wording in the CFR seems primarily to concern medical interventions in the human body, and in terms of eugenics, practices such as forced sterilisation or forced pregnancies.[890]

Other rights in the chapter on dignity are the right to life, the right to the integrity of the person, the prohibition of torture and inhuman or degrading treatment or punishment and the prohibition of slavery and forced labour. These five rights can also be understood as expressions of different aspects of human dignity. What is more, these five rights of the chapter on dignity of the CFR are absolute, meaning that they cannot be limited, nor can their limitation consequently be justified. This stands in contrast to other fundamental rights, such as the right to privacy, data protection or the right to non-discrimination, which can be limited within the terms of Article 52(1) CFR.

There is a difference however, between the right to human dignity of Article 1 CFR and the other four absolute fundamental rights mentioned in that chapter. The meaning of the prohibition of the death penalty is clear since it is not difficult to recognise an infringement. It is easier to recognise infringements of the prohibition of slavery or of torture than it is for infringements of human dignity. The right to the integrity of the person is explained in Article 3 CFR as referring to different medical and biological procedures and matters of consent in such procedures. However, the meaning of the right to human dignity is the vaguest. Combined

---

[888] C Dupré, *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Bloomsbury Publishing 2016) 166.

[889] Along with the prohibition of making the human body and its parts a source of financial gain and the prohibition of the reproductive cloning of human beings, Article 3 CFR.

[890] FRA, "Article 3 - Right to integrity of the person", https://fra.europa.eu/en/eu-charter/article/3-right-integrity-person.

with the fact that it is an absolute right, this creates problems for application, since if an action infringes human dignity in the least, it is absolutely prohibited. The question posed here is whether forced fingerprinting infringes human dignity, particularly that of children, or of persons with disabilities or persons fleeing persecution from their governments. The answer may be clearer once the analysis of the interaction of human dignity, biometrics and EU law is examined in further detail.

The influence of the ECHR and the case law of the ECtHR on the understanding of human dignity in EU law is significant. One reason is that the CFR recognises explicitly this influence in its Article 52(3). Human dignity is mentioned in the new Preamble to Convention 108 (Convention for the Protection of Individuals with regard to the Processing of Personal Data), which was a key influence in development of biometric concepts in EU law, as previously mentioned.[891] Human dignity may be affected by the way a biometric technology operates or by the data it processes.[892] The AI Act states that AI (which includes biometric technologies such as fingerprint or facial recognition) presents a risk for human dignity as a value of the EU, but also for fundamental rights.[893]

The CJEU has confirmed human dignity to be both a value of the EU legal order and a right in itself in the context of the EU asylum system, but also as an interpretative principle. The *Omega* case is the most important judgment of the CJEU in the matter of human dignity.[894] The facts concerned the simulated shooting at other persons presented as a commercial activity. This game was legal in other Member States but prohibited in Germany on the grounds of human dignity. The CJEU ruled that a measure that restricts the free provision of services in the EU does not have to be based on a uniform conception of human dignity. Human dignity is a common value, and a right in EU law, but can acquire different meanings in diverse EU countries.[895] This understanding of human dignity did not bring about greater clarity to the concept, but it established human dignity as a concept that can influence judgments. It can also be added that human dignity in this case was considered to be a general principle of (EU) law

[891] See 2.8 of the thesis.

[892] The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) has highlighted that the use of live facial recognition technologies in uncontrolled environments is particularly intrusive on the right to privacy and the dignity of individuals, coupled with a special risk of adverse impact on other human rights and fundamental freedoms (Consultative Committee on Convention 108, Guidelines on Facial Recognition 108 T-PD(2020)03rev4 5).

[893] Regulation - EU - 2024/1689, Recital 28.

[894] Case C-36/02 *Omega* ECLI:EU:C:2004:614.

[895] ibid, para 37.

drawn from the constitutional traditions of Member States, but also an independent fundamental right.[896]

The CJEU stated in a 2001 judgment that the fundamental right to dignity is a part of EU law.[897] In a case decided in 2021, the CJEU ruled that Member States may exclude from social assistance economically inactive EU citizens with temporary residence, even if those benefits are provided to nationals of the said Member State. However, benefits must nevertheless be provided to those citizens (with temporary residence) and their children if otherwise their fundamental rights, including the right to human dignity under Article 1 would be infringed by undignified living conditions.[898] The CJEU also interpreted EU law on human dignity by stating that an asylum seeker's human dignity must be respected by allowing the asylum seeker the possibility to provide for themselves and their family.[899]

The Opinion of AG Pikamäe in *WM v Stadt Frankfurt am Main*, a case concerning prison detention, stated that the prohibition of inhuman and degrading treatment or punishment of Article 4 CFR is absolute and also intricately linked to the right to human dignity of Article 1 CFR. The absolute nature of the Article 4 right in the CFR is confirmed by the corresponding Article 3 ECHR, from which no derogation is possible as stated in Article 15(2) ECHR.[900] The meaning and scope of Article 4 CFR is the same as in Article 3 ECHR, in accordance with the provisions of Article 52(3) CFR.[901]

The CJEU also used the concept of human dignity as an interpretative principle for secondary EU law, in particular concerning the entirety of the asylum process.[902] This raises the further use of human dignity as a tool for interpretation for the CJEU, besides the use of human dignity as a value, a right, and a foundation for other rights.

---

[896] ibid, para 34.

[897] Case C-377/98 *Netherlands v Parliament and Council* ECLI:EU:C:2001:523, paras 70-77.

[898] Case C-709/20 *The Department for Communities in Northern Ireland* ECLI:EU:C:2021:602.

[899] Joined Cases C-322/19 and C-385/19 *The International Protection Appeals Tribunal and Others* ECLI:EU:C:2021:11*,* para 69.

[900] Case C-18/19 *WM v Stadt Frankfurt am Main* ECLI:EU:C:2020:130*,* Opinion of Advocate General Pikamäe, para 123.

[901] ibid, para 108.

[902] N Bačić Selanec and D Petrić, "Migrating with Dignity: Conceptualising Human Dignity Through EU Migration Law", (2021) 17(3) European Constitutional Law Review, 498–516, 503, doi:10.1017/S1574019621000262.

4.3.3.1. Borders, Migrants and Control: Human Dignity in EU Secondary Legislation

Many key pieces of EU legislation concerning migration, asylum and processing of biometric data of migrants reiterate the commitment to respect for human dignity. The Schengen Borders Code stipulates that border guards must fully respect human dignity, particularly of vulnerable persons.[903] Likewise, the Frontex Regulation demands respect for human dignity in the performance of tasks which include access to asylum, and in the context of return operations.[904] Bačić Selanec and Petrić note that the dignity case law regarding the migration of third-country-nationals (TCNs) applies to the human dignity of Article 1 CFR in conjunction with other Charter rights, mostly with the prohibition of torture and inhuman or degrading treatment of Article 4 and the right to private life of Article 7 CFR.[905] Regarding these different conceptions of human dignity in EU law, it can be concluded that it represents a constitutional value in the Treaty of the European Union (TEU),[906] a fundamental right in itself, a general principle of EU law, but also a moral foundation for other fundamental rights.

4.3.3.2. Fingerprints and the Consequences of Refusal in EU and National Laws

EU legislation that governs the processing of biometric data includes a reference to human dignity. The Eurodac 2024 Regulation states that the regulation fully respects human dignity and fundamental rights,[907] and that Member States must respect the right to dignity and physical integrity of the person during the fingerprinting procedure and when capturing his or her facial image.[908] This statement, albeit formulaic, represents the legislator's acknowledgement that biometric procedures have the potential to infringe human dignity. The Eurodac 2024 Regulation specifies that it is the national laws that set the administrative measures for ensuring compliance with the obligation to provide biometric data, and that these national measures must be proportionate, effective and dissuasive and may allow the use of coercion.[909] If the national measures fail to ensure cooperation, the provisions of EU asylum law on this issue apply.[910] It should be noted that the obligation to provide a facial image for Eurodac, in addition to providing fingerprints, will raise new problems. Muslim women may

[903] Regulation (EU) 2016/399, Article 7(1).
[904] Regulation (EU) 2019/1896, Article 43(4), Article 50(3).
[905] N Bačić Selanec and D Petrić, "Migrating with Dignity: Conceptualising Human Dignity Through EU Migration Law" (2021) 17(3) European Constitutional Law Review 498, 503.
[906] Article 2 TEU.
[907] Regulation (EU) 2024/1358 (Eurodac 2024 Regulation), Article 1(2).
[908] ibid, Article 13(2).
[909] ibid.
[910] ibid, Article 13(4).

be forced to remove their veils, something that has already been registered as problematic.[911] The introduction of facial recognition may cause particular problems for fundamental rights which will be explored in the following section, after an analysis of the interaction between human dignity and fingerprinting. The EDPB stated that use of facial recognition objectifies the human face, and that human dignity requires that individuals are not treated as mere objects.[912]

Exceptionally, Member States are not required to collect biometric data if this is impossible due to the condition of the fingerprints or the face of a vulnerable person, for which the person is not responsible.[913] Importantly, the Eurodac 2024 Regulation makes the exception to provide fingerprints not just for any vulnerable person, but only for a person who is physically unable to provide fingerprints. In other words, this provision does not extend to persons who are vulnerable due to having suffered trauma, persecution, gender violence, mental illness or on account of being a (small) child over the age of six, for which there remains the fiction that they can be forced in a dignified and proportionate manner. Further, Member States are not required to collect biometric data if this is not possible for reasons of health of the data subject or for the protection of public health. Member States must collect biometric data within 48 hours of the expiry of these health-based exceptions.[914]

The refusal of a migrant to provide fingerprints may result in several negative outcomes for the person. The Eurodac 2024 Regulation envisages the possibility of administrative sanctions, which includes detention if the person refuses to provide fingerprints.[915] In short, the refusal may affect the application for asylum, may lead to detention, or may result in fingerprints being taken by the use of force. These administrative sanctions are regulated by EU law and have substantial effects on the fundamental rights of migrants. Particularly important are the implications on fundamental rights of forced fingerprinting, which raises concerns of human dignity. The refusal to provide fingerprints leads not only to the possibility of physical or psychological coercion, but also to sanctions that impact fundamental rights, including the right to asylum. It is revealing that according to FRA's report which considers the questions

[911] A woman was allegedly beaten because she did not want to reveal her face for taking of a photograph. FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 54.
[912] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (2022).
[913] Eurodac 2024, Article 13(5).
[914] Eurodac 2024, Articles 15(2), 18(3), 20(3), 22(6), 23(5), 24(5) and 26(4).
[915] FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 54; Eurodac 2024, Recital 53.

of human dignity and fingerprinting, there were almost a million recorded cases of persons being unable to provide fingerprints for the VIS, but no statistics existed for Eurodac.[916]

Depending on the legislation and practice of a particular Member State, migrants can be put into detention for refusing to have their fingerprints taken. The ECtHR examines the detention of irregular migrants in the framework of Article 5 ECHR. The ECHR serves as a guide to interpret Article 6 CFR.[917] Thus, both EU and ECHR law allow the detention of migrants, including in the context of refusing to have fingerprints taken.[918] Another set of consequences for refusing concerns the outcome of the asylum application. The Asylum Procedures Directive states that refusal to provide fingerprints (as required by Eurodac) may result in an accelerated asylum procedure.[919] Regulation (EU) 2024/1348, which will replace the above mentioned directive from 2026, states that the applicant must be informed that a refusal to provide fingerprints or a facial image may result in the rejection of the asylum application or a declaration of implicit withdrawal of the asylum application.[920]

As stated, Eurodac requires that national rules specify sanctions for failure to provide fingerprints. Croatian rules concerning the fingerprinting of migrants, the right to asylum and biometrics can be used as an example of how EU law interacts with national law on the subject of human dignity and fingerprinting. First of all, the Croatian Aliens Act stipulates that TCNs will be refused a residency permit if they do not agree to be fingerprinted.[921] The same Act states that TCNs who reside illegally, without identification papers or if there is doubt about their identification, or TCNs who are in the process of deportation, can be fingerprinted, have their irises scanned and their facial images taken without their permission for the purpose of determining identity or for law enforcement purposes concerning serious crimes.[922] TCNs can be put into detention on the grounds that they refused fingerprinting.[923] According to Croatian law, TCNs can apply for asylum at international border crossing points, or in limited circumstances, at police stations or at migrant residence centres, and are obliged to provide

[916] FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 48.
[917] Article 6 (3) TEU and Article 52 (3) of the Charter.
[918] FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 55-56.
[919] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast) [2013] OJ L 180/60, Article 31(8)(i).
[920] Regulation (EU) 2024/1348, Recital 31.
[921] Zakon o strancima NN 133/20, 114/22, 151/22 (Aliens Act), Article 170(2). All translations from Croatian are made by the author.
[922] ibid, Article 217(2).
[923] ibid, Article 214(3).

fingerprints and have their photograph taken.[924] If they refuse, they will be fingerprinted by force.[925] Further, if migrants refuse to provide these personal data, their request for international protection will be processed in a special, accelerated proceeding.[926]

4.3.3.3. Fundamental Rights of Vulnerable Persons and Forced Fingerprinting

In its discussion of the fundamental rights implications of the obligation to provide fingerprints for Eurodac, FRA notes that "it is difficult to imagine a situation where physical or psychological force to obtain fingerprints for Eurodac would be justified".[927] However, FRA avoids explicitly stating that using force would be categorically contrary to fundamental rights. Instead, it focuses on all the aspects of the procedure of fingerprinting, such as providing enough information to migrants. The report does state that the use of either physical or psychological force entails a high risk of violating fundamental rights.[928] Likewise, FRA's practical guidance merely advises border guards not to use force,[929] but this is difficult to square with the obligation to (always) take fingerprints.

Asylum seekers and irregular migrants may refuse to provide fingerprints for Eurodac in order to avoid being transferred under the Dublin rules to another EU Member State, or because they fear that their personal data will be shared with their country of origin.[930] FRA has found that disproportionate force has been used against asylum seekers and irregular migrants.[931] The inability to provide fingerprints in the context of Eurodac may lead to the suspicion that the person is trying to avoid the procedure, even though officers interviewed by FRA reported that they rarely encountered intentional damaging of fingerprints.[932]

The human dignity of certain categories of persons is particularly at stake when their fingerprints are taken, due to physical factors or problems with understanding the consequences of the procedure. These include persons who are vulnerable due to their physical or mental condition, or persons who due to heavy physical work are unable to provide

[924] Zakon o međunarodnoj i privremenoj zaštiti NN 70/15, 127/17, 33/23, 17/25 (Act on International and Temporary Protection), Article 33(5).
[925] ibid, Article 33(7).
[926] ibid, Article 41(10).
[927] FRA, "Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac" (2015) 1.
[928] ibid, 2.
[929] FRA, "Border Control at External Land Borders and Fundamental Rights – Practical Guidance" (2022) 3.
[930] FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 10.
[931] ibid, 10.
[932] ibid, 48.

fingerprints (of sufficient quality).[933] A question arises of how an officer responsible for initial fingerprinting can, in advance and in the circumstances, determine whether the person has physical or mental difficulties or other visible or hidden vulnerabilities that would require special consideration. This insurmountable practical problems may undermine the human dignity of the data subject.[934] Some precautions are taken, depending on the Member State, such as by migrants filling out forms where they can designate their specific circumstances, but even these and other measures do not work well in practice.[935] Given these findings, FRA has advised EU Member States and Frontex to avoid using either physical or psychological force while fingerprinting.[936] FRA stated that suspected victims of torture, victims of sexual or gender-based violence or people who have suffered trauma should not be coerced into providing fingerprints.[937]

However, it is quite clear that it is impossible to detect vulnerable persons in advance. It is true that the human dignity of such persons will be harmed when they are forcefully fingerprinted. Secondly, vulnerable persons are often those that are entitled to be recognised as refugees. In other words, a large proportion of asylum seekers should not be required to provide fingerprints, since many of them have suffered trauma, violence or persecution that makes forced fingerprinting particularly traumatic. Nevertheless, EU law clearly requires fingerprinting of asylum seekers. In other words, the coercive fingerprinting of asylum seekers necessarily involves infringing the human dignity of a substantial number of people. Despite this, it was noted that FRA has not stated unequivocally that forced fingerprinting undermines human dignity and that it *must* therefore be prohibited. This position is understandable, since if fingerprinting were merely optional, the Eurodac system, and consequently the Dublin system would fall apart. Eurodac, and the Dublin system by extension, rely on fingerprinting to identify migrants and to determine whether and where they have applied for asylum before.

---

[933] ibid, 43-45.

[934] Fingerprinting is stressful for the staff, especially at nights or at times of arrival of large numbers of people, as observed by FRA. See FRA, "Opinions Biometrics", https://fra.europa.eu/en/content/fra-opinions-biometrics.

[935] "Observations during the field research, however, do not corroborate these findings. Observations at DMCPs and their service providers indicated that typically all applicants were treated the same, although wheelchairs and small steps for children were available in some DMCPs (VFS Lagos and Lviv). FRA observed a scenario where persons accompanying a visa applicant helped by pressing his hand onto the fingerprinting device. As the embassy staff were behind a glass window, they were unable to help". FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 45.

[936] FRA, "Opinion 4 on Biometrics", https://fra.europa.eu/en/content/fra-opinions-biometrics.

[937] ibid.

Overall, there are two broad reasons that explain why forced fingerprinting infringes human dignity. One reason that human dignity is infringed is if that person has a physical or psychological disability that prevents them from complying with fingerprinting. If such a person is forced, they are objectified, treated as a thing, and thus their human dignity is infringed. A second group of reasons that can be understood to cause the infringement of dignity is the capacity to understand the procedure, its consequences, and personal rights. This is particularly problematic in fingerprinting any (irregular) migrant because it is clear that such a migrant can hardly comprehend the web of rules, actions and consequences that stem from fingerprinting. Their rights according to the GDPR, such as the right to rectification, the principles of data processing, such as the principle of accuracy of data, the particular rules applicable to the processing of sensitive data, and, on top of that, the calculation of how the decision to provide fingerprints affects the outcome of the request for international protection, including the right to asylum. One should here recall that legislation acknowledges, as has been pointed out, that human dignity may be infringed in the process, but the important question is under what specific circumstances it is infringed. Finally, concerning the reasons why and how human dignity is infringed by forced fingerprinting, one should refrain from making a taxative list of actions that infringe human dignity and give this concept the space it needs to be applied in all kinds of circumstances that humans can envisage for other humans.

In conclusion, coerced fingerprinting, which is a matter of fact in EU and national law, cannot easily coexist with the right to human dignity, as it stands. One has to give way to the other. Currently the principle of forced fingerprinting of migrants prevails. To change this and to give an advantage to the enforcement of fundamental rights and human dignity in particular requires changing the basic premise on which the asylum and migration system function.

4.3.3.4. The Effects of Fingerprinting on the Right to (Seek) Asylum

The obligation to provide fingerprints affects the fundamental right to asylum in a way that should be better recognised. The right to asylum and the principle of non-refoulement are strongly associated with EU asylum law.[938] The principle of non-refoulement in the broadest sense may be affected by the refusal of a person to be fingerprinted, since such a refusal may lead to an accelerated asylum procedure and deportation. The right to asylum might in effect be suspended by the refusal to provide fingerprints, as was already noted. The principle of non-refoulement may also be affected by the difference between the reality and practice of EU

[938] Article 18 CFR and Article 78(1) TFEU.

law.[939] It should be noted that there is still a lack of doctrinal clarity on the overlap between the right to asylum of Article 18 CFR and the principle of non-refoulement, as noted and explored by Costello.[940] The right to (seek) asylum may be interpreted to mean the right to ask for asylum or even the right to be recognised as a refugee. Non-refoulement is recognised in legislation concerning the so-called Pact on Asylum, including in the Screening Regulation,[941] or the Asylum Procedure Regulation.[942] There is significant literature on questions of the scope of the right to asylum and on the tensions between EU asylum law and international law, as well as within different Member States and their approach to the dilemma of security and human rights.[943] However, whatever the exact content of the right to asylum is, this right may be forfeited if the person does not agree to fingerprinting.

The refusal to provide fingerprints may significantly affect the person's right to asylum. The right to asylum, as a fundamental right under Article 18 CFR does not, on the face of it, include the obligation to provide biometric data.[944] However, taking into account all the provisions relating to asylum, the right to asylum is coupled with the obligation to provide fingerprints, because access to asylum is practically conditioned upon providing fingerprints, as stipulated in secondary EU law such as the Eurodac 2024 Regulation and national laws. This means that in practice the right to asylum has been implicitly changed by the requirement in Eurodac to take fingerprints (and soon also the requirement of collecting facial images for facial recognition databases). EU biometric law has thus affected the basic definition of a refugee, meaning that a refugee is a person who, owing to a well-founded fear of persecution on defined grounds, is outside their country and is unable or unwilling to seek the protection of their own

---

939 I Goldner Lang and B Nagy, "External Border Control Techniques in the EU as a Challenge to the Principle of Non-Refoulement" (2021) 17(3) European Constitutional Law Review 442.

940 C Costello, *The Human Rights of Migrants in European Law* (Oxford University Press, 2016).

941 Regulation (EU) 2024/1356, Articles 3 and 10.

942 For example, Regulation (EU) 2024/1348, Article 10(5).

943 See, for example, Violeta Moreno-Lax, "Mutual (Dis-)Trust in EU Migration and Asylum Law: The 'Exceptionalisation' of Fundamental Rights". In S Iglesias Sánchez and M González Pascual (eds.), *Fundamental Rights in the EU Area of Freedom, Security and Justice* (Cambridge University Press, 2021); M Moraru, "The EU Fundamental Right to Asylum: In Search of Its Legal Meaning and Effects". In S Iglesias Sánchez and M González Pascual (eds.), *Fundamental Rights in the EU Area of Freedom, Security and Justice* (Cambridge University Press, 2021); E Guild, "The Europeanisation of Europe's Asylum Policy," International Refugee Law (2017) 18(3-4), https://doi.org/10.1093/ijrl/eel018.

944 Setting aside the possible differences in meaning of the right to asylum and the right to seek asylum and the meaning of either of these concepts in EU law, as succinctly delineated in I Goldner Lang and B Nagy, "External Border Control Techniques in the EU as a Challenge to the Principle of Non-Refoulement" (2021) 17(3) European Constitutional Law Review 442.

country, and, additionally, a person who has provided fingerprints and a facial image. Otherwise, refugee status may not be recognised.[945]

One may be reminded of a similar effect of biometric law that was detected in relation to the right to free movement. As was stated in the analysis of *RL v Wiesbaden*, it can be interpreted that the position of the CJEU was that biometrics are used to facilitate the right to free movement, not as a restriction of it.[946] The logic of the Court was that free movement requires identity documents, and identity documents require biometric data in order to be reliable. However, this means, in the opinion of this author, that the fundamental right to free movement has effectively been changed by biometric law, since free movement entails an obligation to provide one's fingerprints. Similarly, the right to asylum seems to implicitly require the obligation to provide fingerprints. This all means that the right to asylum, which is a fundamental right belonging only to non-citizens, and the right to free movement, which belongs to EU citizens, both imply an obligation to provide biometric data.

There is the flip side of the coin of forced fingerprinting which is related to pushbacks. The significant problem of "alleged" pushbacks will not be addressed in any detail in this thesis.[947] Pushback is the practice of public authorities physically pushing migrants back across the border, or not allowing them to access the territory, by using various degrees of force. Pushbacks are, though not categorically, contrary to international law and fundamental rights.[948] Pushbacks negate the human dignity of an asylum seeker, but they also infringe other fundamental rights, notably the right to asylum. The practice of pushback is linked to biometrics because it represents the policy of the refusal of public authorities to register migrants (so that the Member State concerned will not be responsible for the irregular migrant under the Dublin system). Pushbacks thus represent a tactic of the State to avoid fingerprinting migrants, which is a reversal of the situation in which the migrant is the one actively avoiding fingerprinting. The situation where the migrant does not want to be registered in a certain

---

[945] It can here also be noted that case law of CJEU points to similar logic regarding the free movement of EU citizens and biometrics. The judgment in *RL v Wiesbaden* in effect stated that free movement is a right of EU citizens which is coupled with the obligation to provide biometric data. Free movement thus includes the obligation of the citizen to provide fingerprints. This perspective on the right to free movement of EU citizens is not visible until one considers EU biometric case law.

[946] See 3.2.6.2 of this thesis.

[947] On allegations of pushbacks, see, for example, the contribution of the Border Violence Monitoring Network (BVMN) "Input by Civil Society Organisations to the EUAA Asylum Report 2024 by the Border Violence Monitoring Network" https://euaa.europa.eu/sites/default/files/2024-02/border_violence_monitoring_network.pdf.

[948] I Goldner Lang, "Pushbacks against the Child's Best Interests" Ver Blog, 2022/1/07, https://verfassungsblog.de/pushbacks-against-the-childs-best-interests/ DOI: 10.17176/20220107-195129-0.

Member State, and that State does not want to register them, has led to situations similar to that during the so-called migrant crisis which reached its peak in 2015, leaving its trail in the case law of the CJEU.[949]

4.3.3.5. The Paradox of Proportionate Coercion and Human Dignity

Forced fingerprinting of vulnerable persons raises a significant legal conundrum. It is not possible to effectively detect vulnerable persons in advance of fingerprinting since this would require detailed examination. Besides, many categories of vulnerable persons are not exempted from forced fingerprinting in any case. As a consequence, the right to human dignity and other fundamental rights such as the right to asylum are being infringed by the forced fingerprinting of certain categories of persons.

There is no easy solution to this problem. All persons, as a general rule, are fingerprinted, by force if necessary. This is the current practice. This approach is necessary for a functional Eurodac system. The second solution would be to focus on human dignity and other fundamental rights, which would require putting effective mechanisms in place to make sure vulnerable groups, including children, people with mental or physical illnesses or people who have suffered trauma are exempted from forced fingerprinting. However, this solution is impossible to apply, since there is no method to effectively detect such vulnerable persons, especially in the hectic context of the fingerprinting procedure. The second solution would thus require abandoning forced fingerprinting altogether. If the fingerprinting is optional, it is clear that it would become useless since most migrants would opt out of the processing of their biometric data. This would prevent Eurodac from effectively determining the identity of migrants, and the asylum system would have to rely on 20th century methods of collecting names, date of birth, and other biographical information which are prone to error, unlike biological characteristics. In other words, either there is a focus on the identification of migrants, which requires forced fingerprinting, or priority is given to fundamental rights, in which case fingerprinting must be optional.

The FRA interpretative sources on fingerprinting and human dignity, as well as the Eurodac 2024 Regulation, implicitly argue that there is a third way that can square human dignity and the use of force against children and vulnerable groups. This requires imaginative legal

[949] I Goldner Lang, "Croatia and EU Asylum Law: Playing on the Sidelines or at the Centre of Events?" In V Stoyanova and E Karageorgiou (eds.), *The New Asylum and Transit Countries in Europe during and in the Aftermath of the 2015/2016 Crisis* (Brill, 2018).

thinking from both the legislator and the fundamental rights agency which has not condemned forced fingerprinting as contrary to fundamental rights. The basic idea is to introduce proportionality to (absolute) fundamental rights. The claim is that there can be a proportionate level of coercion that does not infringe fundamental rights.

Eurodac acknowledges that human dignity and physical integrity must be respected in the process of fingerprinting, which implies that the legislator recognises that human dignity can be affected in this process.[950] Human dignity and the right to physical integrity are absolute rights. Therefore, these cannot be limited by the application of the proportionality principle. Eurodac nevertheless allows for "proportionate" measures which may include coercion.[951] This idea is problematic because it implies that there is a way to use force against all categories of migrants, including those who are vulnerable, while at the same time not infringing their dignity or physical integrity. The very idea of proportionate coercion, which is also a measure of "last resort", is contradictory. This is best exemplified in the approach of Eurodac to the forced fingerprinting of (small) children.

A deeply problematic provision in the Eurodac 2024 Regulation states that no form of force may be used against minors to force them to give biometric data, but when permitted by law, a proportionate degree of coercion may be used, while respecting the human dignity and physical integrity of the minor.[952] Paradoxically, the rule thus states that no force may be used against minors, but that coercion against minors can be used, proportionately. "Minor" is a synonym in Eurodac 2024 which uses it interchangeably with the term "child" on the grounds that "coercion may be used against children" leaves an even worse taste than using the word "minor" in its stead. Eurodac uses the notion of "proportionate coercion" repeatedly in relation to children.[953] This would imply that a small amount of coercion (against a seven-year-old child, for example) does not infringe human dignity, but that disproportionate coercion infringes human dignity. This reasoning in Eurodac introduces, through the back door, a proportionality assessment to the right to human dignity, by activating human dignity only when (un)certain thresholds of coercion are applied to children. The same critique of using proportionality can be seen in relation to the right to physical integrity and proportionality.

[950] Eurodac 2024 Regulation (Regulation (EU) 2024/1358), Article 13(2).
[951] ibid, Article 13(3).
[952] ibid, Article 14(1), fourth paragraph.
[953] ibid, Article 14.

FRA refrains from saying that coercion is directly contrary to the fundamental rights of any category of migrants. This EU agency for fundamental rights states that applying physical force must be done in a proportionate manner[954] and that "excessive" use of force diminishes human dignity, thus amounting to inhuman and degrading treatment prohibited by Article 4 CFR and Article 3 ECHR. The ECtHR's case law on this point provides that the use of force must be proportionate and necessary in the circumstances, thus falling short of prohibiting the use of force in actions relating to determining identity.[955]

In another analysis of the effects of fingerprinting on fundamental rights, FRA raises an original legal argument. FRA imagines a two-tier assessment of the implications on fundamental rights of forced fingerprinting. There is firstly the use of force that amounts to inhuman and degrading treatment and is thus prohibited and cannot be justified. Secondly, the forced fingerprinting of lesser intensity amounts only to an infringement of the right to physical and mental integrity. In this second, less malevolent, case, FRA argues that a necessity and proportionality analysis can be made to determine whether the use of force is justified.[956]

There are two problems with this view. First of all, it is difficult to distinguish between levels of intensity in forcing fingerprints that represent inhuman and degrading treatment from coercive treatment that is merely an infringement of physical and mental integrity. Even more problematic is that FRA distinguishes between two absolute fundamental rights. Both the prohibition of inhuman and degrading treatment and the right to physical integrity are absolute fundamental rights, meaning that any infringement cannot be justified in accordance with Article 52(1) CFR. Therefore, this approach of FRA introduces a proportionality assessment to absolute fundamental rights, which is wrong. But this approach of FRA shows how deeply entrenched is the idea that any fundamental right and any behaviour can be justified with the tools of proportionality. In this sense, proportionality is revealed not as a principle which allows the weighing of private against public interests (or fundamental rights against one

---

[954] FRA, "Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights" (2018) 54.

[955] *Dembele v Switzerland*, App. No. 74010/11 (ECtHR, 17 February 2014) para 41.

[956] "Use of force that does not amount to inhuman or degrading treatment or punishment prohibited by Article 4 of the Charter and Article 3 of the ECHR can still raise fundamental rights concerns, particularly in light of Article 3 of the Charter, which enshrines the right of everyone to respect his or her physical and mental integrity. When force is used to compel a person to do something, the circumstances of each individual case must be assessed to determine whether the use of force was necessary and proportionate and would thus still constitute lawful interference in light of the standards set forth in Article 52 (1) of the Charter."
FRA, "Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac" (2015) 9.

another), but as a tool that allows public authorities, courts, or institutions to justify their conduct. By introducing the idea that the proportionate coercion of any person in the fingerprinting procedure is justified, EU secondary legislation and FRA's interpretive sources change the meaning and scope of (absolute) fundamental rights, by making them subject to an unclear assessment of proportionality.

It should be noted that the question is not whether public authorities can use force at all. They have to be able to use force, as that is the defining characteristic of their authority and the monopoly on coercion that they hold. An organised political entity would not be able to control its territory and provide security to its population without the possibility to use force. The question is, however, whether the use of force in the application of forced fingerprinting, upon vulnerable human beings, can be justified considering its effects on human dignity. Even if such a use of force can be justified, the next question is what the limits are in the use of force. Neither of the questions is adequately answered in the current law and practice of forced fingerprinting.

4.3.4. Conclusion: Human Dignity is Not Properly Utilised but Remains an Important Check on Biometrics.

Human dignity is inviolable and must be respected and protected. Anything that follows this statement should not qualify it so that it becomes completely devoid of meaning. Human dignity was chosen in this thesis as a framework for the analysis of the issue of (forced) fingerprinting because it is undisputed that human dignity belongs to any migrant and is also a value that reveals the true nature of a legal order and of how aligned its values are with its practices. It is clear to anyone who studies biometrics and the obligations it brings that biometrics do not apply equally to all categories of persons. The kings and queens of Britain famously do not need a passport supposedly because it is issued in their name. In a similar manner, there is a biometric hierarchy in EU law so that EU citizens need to provide two fingerprints which are stored only on the document, with no threat of violence if they refuse. However, less privileged groups such as foreigners have to provide more fingerprints (four in the case of the Entry/Exit system (EES)) and these biometric data are stored in remote databases. Those scaling the walls of Fortress Europe uninvited must provide all ten fingerprints, and these fingerprints are stored remotely, for longer, and there are methods of coercion and detention to enforce the biometric law. At the bottom of this biometric hierarchy, in certain respects even intertwined with irregular or illegal migrants, are criminals, whose

fingerprints but also cellular or DNA samples are stored and kept for longer periods of time. The question raised by human dignity is how the use of force against vulnerable people escaping persecution and against children can be justified in terms of human dignity and associated fundamental rights. This differential treatment is more problematic considering the roots of biometrics, which developed from eugenics. Human dignity and related rights such as the right to the integrity of the person were develop precisely to counter the terrible consequences of applying eugenics, an offshoot of which were biometrics.

This part of the thesis has determined that human dignity is a core value of the EU legal order, a right in itself, a foundation for other fundamental rights, and in particular for absolute fundamental rights, which is also a tool the CJEU may use for interpretation. Unfortunately, neither of these many meanings is clearly applied in the sense of what red lines it draws for public authorities using biometrics. This does not have to be so. The wording of the CFR leaves no doubt that human dignity is a right. The problem then lies in interpretation, both by public authorities but also institutions which are reluctant to clearly assert that some behaviours, such as forcing children or people with (hidden) disabilities to provide fingerprints, violate their right to human dignity. Simply put, the right to human dignity should prevent coercion against certain vulnerable groups in the context of collecting biometric data. Names and other biographic data should suffice in their case.

Human dignity is particularly useful for understanding how, and why, biometrics developed and what problems biometrics cause. Although privacy is the most used legal framework to assess biometrics (as the processing of biometric data which infringes privacy, in most cases), privacy does not adequately convey the effects of coercion on human individuals, since coercion does not concern simply revealing information. This is why human dignity is an important concept for understand biometrics as a legal phenomenon.

It could be argued that human dignity being an absolute right is a hindrance to the application of biometrics. Since any infringement of human dignity (and associated absolute rights) is prohibited, it cannot be used at all in the context of biometrics, except as a total ban on certain practices. The author of this thesis disagrees with the notion that there can be a proportionate level of coercion of small children or of people who are unable to understand to process they have submitted to (as well as certain other vulnerable groups). However, the question of the threshold of force is relevant. Any action of public authorities involves a certain level of coercion, or threat, implicit or explicit. That is why positive liberty, or genuinely free choice,

is hard to imagine in the relations between an individual and the State. Nevertheless, coercion applied in the case of fingerprinting raises huge risks of violations of fundamental rights, particularly of vulnerable people. This is undisputed and recognised by the EU legislator and interpretative sources. Since it is impossible to properly distinguish those upon whom force can be applied without diminishing their human dignity from those who are vulnerable to coercion, it becomes clear that human dignity, as the law stands, is infringed on a large scale by Eurodac. This might be seen as an academic argument, since the political reality prevents abandoning compulsory biometrics for the purpose of controlling immigration, but that is beyond the legal scope of this work.

Despite this unfortunate legal and political reality, fundamental rights, and human dignity in particular, remain hugely important for restricting the growing use of biometrics. Much like other modern technologies and technological business concepts, biometrics need to be employed on a large scale to be useful. Every member of a certain group has to be enrolled in order for biometrics to provide accurate identification. While fundamental rights do impose some restriction on the actions of public authorities, there is clear recognition in the legal acts that fundamental rights such as human dignity and the right to physical integrity play a role when it comes to fingerprinting and processing biometric data, even if these are not properly applied. Secondly, the legal concept of human dignity, even if it is currently just an underdeveloped kernel of an idea, has the potential to grow, to be better applied and interpreted and to become a fully fledged framework for limiting violation of the rights of migrants and asylum seekers. There is little doubt that without fundamental rights, the situation would be even more detrimental to migrants and to all other human beings in relation to the biometric power of the State.

4.4. The Right to Non-Discrimination in EU Biometric Law: A Viable Route to Challenge Algorithmic Bias?

4.4.1. Structure of the Section and the Main Arguments

This part of the thesis is a result of the research the author conducted over the past three years of his doctoral studies. Algorithmic bias, particularly in facial recognition, is one of the most prominent topics in legal and more technically oriented academic writing, and one encounters it even earlier than the issue of privacy and biometrics. It is thus interesting that the right to non-discrimination (and the right to equal treatment) has rarely decided cases concerning the use of biometrics. Biometric case law, as was demonstrated in the previous chapter, is decided by using the privacy and data protection legal framework, as far as EU (biometric) law is concerned. This section explores the potential to use the fundamental right to non-discrimination to challenge biometric practices in EU migration. The basic hypothesis of this part is that non-discrimination is not an appropriate framework for addressing problems raised by the use of biometrics.

To make this argument, this section analyses the relation between bias and discrimination, the legal framework for non-discrimination and biometrics in the EU, the case law related to algorithmic bias, the causes of algorithmic bias, and possible solutions. The first argument is that the non-discrimination legal framework is very demanding. The ECHR and EU legal framework for non-discrimination is not appropriate for tackling algorithmic bias due to its demanding requirements, especially in the context of proving discrimination by algorithms.

The second argument is that technology is rapidly progressing so that any proof that certain algorithms exhibit bias against certain groups is soon superseded by changes and improvement in the technology. Thus, legal science always plays “second fiddle” and a catch-up game to technological development. Newer algorithms are without any distinguishable algorithmic bias. However, the claim against algorithmic bias should not be based on a fleeting technological moment.

The third argument holds that algorithmic bias should be measured in relation to the system that was replaced by the algorithms, and that removing algorithmic bias may not be practically feasible. The requirements of fairness and human dignity should lead us to algorithms that are less biased than the human decision-makers they replace, even if they still exhibit algorithmic

bias. After an analysis of these three main arguments, the thesis provides a number of practical recommendations on how to reduce bias in facial recognition systems. A final idea examines whether algorithms can be fair and accurate, or if there has to be a choice between the two.

4.4.2. Understanding Algorithmic and Biometric Bias as Legal Phenomena

Imagine that side by side there are two photographs showing a young person's face. On the left is a student visa applicant, who was enrolled but never commenced their studies. On the right, a photograph on an asylum application shows a person whose request for asylum was granted within a day of the application. However, according to the Canadian public authorities, both photographs are of the same person. This means that the person who applied for a student visa from Kenya, upon arrival in Canada, applied for refugee status, claiming to be from Somalia.[957] In other words, the asylum applicant was lying in their application, and so their refugee status should be rescinded. The authority reached the conclusion that the person was the same by using facial recognition software, which automatically compares databases of student visa applications and those of asylum seekers and other sources to find matches that previously eluded public authorities.[958]

One issue arising from such cases of facial recognition is whether the decision can be made automatically if it has such profound effects on the right of the individual, and particularly since it is difficult to explain how the algorithm arrived at the decision. Another question is simply who is telling the truth: the refugee or the algorithm? This question depends on whether the machine should be trusted, which in turn depends on how accurate or biased the machine is. For human eyes looking at the two photographs, the truth is not clear. However, it does not take a quantum computer to rightly guess that the mentioned photographs depict faces of (a) Black person(s).

The use of facial recognition AI in Canada, by which the refugee status of hundreds of persons was challenged, resulted in at least one judgment. In *Asha Ali Barre*, the judge ruled against the decision to remove the refugee status of a person who was identified by an AI algorithm as

---

[957] T Choi, "Biometrics Use by Canadian Border Agency Increasing. Maybe It Already Has" *BiometricUpdate.com* (January 25, 2022) https://www.biometricupdate.com/202201/biometrics-use-by-canadian-border-agency-increasing-maybe-it-already-has.

[958] Example taken from a string of cases originating in Canada, where more than a hundred refugees were deemed to have lied about their origin after AI tools were used by public authorities to check their claim, often years after asylum was granted. See N Keung, "Are These Two Photos of the Same Person? Canada's Controversy over Asylum-Seekers and 'Photo Matching'" *Toronto Star* (21 January 2022) https://www.thestar.com/news/canada/are-these-two-photos-of-the-same-person-canada-s-controversy-over-asylum-seekers-and/article_2edca377-85ce-57af-9f40-4aff6cda8293.html.

having another, fake identity. The reason the court reached its decision was that the Canadian authority's statement that the photographs were a match lacked a coherent explanation.[959] The court was especially irked by the authority's argument that the two photographs were of the same person because they obviously had a shared ethnic heritage.

4.4.3. Algorithmic Bias in Legislation and Academic Writing

The questions of algorithmic bias, algorithmic discrimination and fairness in relation to these phenomena have steadily grown with the rise of AI and facial recognition in particular. Algorithmic bias and algorithmic fairness are prominent issues in the USA, which is not surprising since it is the birthplace of many associated modern technologies. One legislative initiative from the USA is the US Blueprint for an AI Bill of Rights, which recognised algorithmic discrimination as one of AI's most important legal phenomena. The document, issued during the Biden administration, defined algorithmic discrimination as something that occurs when automated systems contribute to unjustified different treatment or impacts that disfavour people based on their race, colour, ethnicity, sex or any other classification protected by law. The document argued that algorithmic systems should be designed in an "equitable" manner.[960]

In Europe, algorithmic bias is also a prominent topic, either in legislation, case law or in secondary, interpretative sources. The AI Act states that social scoring systems may lead to "discriminatory outcomes" and may violate the right to dignity and non-discrimination, as well as the values of equality and justice.[961] Related to this, public administrations have recently started to use algorithms to assess whether, for example, a person engages in social security fraud. An algorithm may single out a person as possibly committing fraud by considering diverse factors, such as their gender, marital status, income, savings, health status, water consumption, number of children, address and many more factors. An example of such notorious software was System Risico Indicatie (Syri), which was used by the Dutch government to detect potential social benefit fraud. The Hague District Court ruled that Syri violated Article 8 ECHR, which is the right to privacy.[962] It is very telling that the judgment

[959] Canadian Federal Court, *Barre v Canada* 2022 FC 1078.
[960] Biden White House, "Blueprint for an AI Bill of Rights" (2022) https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/.
[961] Regulation (EU) 2024/1689, Recital 31.
[962] Rechtbank Den Haag, *Syri* ECLI:NL:RBDHA:2020:1878.

examined the algorithm in significant detail,[963] considering issues such as deep learning and algorithms, profiling, and transparency, yet the case was decided within the framework of privacy, not non-discrimination. The Court determined that Syri was biased against persons of lower economic status and of immigrant background,[964] but since there was no insight into the algorithm or the statistics, it was hard for the claimant to establish a case of *prima facie* discrimination. In a similar case, an NGO managed to gain insight into how an algorithm used by the Rotterdam municipality detected potential social security fraud, and it was shown that the algorithm associated fraud with factors such as being a financially struggling single mother.[965]

The AI Act furthermore touches upon the issue of (algorithmic) discrimination in relation to the overly sensitive issue of allowing so-called real time remote biometric recognition, which is effectively biometric surveillance. This was discussed previously in section 2.7.5 of the thesis. More directly, the AI Act recognises that AI algorithms used in healthcare may cause discrimination.[966] One of the obligations imposed on high-risk AI systems is data governance, which includes treating data in order to avoid bias.[967] In Article 15(3), the AI Act further attempts to limit bias in so-called feedback loops.

The issue of algorithmic bias may be particularly pertinent in the context of EU migration. Facial recognition is widely used at the level of individual Member States in immigration databases, but Eurodac will soon implement facial images for facial recognition in addition to already existing fingerprint recognition.[968] Thus, potential problems relating to bias in facial recognition with regard to gender or skin colour might become a problem for Eurodac and other EU information systems. Discrimination, or bias, based on religion, may become a problem in view of the fact that a person's head might be completely or partially covered, which could

[963] Though the government refused to provide the inner workings of the algorithm by arguing that it would allow other individuals to avoid being discovered as those committing fraud, which is akin to saying that rules of behaviour will not be made known so that the persons are not able to adjust their behaviour.
[964] Rechtbank Den Haag, *Syri* ECLI:NL:RBDHA:2020:1878, para 6.93.
[965] F Kollias, "Suspicion Machines Methodology" (*Lighthouse Reports*, 6 March 2023) https://www.lighthousereports.com/suspicion-machines-methodology/.
[966] Regulation (EU) 2024/1689, Recital 68.
[967] ibid, Article 10(2)(f).
[968] As mentioned previously in the thesis, for example in 3.3.2.7.

reduce the accuracy of facial recognition algorithms for those persons, thus causing indirect discrimination on the basis of religious beliefs and gender.[969]

There is growing case law from European courts which have at least touched upon the problem of algorithmic discrimination in the specific context of facial recognition. Already discussed in the thesis was the ECtHR's *Glukhin* case, which concerned the use of facial recognition by public authorities to suppress protests.[970] Even more pertinent was the judgment in *R (Bridges) v the Chief Constable of South Wales Police*, where the English domestic court ruled that the use of facial recognition on public streets infringed, again under Article 8 ECHR, the right to respect for private life (privacy).[971] This case discussed the issue of indirect discrimination (by the use of facial recognition) on grounds of sex and race because it produces a higher rate of positive matches for these groups, but the Court did not engage with Article 14 ECHR on the prohibition of discrimination.[972]

EU institutional actors have studied the issue of algorithmic bias and biometrics. For example, the Fundamental Rights Agency (FRA) has discussed AI, bias and fundamental rights.[973] The EDPB has examined facial recognition in law enforcement and the Consultative Committee of Convention 108 has recognised the possibility of facial recognition causing bias or discrimination.[974]

If one explores the roots of the claim that algorithms are biased against certain groups, a number of prominent articles come to the fore. Many academic papers have raised the issue of algorithmic discrimination particularly in relation to gender and biometric recognition. One of the most significant papers on this topic is "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" by Buolamwini and Gebru, which showed that algorithms are most biased against women of dark skin. The paper, however, depends for its conclusion on the state of technology that has since been surpassed.[975] This influential paper

[969] The problem of head covering and human dignity in relation to Eurodac was briefly mentioned in the previous section (4.3.3).
[970] *Glukhin v Russia*, App. no. 11519/20 (ECtHR, 4 July 2023).
[971] *R (Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
[972] ibid, para 52.
[973] FRA, "Data Quality and Artificial Intelligence – Mitigating Bias and Error to Protect Fundamental Rights" (2019).
[974] EDPB, "Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement" (2022) para 27; Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data "Guidelines on Facial Recognition" (2021), 15.
[975] J Buolamwini and T Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81(1) Proceedings of Machine Learning Research. For example, the paper cites NIST

has been cited many times on this main (ideological as well as technological) point. In another example, a paper by Valdivia, Corbera Serrajòrdia and Swianiewicz examines the fairness of biometrics in Eurodac, building on the foundations laid by influential papers such as "Gender Shades". The authors however make an unconvincing case that biometrics are biased. They use the case of an Iraqi migrant who was identified as having previously applied for asylum by Eurodac fingerprint recognition contrary to his statements. The authors lament the fact that the authorities trust the Eurodac fingerprint system over the "narrative" provided by the migrant.[976] Among the most influential papers on algorithmic bias and fairness from mostly a technical perspective is "Big Data's Disparate Impact" by Barocas and Selbst, which stresses that the accuracy of a system depends on the quality of the data input.[977]

4.4.4. Theoretical Framework for Understanding Algorithmic Bias

An algorithm is a clearly specified mathematical process for computation, or a set of rules that, if followed, will give a prescribed result. The word is Arabic in origin, first appearing in ninth-century mathematical writings.[978] In modern terms, one could think of an algorithm as a computer programme.[979] Algorithmic bias is not a term that has a universal definition nor a precise meaning. Bias may mean unfavourable treatment of a certain group of persons. Some refer to algorithmic discrimination instead of algorithmic bias. There are many theoretical frameworks for understanding what causes bias in algorithms, some of which will be used as a basis for discussion here. [980]

Algorithmic bias is caused by three types of problems. The first type is related to the problem of input data. This means that the development of the algorithm did not adequately use data in the programming or machine-learning phase of development. This may be caused by simply using too little data (for example, using too few samples of human faces) or using

reports on facial recognition algorithms which indeed had shown bias against persons of darker skin and females in comparison to males, but this has been reversed in newer testing by NIST.

[976] A Valdivia, JC Serrajòrdia and A Swianiewicz, "There Is an Elephant in the Room: Towards a Critique on the Use of Fairness in Biometrics" (2022) 3 AI and Ethics 1407.

[977] S Barocas and AD Selbst, "Big Data's Disparate Impact" (2016) 104(3) California Law Review, 671–732.

[978] S Russell and P Norvig, *Artificial Intelligence: A Modern Approach, Global Edition* (Pearson Higher Ed, 2021), 27.

[979] FZ Borgesius, "Discrimination, Artificial Intelligence, and Algorithmic Decision-making", Council of Europe, 2018.

[980] P Hacker, "Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law" (2018) 55 Common Market Law Review 1143; S Barocas and AD Selbst, "Big Data's Disparate Impact" (2016) 104(3) California Law Review 671–732; J Kleinberg and others, "Discrimination in The Age of Algorithms" (National Bureau of Economic Research 2019) https://doi.org/10.3386/w25548.

unrepresentative data (using mostly male faces to develop a facial recognition algorithm) or making mistakes in labelling, for example by labelling an object as a bus while it is actually a truck, which leads to the recognition algorithm having the wrong ideas about reality and thus making wrong decisions. All these cases of "bad" data are relatively simple to resolve. Using bigger datasets and having a better representation of data have resolved some of the most notorious problems associated with, for example, facial recognition. Many commentators of algorithmic bias have in mind primarily this kind of mistake that relates to problems with input data. However, not all algorithmic bias can be resolved by improving input data.

The second broad cause of algorithmic bias can be termed historical bias. This type of bias is more subtle are more difficult to rectify. It describes the phenomenon by which an algorithm does not produce inaccurate or biased results because of low quality input data, but because it reproduces the biased practices of humans. For example, an algorithm for assessing CVs for programming jobs may favour male applicants, but not because the input data were wrong, but because the algorithm replicates bias or discrimination that may have existed in past employment practices where male candidates were preferred over female ones. The same applies for an algorithm (such as the notorious COMPAS)[981] which may classify Black persons as having a greater chance of committing crimes. The data that show that Black persons commit crimes are accurate, but this may be caused by a justice system that could be historically biased against such persons. This cause of algorithmic bias is more difficult to resolve. One way to tackle this problem is to introduce positive discrimination (or affirmative action in the US context) by which the algorithm is intentionally biased in favour of a certain historically underrepresented group. Positive discrimination practices, however, raise new problems, especially when they need to be implemented by algorithms. The first issue is how to quantify this advantage (positive discrimination) in precise mathematical terms. Secondly, positive discrimination requires an algorithm to have access to certain protected categories, such as knowing the gender, age, or ethnicity of a person to be able to account for these injustices, which means allowing it to process sensitive personal data.

Therefore, there is often a trade-off which is unacknowledged between accuracy and fairness. Sometimes, algorithms which produce a decision with legal effects cannot be both fair and accurate. For example, an algorithm that decides whether a person is creditworthy can consider

[981] C Engel, L Linhardt and M Schubert, "Code Is Law: How COMPAS Affects the Way the Judiciary Handles the Risk of Recidivism" (2024) Artificial Intelligence and Law.

the race, gender or sex, age of the person, health, or the place where the person lives. This will allow the algorithm to reach a more accurate decision on how likely it is that a person will default on their obligations, thus requiring a higher interest rate on the borrowed money. However, accurate algorithms may perpetuate historical bias against poorer people, who are also more often of a certain ethnicity or race. Thus, to make the algorithm fairer, it is necessary either to hide these protected (sensitive) characteristics or artificially favour certain protected groups (positive discrimination).

If the traits are hidden, however, the algorithm may reconstruct the characteristics by using proxies. The algorithm may come to the conclusion that persons using public transportation are more likely to default on credit than persons using private cars, which may represent indirect discrimination of persons of a certain ethnicity that are more prevalent in city centres than in the suburbs. To avoid this, one solution is to prohibit the use of proxies. However, the downward spiral of prohibiting the algorithm from knowing detailed information leads to the algorithm being less accurate to the point where it is useless. Thus, there is often a choice to be made between making algorithms either fair or accurate.[982] Positive discrimination raises the problem of how much to mathematically favour certain groups; should, for example, descendants of persons that served in the Homeland War be given extra points at university entrance exams (as may be the case in Croatia), but then how many points is the correct level of fairness? Interestingly, the AI Act has taken this debate on accuracy and fairness into account since the AI Act exceptionally allows the processing of sensitive personal data in order to prevent and account for bias.[983]

The third cause of algorithmic bias, which can be called "unequal ground truth" is the most subtle and hardest to eradicate. Unequal ground truth can be described as the situation where an algorithm produces different results for different categories of persons, but not because of either "bad" data or historical discrimination, but rather because of genuine differences between certain groups (this is often not mentioned in legal or other analyses of algorithmic bias due to being politically problematic). One benign hypothetical example would be an algorithm devising car insurance rates for men and women. Such an algorithm would assign men higher rates for car insurance because, on average, men present a higher risk (they generally drive more expensive cars with more powerful engines and engage on average in more risky behaviour).

[982] See also J Kleinberg and others, "Algorithmic Fairness" (2018) 108 AEA Papers and Proceedings, 22.

[983] Regulation (EU) 2024/1689, Article 10(5).

This algorithm would therefore exhibit bias against men. This bias would not be caused by incorrect input data – the fact that men are associated with a higher risk for car insurance companies is true. This algorithmic bias would not be caused by historical bias either – it would be quite implausible to claim that there is historical bias against men in favour of women. This bias would simply be the result of what can be called unequal ground truth, namely that the algorithm exhibits bias that is a correct and fair representation of the facts of the real world.

The question is not only how to resolve this kind of algorithmic bias, but whether it should be resolved at all. EU law prohibits directly discriminating against men in car insurance rates.[984] But the effect of such a measure is problematic since there is evidence that men pay even higher car insurance than before the measure,[985] since the rates are more strongly calculated now by "proxy" attributes, such as the cost of the vehicle or its engine power. More often, it is men that drive such cars, so a case of algorithmic bias may remain in the form of indirect discrimination (though justified in the eyes of EU law) even if direct discrimination is prohibited. The effect is that car insurance rates have risen as a result of this gender-neutral pricing requirement. Therefore, translating fairness, as a construct from the social sciences to natural sciences, is not only difficult, but may cause unintended consequences.

Fingerprint recognition algorithms do not exhibit these kinds of biases. It may be argued that fingerprint recognition may be biased against physical labourers and persons who have defects with their fingerprints, since these categories of persons may have trouble in providing a fingerprint of sufficient quality and thus may be in a worse position than other persons. Facial recognition, on the other hand, may have different accuracy rates for persons of different gender, age, or skin colour. However, this problem with facial recognition is diminishing with better algorithms and in particular with the higher quality of input data. An additional problem in tackling algorithmic bias is how to measure the performance of an algorithm: its "accuracy" or "quality". This was previously discussed in section 1.7.2.6 of the thesis. Another problem, also previously discussed in section 3.4.3 of the thesis, is the fact that what is actually used by the algorithm to conduct facial recognition is not a photograph but a mathematical representation called the biometric template.

[984] Case C-236/09 *Test-Achats* ECLI:EU:C:2011:100) and Council Directive 2004/113/EC.
[985] P Collinson, "How an EU Gender Equality Ruling Widened Inequality" *The Guardian* (14 January 2017) https://www.theguardian.com/money/blog/2017/jan/14/eu-gender-ruling-car-insurance-inequality-worse.

4.4.5. The Three Arguments Against the Use of Non-Discrimination Legal Framework for Tackling Biometrics

When algorithms are discussed in academic papers, discrimination is often taken in the ordinary sense of the word, as self-evident unjust treatment of certain groups of people. It may be said that discrimination, when understood as differentiation, discerning or sorting, is the very nature of every (biometric) algorithm, as well as any human decision-making. But, in the legal sense, discrimination has a nuanced and highly specific meaning, depending on the jurisdiction. Authors discussing algorithmic discrimination from a technological perspective may not have a proper understanding of legal discrimination. One example is a paper discussing ways to reduce discrimination and increase the fairness of algorithms by Kleinberg and others.[986] In this paper, the authors propose a solution for making algorithms fairer, but they do not define what they mean by discrimination which is satisfactory from a legal perspective. The opposite situation may also be true, as when legal scholars (such as the one writing these words) interpret modern technologies in legal terms while lacking the deep technological insights that technical experts have.

There is great value in trying to bridge the gap of understanding as far as possible. The legal perspective is crucial in properly framing questions of bias and policy choices that have to be made in the design and operation of biometric algorithms. The following section represents the reasoning behind three arguments that the non-discrimination legal framework in EU law is not appropriate for restricting the effects of biometrics, in EU migration and asylum law in particular.

4.4.5.1. The Non-discrimination Legal Framework Is Challenging in Relation to Algorithmic Bias

This section will present a short overview of the applicable non-discrimination legal framework. The purpose is to show the difficulties in applying this framework to issues of biometrics and facial recognition.

Discrimination is prohibited in the EU, by primary and secondary legislation, as well as by the ECHR and national legal systems. Article 20 CFR prescribes that everyone is equal before the law. Article 21 lays down that any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other

[986] J Kleinberg and others, "Algorithmic Fairness" (2018) 108 AEA Papers and Proceedings 22.

opinion, membership of a national minority, property, birth, disability, age or sexual orientation is prohibited. Furthermore, within the scope of application of the TFEU and the TEU, discrimination on grounds of nationality is also prohibited.[987] There is a number of secondary legislative acts that prohibit discrimination in more specific circumstances. These include directives (which have to be transposed into national law) on racial equality,[988] on employment,[989] on the basis of gender in regard to goods and services,[990] and on gender equality generally.[991] As a general observation, non-discrimination law lacks an overarching regulation like the GDPR, which means that the non-discrimination legal framework is more complex than data protection law and also that it is more varied than the data protection legal framework.[992]

The ECHR prohibits discrimination in its Article 14 and Article 1 of Protocol No. 12. Article 14 includes the ancillary nature of non-discrimination in the sense that it complements other substantive provisions, while Protocol No. 12 prohibits discrimination in the enjoyment of legal rights.[993] Nevertheless, the application of Article 14 is not dependent on the violation of another substantive provision.[994] There is also discrimination by association, whereby a person is discriminated based on their association with a person of a certain characteristic.[995] Discrimination can be direct or indirect. Direct discrimination concerns a legal difference that is made in treatment which is solely based on a certain identifiable characteristic, such as ethnicity.[996] Indirect discrimination represents a formally neutral practice which has a discriminatory effect on a certain group of people. This practice, law or policy does not have to have an intent to discriminate.[997] EU law understands direct and indirect discrimination in a

[987] Article 21(2) CFR.
[988] Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180/2.
[989] Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L 303/16.
[990] Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services [2004] OJ L 373/37.
[991] Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2006] OJ L 204/23.
[992] For a good overview of data protection law and non-discrimination law in the context of algorithms, AI and modern technologies, see FZ Borgesius, "Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence" (2020) 24 International Journal of Human Rights 1572.
[993] ECtHR, "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention on the Prohibition of Discrimination" (31 August 2024).
[994] ECtHR, "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention on the Prohibition of Discrimination, Updated on 31 August 2024, 6-7.
[995] *Škorjanec v Croatia*, App. no. 25536/14 (ECtHR 28 June 2017).
[996] *Biao v Denmark*, App. no. 38590/10 (ECtHR, 24 May 2016).
[997] *DH and Others v the Czech Republic*, App. no. 57325/00 (ECtHR, 13 November 2007).

similar manner.[998] It is clear that modern technologies, AI, or biometrics are potentially related to indirect discrimination. For example, a biometric recognition system may work less accurately with darker skin colours, which may indirectly discriminate against a certain race or ethnicity.

The ECHR has developed a test for discrimination which consists of a number of steps. The first step is to determine whether there has been a difference in the treatment of persons in similar situations or a failure to treat differently persons who are in different situations.[999] If there is a difference in treatment, the second step of the analysis is to determine whether this treatment pursues a legitimate aim. In other words, this allows the authorities to justify their differential treatment.[1000] One reason for the difference in treatment might be that the government engages in positive discrimination or is using legal inequalities to correct for factual inequalities.[1001]

Objective and reasonable justification consists of having a legitimate aim, such as, for example, national security, and of a proportionality assessment, which means striking a fair balance between the community interest and the rights of the individual. When it comes to the application of modern technologies, such as biometrics, the margin of appreciation afforded to the government in weighing the opposing rights and interests may be wider or narrower, depending on the circumstances.[1002] The possibility to refute discriminatory behaviour by showing an objective justification provides another "chink in the armour" of using indirect discrimination against practices involving algorithmic (biometric) bias. Objective justification means that (in the case of biometrics used for migration and border control) public authorities may provide reasons to justify its use of biometric algorithms that may not treat all persons equally on the basis of their racial origin. For example, using biometrics, even if they do exhibit discrimination against people of darker skin colour, may be justified by reasons of public security, preventing illegal migration, or preventing identity and travel document fraud.

---

[998] FZ Borgesius, "Discrimination, Artificial Intelligence, and Algorithmic Decision-making", Council of Europe – 2018, 19.

[999] ECtHR, "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention Prohibition of Discrimination". Updated on 31 August 2024.

[1000] The right to non-discrimination may also apply in horizontal situations, between private parties.

[1001] *Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium v Belgium* (Merits) App. no. 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64) (ECtHR, 23 July 1968) para 10.

[1002] *S and Marper v UK*, App. no. 30562/04 and 30566/04 (ECtHR, GC, 4 December 2008) para 102.

The burden of proof of showing difference in treatment lies with the applicant, while the burden of proof in proving that the difference is justified rests with the government.[1003] Indirect discrimination is hard to prove, especially since the evidence for difference in treatment of different categories of persons may lie with the perpetrator, that is, the government. This is why the burden of proof on the applicant is eased so that there is only a need to prove *prima facie* discrimination, after which the burden of proof shifts to the government. Nevertheless, it is often difficult, particularly in cases of the use of AI or algorithmic decision-making, to prove, statistically, *prima facie* discrimination.[1004]

This is exemplified by the cases that have already been analysed, such as *Syri*[1005] or *Bridges*,[1006] both before national courts in the Netherlands and the UK, where parties had difficulties in gaining access to how the algorithm actually makes its decision, and to statistics, which may not even exist, which could prove that the algorithm treats different groups in a statistically different manner. For example, the police may not collect statistics on how often a biometric recognition system makes a mistake in identification in relation to different ethnicities. When it comes to opaque algorithms, a person may not be able to gather any coherent evidence on how the algorithm operates and on whether it indirectly affects certain protected groups. There may be no such statistics gathered by public authorities, the algorithm may be protected from inquiry by the law of intellectual property, and finally, deconstructing how an algorithm actually works, even if it does not operate as a "black box", requires technical, personal, and financial capacity.

A rare case which determined the existence of racial bias in an identity check procedure is *Wa Baile v Switzerland,* from 2024.[1007] In this judgment, the ECtHR stated that there was discrimination on racial grounds against a dark-skinned individual who was singled out for an identity check. However, this case involves bias exhibited by human actors, not by algorithms.

In the *Marper* case, the ECtHR decided that the indiscriminate collection and retention of biometric data of individuals is contrary to their right to a private life, but the Court also held that it is not necessary to examine the same complaint under Article 14 ECHR (the right to non-

[1003] *Timishev v Russia*, App. nos. 55762/00 and 55974/00 (ECtHR, 13 December 2005) para 57.

[1004] FZ Borgesius, "Discrimination, Artificial Intelligence, and Algorithmic Decision-making", Council of Europe – 2018, 19.

[1005] Rechtbank Den Haag, *Syri* ECLI:NL:RBDHA:2020:1878.

[1006] *R (Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

[1007] *Wa Baile v Switzerland*, App. nos. 43868/18 and 25883/21 (ECtHR, 20 May 2024).

discrimination). One way of understanding why the Court decided to resolve this case under Article 8 (privacy) and not under Article 14 is to recall that for an infringement of privacy, it is enough to establish that there was a certain biometric technology applied to an individual.[1008] However, to establish *prima facie* discrimination in such a case, there needs to be more elaborate proof that there is an actual difference in treatment between two similar groups.

Huber is an important CJEU judgment which reflects the (similar) framework of non-discrimination in EU law concerning the storing of personal data in national databases.[1009] The judgment also connects data protection law to non-discrimination. In that judgment, the CJEU confirmed that the processing of personal data does not infringe the prohibition of discrimination on grounds of nationality if it is necessary and effective in achieving the goal of the legislation. In cases involving the processing of personal (biometric) data, the data subject may require access to their personal data, as a right under the GDPR.[1010] Individuals also have the right to contest the decision of automated decision-making (ADM).[1011] These may be useful in building an anti-discrimination case, since ADM includes facial recognition decisions, but the rights bestowed by the GDPR in relation to ADM are often limited, as mentioned previously.[1012] The Interoperability Regulations specify that the processing of personal data for the purposes of connecting interoperable EU information systems must not result in discrimination on any protected grounds and must fully respect human dignity, integrity and privacy.[1013] The Interoperability Regulations further require the Commission to assess whether the interoperability components have impacted the right to non-discrimination,[1014] as well as to evaluate the discriminatory effects of the MID component in particular.[1015] This is at least an acknowledgement of the potential of (biometric) information systems to cause discrimination.

This analysis has shown a number of reasons why it would be exceedingly difficult for individuals to use the non-discrimination legal framework to counter biometrics. Another reason for this inequality of arms is the fact that persons who may be discriminated against by the use of biometric algorithms are often TCNs, with few financial resources, and who lack the skills to navigate a complex and foreign legal system. Such persons might be highly reluctant

[1008] See the analysis of case law in 2.8.2.2 and 3.2.1 of the thesis.
[1009] Case C-524/06 *Huber* ECLI:EU:C:2008:724.
[1010] Regulation (EU) 2016/679, Article 15.
[1011] ibid, Article 22(3).
[1012] See 2.3.3 of the thesis.
[1013] Article 5 of Regulation 2019/818 and Regulation 2019/817.
[1014] Article 74(4)(b) of Regulation 2019/818; Article 78(4)(b) of Regulation 2019/817.
[1015] Article 74(6) of Regulation 2019/818; Article 78(6) of Regulation 2019/817.

to make an adversary out of the public authorities from which they seek the right to reside or international protection. Secondly, the lack of case law on biometrics and discrimination, in spite of there being potentially discriminatory elements, shows that biometric law is oriented towards privacy and data protection much more than towards non-discrimination.

4.4.5.2. Facial Recognition Algorithms No Longer Discriminate

This is the second argument in support of the main proposition that the non-discrimination legal framework cannot be effectively used to address problems raised by the use of biometrics. As noted in this chapter, the NIST report of 2015 still concluded that "gender classification is more accurate in males than females".[1016] However, facial recognition algorithms no longer show what could be considered algorithmic bias. The NIST 2020 Face Recognition Vendor Test states in bold terms: "We consider demographics, and note that for the more accurate algorithms, error rates are so low that accuracy variations across sex and race are insignificant".[1017] This testing involves more than a hundred algorithms provided by private developers. NIST (the National Institute of Standards and Technology) is an eminent research institute respected for its independent research. It has conducted a variety of tests of biometric algorithms simulating different circumstances, such as before boarding a plane, checking travel documents, using one-to-one (biometric verification) and one-to-many (biometric identification) tests, as well as accounting for demographics such as race and sex in these reports.

False negatives are caused by poor lighting conditions when taking photographs, which may affect more seriously dark-skinned individuals, but this can be resolved by using algorithms that are more tolerant of poor image quality or by improving lighting and the camera. In other words, bias is not caused by the algorithms (provided that these are among the newer and better performing ones) but by the conditions in which the facial image is acquired. False positives, on the other hand, must be mitigated by algorithm developers, not by improving external conditions.[1018] For example, a more recent NIST report claims that images taken for the purpose

[1016] ML Ngan and P Grother, "Face Recognition Vendor Test (FRVT) – Performance of Automated Gender Classification Algorithms" (*NIST*, April 20, 2015) https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification.
[1017] P Grother and others, "Face Recognition Vendor Test (FRVT) Part 7" (National Institute of Standards and Technology (US) 2021) https://pages.nist.gov/frvt/reports/travel/frvt_travel_report.pdf.
[1018] P Grother, "Face Recognition Vendor Test (FRVT) Part 8" (National Institute of Standards and Technology 2022) https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8429.ipd.pdf.

of visas have no errors except in the case of noticeably young children and a few low-quality greyscale images.[1019]

However, it should be noted that even remarkably high accuracy (false positive or false negative) may translate into a significant number of mistakes when applied to a large group of people. Putting the NIST results and the best algorithm for facial recognition to a hypothetical test still resulted in about thirteen false positives and thirty-three false negatives concerning 25,000 facial images.[1020] EU biometric information systems enrol millions of persons; thus, it remains important to examine their fundamental rights implications.

It can be concluded that if the best available biometric technology is used, there seems to be no significant algorithmic bias. It may nevertheless be necessary to insist that the technology procured by public funds and which affects the fundamental rights of millions must be the best available. This could be done by requiring that the biometric recognition systems used in EU information systems operate technically at the level of the best performing facial recognition algorithms as published by NIST or other reputable sources.

4.4.5.3. The Fairness of an Algorithm Is More Relevant than Algorithmic Bias

This is the third argument in support of the thesis that the non-discrimination legal framework is not adequate to address issues raised by the use of biometrics. Bias is inherent in all decision-making, and it is not a special characteristic of algorithms. Requiring that algorithms be completely unbiased may be impossible, but also unwise if the goal is to reduce bias against migrants. There needs to be a legally determined minimum level of performance that an algorithm must be able to achieve. However, the performance of a biometric algorithm should certainly not exhibit significant bias towards certain protected groups.

The yardstick for assessing algorithmic (biometric) bias should be relative, not absolute. This means that one should examine algorithmic bias in relation to the performance of the system that the algorithm replaced. It may be the case that previous (human) decision-making was even more biased against certain groups of people. This could be hard to prove as well, due to the lack of statistics. Border control and identity control have been conducted for an exceptionally

[1019] ibid, 16.

[1020] M McLaughlin and D Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist", Information Technology and Innovation Foundation | ITIF (January 27, 2020) https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms.

long time, while biometrics have been used only in the last few decades in the sphere of EU migration and asylum law.

The question is, prior to the introduction of fingerprint recognition for Eurodac, what was the level of accuracy and of bias in conducting border and migration control? Modern asylum authorities exhibit bias in their human decision-making, as research has shown.[1021] The asylum system can be likened to a game of roulette because there are many unpredictable human factors, unrelated to the asylum applicant, which may sway decisively the decision.[1022] Fingerprinting and facial recognition did not worsen the situation in terms of bias. Fingerprinting or facial recognition, as far as the right to non-discrimination is concerned, should be permitted if they perform in a less biased manner than the human system alternative. There can also be a policy choice of mandatory human decision-making in certain spheres, even if it is more biased than automated decision-making. But the reasoning behind such a choice would not be discrimination, but for reasons relating to human dignity.

The Court of Justice has already implicitly adopted this relational logic towards biometrics, as can be deduced from *Schwarz*.[1023] To the argument of Mr Schwarz, according to which ascertaining identity by fingerprints is liable to mistakes, the Court held that absolute reliability is not needed. It is enough that the method significantly reduces mistakes or fraud.[1024] The Court rightly stressed that the absolute reliability of biometrics is not a criterion for its suitability, but whether biometrics improve the reliability of establishing identity or the validity of a document in relation to previous methods of identification and validation. The Court centres the biometrics debate on the question of whether the use of biometrics improves the outcome compared to previous methods. In other words, the question is not whether biometrics are accurate, but how accurate biometrics are compared to the alternatives. This argument holds true for biometrics and is applicable in the context of any discrimination associated with (biometric) algorithms.

Fairness remains a key concept that denotes something broader than discrimination and bias, by taking account of the broader societal context. The question may remain about how to measure the fairness of algorithms. One idea is to rely on technical standards. For example, the

[1021] M Emeriau, "Learning to Be Unbiased: Evidence from the French Asylum Office" (2022) 67 American Journal of Political Science 1117.
[1022] J Ramji-Nogales, AI Schoenholtz and PG Schrag, *Refugee Roulette: Disparities in Asylum Adjudication and Proposals for Reform* (NYU Press 2011).
[1023] Case C-291/12 *Schwarz*.
[1024] ibid, para 43.

ISO/IEC 19795-10:2024 standard formulates measures of aggregate equitability, which is a performance measure that combines multiple measures into an aggregate metric of overall differential performance.[1025] Differential performance means the difference in biometric system metrics across different demographic groups.[1026] One solution is thus to rely on or to consider these legitimate attempts to mathematically express the fairness of biometric algorithms.

There is also another neglected aspect of the fairness of biometrics that should be raised. Hypothetically speaking, one could imagine the following situation. Algorithm A, which is 99.98% accurate, but when it does make mistakes, it always concerns Black persons. Algorithm B, which is 99.96% accurate, but makes mistakes more equally across demographic groups. If public authorities adopt algorithm A, this improves overall accuracy, but there is a strong claim that such an algorithm is discriminatory, because it disproportionately makes mistakes with Black faces. One could express the two algorithms as having higher overall or specific accuracy. If one opts for algorithm B, however, there are more mistakes, with Black faces as well as other faces, but there is no bias against persons of darker skin. Thus, a fairness measure is needed to convey the idea that an algorithm can be fairer even if it is less accurate. There is a need to make a policy choice framed by a discussion on the concept of fairness.

4.4.6. Conclusion: How to Counter Algorithmic Bias

This analysis has shown that the non-discrimination legal framework is not suitable for challenging biometric practices in the sphere of EU migration and asylum law. This is for three reasons. The first reason is the lack of transparency of algorithms and the lack of statistics, coupled with the demanding legal framework for proving discrimination. The second reason is that facial recognition algorithms are rapidly improving, so that any claim about their bias soon becomes obsolete and no longer holds true. Thirdly, the approach of using the right to non-discrimination might not be appropriate on the grounds that biometrics might not be more discriminatory than the practices of human decision-making they replaced. It is important to determine a fair outcome and then strive to regulate algorithms in line with that conception of fairness.

[1025] ISO/IEC 19795-10:2024(en) Information technology — Biometric performance testing and reporting Part 10: Quantifying biometric system performance variation across demographic groups.

[1026] ISO/IEC 19795-10:2024(en) 3.1.

This analysis makes it clear that biometric algorithms should not be given free reign upon the migrant population in the EU. There are strong grounds for claiming that biometrics infringe the fundamental rights to privacy and data protection, depending, as was examined in the previous chapters, on a number of factors that make up a biometric system. Furthermore, it has been shown that the right to human dignity should be understood as precluding the use of certain biometric practices, in particular the use of coercion to collect fingerprints against vulnerable people and against children in particular.

However, there are practical recommendations that can be made in relation to addressing algorithmic bias or keeping it to a minimum in biometric recognition systems. First, algorithms need to be trained on high quality data: large and representative samples. This should be clearly stipulated by legal requirements. Secondly, algorithms differ in their performance. State-of-the-art algorithms must always be used. Adherence to strict technical standards and with references to relevant institutions which test biometric algorithms should also be stipulated as a legal requirement. The level of performance should not be lower than what the best solutions can provide. The EU migration and asylum system should not be the testing grounds for new technological solutions or a place where obsolete software or hardware systems are procured. In the application of algorithms, the applicable human rights and fundamental rights law must be upheld, along with the data protection legal framework. There should also be a reasonable approach to biometrics, by using solutions that improve the lives of individuals (and exhibit less bias). Finally, this analysis has stressed that there is a trade-off between fairness and accuracy. In some cases, algorithms cannot achieve both simultaneously. Defining fairness becomes a crucial policy and legal question. Biometric algorithms are merely tools, like books or computers, and it is up to humans to give them moral and legal content.

4.5. Conclusion to Chapter 4.

The main findings following the analysis presented in this chapter are listed here. First, privacy and data protection are the most important fundamental rights for examining the use of biometrics, both in general settings and in migration in particular. However, the way that CJEU applies the fundamental rights analysis is not consistent, as this analysis has pointed out. In the second part, the analysis shows that the right to human dignity could be raised as a barrier to the forced fingerprinting of children and certain other groups of people, but the right to human dignity is currently dormant and not seen as a right, but more as an unenforced value. Finally, the third part of this chapter indicates that there are great difficulties in using non-discrimination

as a fundamental right to restrict the use of biometrics. Nevertheless, discussion of the effects of facial recognition in terms of discrimination, bias and fairness is, as has been shown, of great importance in developing a legal framework for biometrics.

In conclusion, this chapter has provided an answer to one of the important research questions on the effects of biometrics on fundamental rights, particularly in migration and asylum. With this knowledge, it is time to examine the main research question, namely whether and how privacy enhancing tools can be used to minimise the determined negative effects of biometrics on fundamental rights, particularly of migrants and asylum seekers.

Chapter 5: Can Privacy Enhancing Tools Reduce the Limitations of Fundamental Rights Caused by the Use of Biometric Technologies in EU Migration and Asylum?

5.1. Answering the Main Research Question: The Path Taken and the Light at the End

The main hypothesis of this thesis is that privacy enhancing tools, and encryption in particular, can to a large degree mitigate the negative effects of biometric data processing on fundamental rights of migrants and asylum seekers. To explore this hypothesis, several subsidiary research questions were addressed. The first was to discover the rules applying to the processing of biometric data, including the systematisation of EU biometric law and the analysis of the case law. The next important research question concerned the legal nature of the biometric template in the sBMS. The answer was that the biometric template indeed represents biometric data in the meaning of EU law. The third research question investigated the effects of biometrics on fundamental rights. The findings revealed that a number of fundamental rights are affected by the use of biometric technology, most notably privacy and data protection rights. The final research question collates these previous subsidiary questions by examining the effects of the encryption of the biometric template on the privacy and data protection rights of migrants. This chapter will focus on privacy enhancing tools, and on encryption in particular. The main hypothesis is that encryption, along with other privacy enhancing tools, can greatly improve the fundamental rights of migrants in the context of the use of biometric technologies.

The first part of this chapter will explain and critically analyse the existing legal framework for the use of encryption in EU biometric law. This will be followed by a discussion on whether the current legal framework supports the conclusion that there is a right to have one's personal data encrypted, or conversely, whether public authorities might hold the right always to decrypt personal data. The next part of the chapter will analyse the legal effects of encryption by studying the concepts of pseudonymisation, anonymisation, revocability and irreversibility. Two of the most prominent methods of encryption will be studied for their legal effects in light of these four concepts. Finally, the chapter will conclude by answering the main hypothesis with a number of recommendations on how to apply encryption as a privacy enhancing tool in the context of EU biometric law.

5.2. Remarks on the Scope of Investigation of Encryption and Three Examples on Benefits of Encryption

It should be noted that encryption is just one among many privacy enhancing tools. Encryption could also be viewed as one of the methods for cybersecurity.[1027] Cybersecurity is evolving from the right to privacy and data protection to being regarded as a separate right, with the growing recognition of this concept by the CJEU and ECtHR.[1028] In a broader sense, privacy enhancing tools do not need to concern technical solutions. Privacy could be enhanced in the context of the processing of biometric data by a change in the Court's interpretation of this processing, as has already been analysed in this thesis.[1029] Other ways to enhance privacy and data protection would be to more strictly regulate certain parameters that represent a biometric system, such as by lowering the required number of fingerprints processed for the purpose of Eurodac or to require the local storage of biometric data instead of storage in a database.[1030] Furthermore, the privacy and data protection of migrants and asylum seekers would benefit from changes to the legislation, for example with a clearer position on the definition and scope of biometric data,[1031] or a more restrictive policy to AI biometric systems used in migration and asylum, as well as to biometric practices covered in the AI Act which are only superficially prohibited,[1032] to mention just a few points already analysed in this thesis.

This discussion of privacy enhancing tools is primarily concerned with the effects on fundamental rights of privacy and data protection. However, encryption should not be considered to alter the negative effects of biometric technologies on other fundamental rights, such as human dignity and non-discrimination, as well as on other fundamental rights that have not been assessed in the light of biometrics in greater detail in this thesis. Admittedly, this will not be an exhaustive analysis of the technical aspects of encryption. The goal is to clearly examine the untapped potential of encryption as a legal tool for increasing privacy and data

[1027] See, for example, Recital 98 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) PE/32/2022/REV/2 [2022] OJ L 333/80, which states that cybersecurity methods include encryption, particularly end-to-end encryption.

[1028] See PG Chiara, "Towards a Right to Cybersecurity in EU law? The Challenges Ahead" (2024) 53 Computer Law & Security Review; D Duić and T Petrašević, "Data Protection and Cybersecurity: Case-Law of Two European Courts", EU and Comparative Law Issues and Challenges series (Faculty of Law, Josip Juraj Strossmayer University of Osijek 2023)

[1029] See 3.2 and 4.2.3 of this thesis.

[1030] On biometric parameters, which determine the level of limitation of privacy and data protection, see 3.3.2.

[1031] See 2.4.6 of this thesis.

[1032] See 2.7 of this thesis.

protection in biometric data processing. Bearing all these restrictions on the scope of the main research question in mind, there is still significant benefit that can be gained from using encryption in biometric data processing.

Three short examples may illustrate that importance of the encryption of biometric data. After the American military left Afghanistan some years ago, the Taliban seized biometric devices which still contained iris and fingerprint scans as well as biographical information of numerous Afghans. The Taliban used these biometric data to persecute those who assisted the US, such as translators, judges, civil servants, and women.[1033] The accuracy of the biometric technologies and the size of the biometric databases facilitated the persecution of victims by the Taliban regime. If the biometric data had been encrypted, the tragic application of biometrics as a tool of persecution would have been avoided.

The second example concerns Rohingya refugees, and another great injustice facilitated by the use of biometric technologies. The UN High Commissioner for Refugees (UNHCR) had registered hundreds of thousands of Rohingya refugees, including the processing of their biometric data. In an unfortunate chain of events, UNHCR shared the biometric and other data of refugees with the Myanmar government, from whose persecution the Rohingya were fleeing.[1034] The mistake was compounded by the use of biometric technologies, which revealed more information about the refugees than would have been revealed by biographic data alone.

The third example shows the importance of the revocability of biometric data and the use of biometric technologies that has a chilling effect on civil rights. The Pakistani government threatened to block the biometric identity documents of individuals who expressed a certain political opinion. This would prevent individuals from accessing their bank accounts or from travelling abroad, since the biometric data were not revocable.[1035] These examples illustrate the importance of the proper collection, storage and rules for accessing biometric data. They also show the value of encryption. Encryption does not necessarily contribute to greater effectiveness of processing but should be viewed as a limitation of the negative effects of such processing.

[1033] "New Evidence That Biometric Data Systems Imperil Afghans" (*Human Rights Watch*, 30 March 2022) https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans.
[1034] "UN Shared Rohingya Data Without Informed Consent" (*Human Rights Watch*, 15 June 2021) https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent.
[1035] F Hersey, "Pakistani Political 'Hecklers' Threatened with Blocked Biometric ID, Bank Accounts" *BiometricUpdate.com* (22 August 2022) https://www.biometricupdate.com/202208/pakistani-political-hecklers-threatened-with-blocked-biometric-id-bank-accounts.

5.3. The Legal Framework for the Encryption of Biometric Data and Privacy Enhancing Tools

There are several provisions in EU law concerning encryption which, taken together, could be interpreted as representing an obligation to encrypt biometric data and provide other privacy enhancing tools. In addition, it can be argued that fundamental rights to privacy and data protection themselves imply an obligation to encrypt biometric data. In order for the processing of biometric data to be a justified limitation of fundamental rights, it has to be suitable, necessary and proportionate, in accordance with Article 52(1) CFR. If an encryption method is viable and limits the diminishing of privacy, it thus becomes necessary to use it, under the proportionality test of Article 52(1) CFR. Data protection in the EU legal order, besides being a fundamental right, is based on Article 16 TFEU which extends the right to data protection to everyone.

The obligation to encrypt therefore changes with the availability of technical methods for the protection of biometric data. Just as an old photograph may become biometric data as it becomes possible to conduct biometric recognition with better technology, so does the obligation to encrypt change as it becomes possible to apply encryption.

Article 25 GDPR defines data protection by design and default.[1036] This provision requires the data controller to implement appropriate technical and organisational measures, by considering the state-of-the-art, the costs, the scope and purpose of the system in question and other factors. This Article does not lay down any definite requirements for privacy enhancing tools, and in this sense it may be seen to be inadequate. Its strength, however, is in its flexibility, by not focusing on any particular technical method but instead requiring the use of the best available method(s) for protecting biometric data. Its effectiveness is thus dependent on interpretation and application. The national courts, national data protection bodies and public authorities themselves must understand the latest available technical methods for protecting and encrypting biometric data in order to be able to apply such provisions.

Among the principles of EU data protection is the principle of integrity and confidentiality of personal data. This includes taking into account available technical methods, pseudonymisation

[1036] The theoretical background of this provision was previously discussed in 2.3.4 of the thesis. The LED contains a corresponding provision in Article 20.

and encryption of personal data.[1037] In this regard, the principle of integrity and confidentiality represents an obligation to encrypt personal data, depending on the circumstances.[1038] Concerning the security of processing, EU data protection law requires that the level of security corresponds to the circumstances of processing and the level of risk for fundamental rights.[1039] These technical and administrative measures include "the pseudonymisation and encryption of personal data" as if the legislators correctly anticipated the close relationship between these concepts by not distinguishing between them as measures for increased security of data processing.

The specific technical tools which need to be implemented according to Article 25 GDPR do not have to be explicitly specified in order to be considered mandatory. Recently, the Croatian data protection authority (AZOP) issued a penalty against a public hospital that had failed to fulfil the obligations of Article 32 GDPR, in particular by not keeping effectively separate logging accounts of hospital staff (to make it possible to determine who had logged into the system and at what point) and, *inter alia*, by not properly securing the personal data of the records of hospital patients by means of encrypted storage or by using methods to implement redundant backups to protect against data theft or data corruption.[1040] These problems were revealed after a significant security breach. A parallel of sorts can be drawn with the ECtHR's case law and with Article 8 ECHR. In *I v Finland*, the ECtHR ruled that there had been a violation of the right to privacy of a hospital employee because there was no logging system in place to effectively show whether other employees had accessed this employee's health data.[1041]

In addition to EU law, national laws of Member States determine the obligations in relation to data protection and encryption of personal data. Croatian law on the processing of biometric data requires that the security of personal data must be ensured by technical measures.[1042] Responsible bodies must use also adequate technical and organisational methods to ensure the security of biometric data, having in mind the latest technical developments, the scope, content and purpose of processing, and the risk for the rights and freedoms of physical persons.[1043] In

---

[1037] FRA, *Handbook on European Data Protection Law - 2018 edition*, 3.6.

[1038] ibid, 4.2.2.

[1039] Regulation 2016/679, Article 32(1)(g).

[1040] Interview with AZOP representative Anamarija Mladinić. See also: https://azop.hr/sedam-novih-upravnih-novcanih-kazni-u-iznosu-od-169-000-eura/.

[1041] *I v Finland*, App. no. 20511/03 (ECtHR, 17 October 2008).

[1042] Article 5(3), Articles 20-22 Zakon o obradi biometrijskih podataka NN 127/19 (Croatian Act on the Processing of Biometric Data).

[1043] ibid, Article 22(1).

relation to the automated processing of biometric data, Croatian law lists ten general administrative and technical measures required for such systems. These include preventing unauthorised reading, copying, changing or deleting data; ensuring that the system can be started again in the case of a break down; and ensuring the reporting of errors and preventing the loss of the integrity of biometric data due to system deficiencies.[1044]

Regulations concerning interoperability and Eurodac in particular also touch upon the issue of encryption. Interoperability regulations report that eu-LISA achieves the security of processing of personal data in particular by appropriate encryption techniques.[1045] It is a duty of Member States to ensure compliance with the rules of EU information systems regarding the security and integrity of personal data.[1046] Article 35 of the new 2024 Eurodac Regulation prescribes that the transmission of all communication between authorities must be secure. Different aspects of the security of personal data collected for the Eurodac system are the responsibility of the Member State (of origin) and eu-LISA.[1047] Regarding in particular encryption, the 2024 Eurodac Regulation lays down that the communication infrastructure between the Central System and Member States must be encrypted,[1048] and that all processed personal data should be encrypted by appropriate encryption methods during transmission.[1049] The specific meaning of encryption is, however, not defined in the regulation.

5.4. A Right to Encryption or an Obligation to Decrypt?

Recent developments in EU and ECHR law reflect a dilemma between protection of the privacy of individuals and security of the state, at the heart of which is encryption. Encryption surely contributes to the protection of fundamental rights, but this may come at the expense of the public authorities' efficiency in dealing with security concerns.

The dilemma between fundamental rights and security is particularly highlighted by the notion that if there remains a way (a backdoor) for public authorities to decrypt any personal data, such as communications, then this backdoor requires that all personal data be encrypted with a calculated weakness which can be exploited by public authorities. However, encryption could

[1044] ibid, Article 22(2).
[1045] Regulation 2019/818 and Regulation 2019/817, Article 42(3)(j).
[1046] ibid, Article 56(1)(h).
[1047] Eurodac 2024, Article 36.
[1048] Regulation (EU) 2024/1358, Article 3(1)(b).
[1049] ibid, Article 48(2)(k).

become so efficient as to prevent public authorities from ever being able to listen in to private communication, or to process personal data more generally.

In 2016 ENISA and Europol had already issued a joint statement expressing the position that mandatory backdoors, which would give law enforcement authorities access to encrypted data, should not be used since they also increase the risk of abuse.[1050] The issue of encryption of personal data and whether there should be backdoor access is highly disputed. In 2022, the EDPB and EDPS issued a joint opinion against the use of any kind of backdoor for end-to-end encryption, even in the context of a regulation for the prevention of child abuse.[1051] End-to-end encryption ensures that the provider of the communication does not have access to the textual messages, since only the private parties that are communicating via the application hold the encryption key which enables them to communicate.[1052]

The position of key EU stakeholders seems to have shifted to the opposite position of requiring mandatory backdoor access. The Niinistö report on strengthening the EU's security is circumspect in relation to encryption. It calls for a robust legal framework to enable access to encrypted data while respecting fundamental rights, adding that (most) "communications are now end-to-end encrypted, so that even if telecommunications providers cooperate with law enforcement authorities, data provided would not be useful".[1053] This report therefore does not seem to take a clear position on whether there should always be a way for public authorities to access any (encrypted) personal data.

The Draghi report, which looks at how to make the EU more economically competitive, highlights encryption as an area of digital technology where the EU economy could have an opportunity to innovate in order to assert its "technological sovereignty".[1054] It is implied in the report that relying on American providers for encryption could leave the EU exposed to security risks.[1055] Further, the EU Commission recently announced a strategy called ProtectEU which

[1050] Europol and ENISA Joint Statement, "On Lawful Criminal Investigation that Respects 21st Century Data Protection" (2016) https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century...%20%281%29.pdf.
[1051] EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022), para 97.
[1052] ibid.
[1053] S Niinistö, Report for the EU Commission "Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness", 115, https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf.
[1054] M Draghi, Report for the EU Commission, "The Future of European Competitiveness (Part A) (2024) 24.
[1055] ibid, 34.

would enable lawful and effective access to data for law enforcement authorities.[1056] In particular, this includes a "Technology roadmap for encryption" which would ensure technological solutions so that law enforcement authorities have access to encrypted data.[1057] In other words, the EU wants to have tools at its disposal to ensure it has access to private communications and other personal data, even if such data are end-to-end encrypted. The NIS2 Directive is ambiguous towards end-to-end encryption and backdoor access, saying that these should be "reconciled" with the essential security and law enforcement interests of Member States. At the same time, end-to-end encryption should remain as a "critical technology for the effective protection of data and privacy".[1058]

With this political and legal background, the *Podchasov* judgment, reached before the ECtHR, holds important lessons regarding the possible right to encryption of personal data.[1059] *Podchasov* strictly limited the possibility of a backdoor for public authorities, but did not categorically prohibit it. The case illustrates the importance of encryption from the perspective of both the individual and the public authorities and shows how encryption is a phenomenon framed within the right to privacy under Article 8 ECHR. Encryption of biometric data can similarly prevent public authorities from decrypting biometric data. Therefore, the encryption debate concerning backdoor access and *Podchasov* is important for the final research question of this thesis.

5.5. Podchasov: The Facts, the Decision, and the Consequences for Encryption.

This case concerned an application used for communication named Telegram. A Russian law required that the data communicated through messaging apps be retained for a certain period so that the government could access it if necessary. This in turn would require the app to change its encryption method for everyone, because its end-to-end encryption did not allow for reading and storing private communication. The law thus required public authorities to have backdoor access. Russian police suspected certain persons of terrorist activity and required the decryption of their accounts on Telegram. Telegram argued that it technically could not comply only in

[1056] EU Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protecteu: A European Internal Security Strategy" com(2025) 148 final.
[1057] ibid.
[1058] Directive 2022/2555, Recital 98.
[1059] *Podchasov v Russia*, App. no. 33696/19 (ECtHR, 13 May 2024).

relation to these parties. As a result of the failure to comply, Telegram was blocked in Russia.[1060]

Telegram claimed that it could only comply with the order by creating a backdoor to communications of all users. This would allow the Russian government to decrypt all communications on Telegram indiscriminately. Telegram would have to store private keys which would mean the end of encryption. Telegram argued that the law leaves the government a broad scope of discretion in choosing whether to use the decryption keys on a person's communication and that would breach the right to privacy of the users. It should be added that it is likely that Telegram had a clear business motivation to oppose the request, since it is likely that nobody would want to use a communication app where the Russian government could spy on their communication.

The problem is that a backdoor must effectively decrypt all personal data, not merely the personal data of targeted persons. The qualities and the guarantees of the law which requires backdoor access are then not as important, because the technical nature of encryption does not allow for a *post hoc*, case-by-case analysis of whether the decryption is justified. Either there is end-to-end encryption, in which case all communications are private, or there is access of public authorities to all communications. The middle approach of satisfying both the privacy of individuals and the security cravings of the public authorities is not technically possible. If the personal data are not encrypted, it is up to the good intentions of the public authorities that they do not spy more than is necessary, but the authorities are given a key which can decrypt any electronic communication. Requiring backdoor access lies on the presumption that men are governed by angels.

The Strasbourg Court analysed the qualities of the Russian law through the lens of the Article 8 ECHR requirements. The Court noted that it had already analysed similar circumstances in *Zakharov v Russia*, where it established that the same law allowed the government generalised access without sufficient safeguards, and thus impaired the very essence of privacy.[1061] The mention of essence evokes the similar language used by the CJEU in the *Schrems 1* judgment (which *Podchasov* judgment mentions), a rare example where the CJEU found a limitation of

[1060] *Podchasov v Russia*, App. no. 33696/19 (ECtHR, 13 May 2024) para 8.

[1061] ibid, paras 55, 80.

the essence of the right to privacy, caused by generalised access to communications enjoyed by public authorities.[1062]

The *Podchasov* judgment refers to a number of important cases, such as *S and Marper*, *Big Brother Watch*,[1063] and *Gaughran* to establish that protection of personal data is fundamental to the right to privacy and that domestic law must have appropriate safeguards, especially when it concerns automated data processing, sophisticated technologies, bulk interception of communications and secret surveillance.[1064]

The condition for interference with the right to privacy is that it is in accordance with the law, pursues one or more of the legitimate aims listed in Article 8(2) ECHR, and that is necessary in a democratic society in order to achieve any such aim. The ECtHR decided that the Russian law is contrary to Article 8 based on an examination of the first criterion, in other words, the qualities of the law in question were not sufficient. Among other reasons, retention of data must be proportionate to the purpose and there must be limits on storage periods. The Court understood the dilemma presented by the backdoor to encrypted personal data and held that in order to enable decryption of some communications, it would be necessary to weaken the encryption of all users. This means that the measure cannot be limited to specific individuals. Backdoors would enable "routine, general and indiscriminate surveillance" of electronic communications.[1065] Based on this reasoning, the Court considered that an obligation to decrypt end-to-end communication is not proportionate to the legitimate interest pursued.[1066]

The Court's decision seems to imply that weakening encryption by the backdoor is contrary to the right to privacy, but it does not state this in a wholly unequivocal manner. There may be space for a measure which would weaken encryption of personal data if the measure were applied in a manner satisfactory to the ECtHR. The paradox is that mass surveillance may only be legal in circumstances necessary in a democratic society, as Article 8 ECHR requires for interference with privacy.

The analysis of EU legislation has shown that it could be argued that EU law contains a right to encryption, because it may be necessary to encrypt personal and biometric data in order to

[1062] Case C-362/14 *Schrems I* ECLI:EU:C: 2015:650, para 94.
[1063] *Big Brother Watch and Others v UK*, App. nos. 58170/13, 62322/14 and 24960/15 (ECtHR, GC, 25 May 2021).
[1064] Podchasov v Russia, App. no. 33696/19 (ECtHR, 13 May 2024) para 62.
[1065] ibid, para 77.
[1066] ibid, para 79.

satisfy the proportionality requirement when processing personal data. However, a legal requirement to leave open the possibility for the government to decrypt personal data may likewise not be categorically contrary to the human right to privacy, depending on the specific circumstances, as shown by the case law of the ECtHR. This conclusion is relevant for the following discussion. Some encryption methods may prevent public authorities from having the possibility to process biometric data in any manner other than for the purpose of biometric recognition. What is more, encryption may make the data anonymous, in which case privacy and data protection do not even apply. The question in this hypothetical case is twofold: should public authorities always have a backdoor (a right to decrypt), and second, what is the legal framework applicable if biometric recognition does not entail the processing of any biometric data? These questions will in large part be left open.

An important insight is that this analysis of encryption holds a valuable lesson for privacy advocates. Courts, legislators and other stakeholders seem to be more inclined to consider arguments in favour of privacy if the debate is centred on the issue of encryption, rather than on the privacy effects of processing biometric data. The processing of biometric data impresses upon the Luxembourg Court an image of the infringement of privacy and data protection, since it has consistently considered fingerprinting not to be of a particularly intimate nature, nor causing discomfort.[1067] Approaching the issue of biometrics from the perspective of encryption, particularly if the threat emanates from Russia or the US (as in the ECtHR's *Podchasov* case and the CJEU's *Schrems*), may bring better results for fundamental rights protection of individuals and migrants and a better reception at the Court.

One author commented that *Podchasov* raises the prospect of a European right to end-to-end encryption.[1068] The right to encryption would not be a surprising development, considering the number of rights that have been established under privacy and data protection, such as the right to rectification, or the right not to be subject to automated decision making. It could also be argued the other way around, that encryption should not be too strong as public authorities may always reserve the right to decrypt personal data, of course, in the narrowest and most extraordinary circumstances.

[1067] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670, para 48.

[1068] J Shurson, "A European Right to End-to-End Encryption?" (2024) Computer Law & Security Review, 55, 106063 2024 doi.org/10.1016/j.clsr.2024.106063.

5.6. The Quest for the Holy Grail: Legal Effects and Methods of Encryption.

Biometric characteristics, such as a face or a fingerprint, are not secrets.[1069] This is the specific problem of biometrics, because a person could have their fingerprint or face scanned without their knowledge. If a biometric system processes as biometric data the "raw" images, a fingerprint or a facial image collected in such a manner could be used for biometric recognition without the knowledge of the person. Furthermore, if the biometric data are not revocable, a person would not be able to get a new biometric identity instead of the one which was compromised. These special characteristics of biometric recognition are the reason that encryption is of such importance. Encryption can be understood as a broad array of methods that reduce the amount of information that can be revealed. Encryption is applied to biometric data, more precisely to the biometric template. This is why the area of applying security methods to biometric technologies is often referred to as biometric template protection (BTP).

Technologies can broadly affect the identification of persons in two ways. One is to make natural persons more easily identifiable. This is the purpose of biometric technologies. There are also emerging technologies that allow for enhancing privacy and data protection, such as methods encrypting biometric data. Since technologies are improving in both of these ways that affect privacy, anyone who applies biometric technologies must be constantly updating their practices not only by making them more efficient in the identification of persons, but also by applying better privacy enhancing technologies as these become available. In this thesis, encryption will be understood by the framework of the following terms: pseudonymity, anonymity, revocability, and irreversibility.

5.6.1. Pseudonymisation and Anonymisation of Biometric Data

Pseudonymisation and anonymisation are important legal concepts for understanding the effectiveness of privacy enhancing tools. Pseudonymised personal data can be attributed to a natural person, but only with the use of additional information, and considering all the means reasonably likely to be used to identify a natural person. A person is identifiable, according to the same Recital 26 of the GDPR, by considering objective factors such as cost, the time required for identification, and the available technology at the time of processing as well as technological developments. These seemingly simple aspects have profound implications. First of all, the borderline between pseudonymous and other personal data is not fixed. It depends on

[1069] B Schneier, "Inside Risks: The Uses and Abuses of Biometrics" (1999) 42 Communications of the ACM 136.

the interpretation of the means that are reasonably likely to be used to make the identification. Secondly, the meaning of pseudonymisation of biometric data may change with the development of new technologies that allow for the deciphering of previously cryptic information.

Pseudonymisation contributes to a higher level of data security. For example, if biometric data stored in Eurodac are encrypted, it means that a key, which is additional information, is required to decrypt the data. Pseudonymisation involves separating personal information into two parts, both of which are needed to understand the personal data. In other words, the meaning of pseudonymisation in EU law corresponds to the meaning of encryption: it is about separating one piece of information into two pieces. The point is to keep the key and the rest of the personal data separate, so that a malicious action would not acquire both. Importantly, both the key and the rest of information are considered personal data in EU law.[1070] The EDPS concluded that biometric data in the form of encrypted biometric templates are pseudonymised.[1071] As early as 2011, the EDPS, when reviewing an EU project that concerned protection of biometric data, concluded that encryption in essence represents pseudonymisation methods for biometric templates.

Encryption may represent more than just pseudonymisation. It can lead to the anonymisation of data. It can also make biometric data revocable and irreversible. These effects may not only be beneficial in the potential case of a malicious attack of a third party on the biometric data but may preserve to a greater degree the privacy and data protection rights of individuals in their relation to public authorities. Personal data should be encrypted in such a manner that public authorities cannot know anything more than is necessary for the purpose of a biometric system. If the purpose of a system is to verify identity, there is no need for the accessing public authorities to discern the actual facial image of a person, or other personal data.

Personal data which are pseudonymised are still personal data, unlike anonymised data which can no longer be used to identify any individual. Anonymous information is that which does not relate to an identifiable natural person, and therefore the GDPR and other data protection laws of the EU do not apply to such information.[1072] For natural persons, the processing of

[1070] EDPS, "Guidelines 01/2025 on Pseudonymisation" (2025) para 86.
[1071] EDPS, "Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)" (2011).
[1072] Regulation (EU) 2016/679, Recital 26.

anonymous data would mean that their privacy is not affected in the slightest. From the perspective of data processors and controllers, processing anonymous information would mean that there are no obligations arising from the privacy and data protection legal framework. Therefore, an encryption method which would allow biometric recognition using anonymous data would hold benefits both for individuals and the public authorities. A potential problem would be whether such biometric recognition using anonymous data could or should be regulated under any legal framework. Thus, the possibility of using biometric data which would be anonymised would represent a sort of holy grail, at least as far as privacy and data protection are concerned, by allowing the purpose of biometric identification to be achieved but without using any personal or biometric data in the sense of EU law.

There are existing norms which can be interpreted as already containing the obligation to encrypt biometric data. It is the general responsibility of the controller to implement appropriate technical and organisation measures for processing personal data.[1073] The data controller must implement appropriate technical measures, among which the GDPR specifically mentions pseudonymisation, while taking into account the risk for fundamental rights and the technological state of the art.[1074] This further requires the controller to use the technical measures necessary for the specific purpose of processing, relating to the amount of data processed, as well as storage and accessibility.[1075]

5.6.2. Irreversibility and Revocability: An Eye for an Eye

Besides pseudonymisation and anonymisation, which are defined in the EU data protection law, two further concepts that capture the benefits of encryption are the irreversibility and revocability of biometric data.

Irreversibility means that it is not possible to revert biometric data to reveal the biometric sample.[1076] In simple terms, biometric data are encrypted so that it is not possible to see, for example, the facial image from which it was processed. Irreversibility is slowly being recognised as a desirable, if not mandatory, trait of biometric data in the legal sphere.

[1073] Regulation (EU) 2016/679, Article 24.
[1074] ibid, Article 25.
[1075] ibid, Article 25(2).
[1076] M Gomez-Barrero and others, "General Framework to Evaluate Unlinkability in Biometric Template Protection Systems" (2018) 13 IEEE Transactions on Information Forensics and Security, 1406.

Interoperability regulations state that biometric data processed in the sBMS of the EU information systems *should* be made irreversible.[1077]

Revocability (also renewability) solves the problem that humans have only a limited number of fingerprints (or only one face and one pair of irises). Revocability allows multiple biometric templates to be created from the same fingerprint. This significantly improves the privacy and data protection of individuals. If their biometric data is stolen or compromised in another manner, individuals can obtain a new biometric identity from the same biometric reference (such as a fingerprint).

There are many technical standards related to the performance of a biometric system or the security of a system. Some of these standards, particularly those that define the minimum level of quality of a fingerprint or facial image, are already applied in EU legislation (e.g. the NIST Fingerprint Image Quality is prescribed for the functioning of EU information systems).[1078] The biometric template protection standard has been set in ISO/IEC 24745:2022 (Biometric information protection). This standard of protection has taken encryption methods such as bloom filters and homomorphic encryption into account. It defines protection of the biometric template in terms of its revocability and irreversibility. Nevertheless, given the effect that technical issues such as encryption can have on fundamental rights, some of these issues cannot be relegated to delegated acts in a legislative procedure because they determine the outcome of the proportionality analysis of justifying the processing of biometric data. Nor can public authorities have discretion on whether and how they will apply these important privacy enhancing tools.

The EU stakeholders have for some years been aware of the importance of encryption and the protection of biometric templates. Trusted Revocable Biometric Identities (TURBINE) was the first EU project that contemplated BTP methods.[1079] The EDPS commented positively on the results of TURBINE, by stating that it describes methods which first pseudonymise biometric data and then make it possible to revoke, if necessary, these pseudo-identities.[1080] There were

[1077] Recital 19 Regulation 2019/817 and 2019/818. See also 3.4.3.2 of the thesis on the irreversibility of the biometric template.

[1078] Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES) C/2019/1280 [2019] OJ L 57/18.

[1079] TrUsted Revocable Biometric IdeNtitiEs (Turbine) https://cordis.europa.eu/project/id/216339.

[1080] EDPS, "Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)" (2011) paras 28-32.

at least two further EU research projects concerned with exploring the issue of how biometric data should be protected. FIDELITY explored how to protect the privacy of individuals in the context of fast ePassport checks.[1081] The SWAN project concerned the security of biometric data for banking over mobile networks.[1082] However, these project approached the issue of biometric technologies primarily as a technological, not a legal, phenomenon.

5.6.3. Two Promising Methods of Encryption of Biometric Data

Achieving revocability and irreversibility is a technical challenge. There are at least two methods that promise to achieve this: bloom filters and homomorphic encryption.[1083]

Bloom filters are a mathematical method of encrypting biometric data (in particular, the biometric template).[1084] Biometric data are translated into a binary sequence (a sequence of zeroes and ones). First, all are initially set to zero, and then are split into smaller parts. These parts are individually hashed (in essence, encrypted) by different methods and put into specific places in the string of data which are set to one instead of zero. This new string of data consisting of zeroes and ones represents the bloom filter and is the protected biometric template. This template cannot be reversed to its original data (irreversibility). It also allows different biometric templates to be generated from the same original biometric data (which is known as renewability or revocability).[1085]

The mathematics of the process are, of course, more sophisticated than are understood here for the purpose of this legal thesis which is primarily concerned with understanding the legal effects of encryption methods. Bloom filter technology can be successfully applied to iris, fingerprint or facial biometric recognition.[1086] Further, it is claimed by technical experts that applying bloom filters does not impair the accuracy of biometric recognition.[1087] However, due to the

---

[1081] Fast and Trustworthy Identity Delivery and Check with ePassports Leveraging Traveler Privacy (FIDELITY) https://cordis.europa.eu/project/id/284862/factsheet.

[1082] "Secure Access Control over Wide Area Network" (SWAN) https://www.ntnu.edu/iik/swan/publications.

[1083] C Busch and others, "A Response to the European Data Protection Supervisor 'Misunderstandings in Biometrics' by the European Association for Biometrics" (2021) 11 IET Biometrics 79, 84; Christian Rathgeb and others, "On Application of Bloom Filters to Iris Biometrics" (2014) 3 IET Biometrics 207.

[1084] C Rathgeb and others, "On Application of Bloom Filters to Iris Biometrics" (2014) 3 IET Biometrics 207.

[1085] C Rathgeb, F Breitinger and C Busch, "Alignment-Free Cancelable Iris Biometric Templates Based on Adaptive Bloom Filters," 2013 International Conference on Biometrics (ICB) (IEEE 2013) <https://doi.org/10.1109/icb.2013.6612976>.

[1086] Marta Gomez-Barrero and others, "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters" (2016) 370–371 Information Sciences 18, 19.

[1087] ibid.

probabilistic nature of bloom filters, they may increase the false positive rate.[1088] The EDPB recommended the use of bloom filters and homomorphic encryption for the processing of contact tracing data in relation to the Covid 19 pandemic.[1089]

Homomorphic encryption has been repeatedly described as the holy grail of encryption.[1090] This designation is based on the idea that homomorphic encryption would allow computation (in this case biometric recognition) on data that remains encrypted (potentially anonymous). In other words, it is not necessary at any point of biometric recognition to decrypt the data. It seems that fully homomorphic encryption is still technically challenging to achieve[1091] and that it can primarily be used in the context of biometric verification, not identification.[1092] The science of homomorphic encryption is relatively new, having been developed in the 20th century. The first working model originates from a doctoral dissertation by Craig Gentry in 2009.[1093]

Homomorphic encryption can be applied on biometric data stored in passports and identification documents in the EU. The biometric data could be stored locally and also be encrypted. At the moment of an individual's arrival at passport control, the public authorities would be able to receive the encrypted data and conduct biometric recognition (by comparison with biometric data processed from a camera at the airport) without decrypting the biometric data stored in the document. This would increase the protection of the privacy of individuals. Not only would there be a lesser limitation of privacy and data protection on account of the processing conducted by public authorities, but the biometric data would also be protected if someone unauthorised physically comes into possession of the document with the biometric data. The eu-LISA has recognised limited revocability as a security issue in the context of border control.[1094]

[1088] P Bose and others, "On the False-Positive Rate of Bloom Filters" (2008) 108 Information Processing Letters 210.

[1089] EDPB, "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (2020), 16.

[1090] M Creeger, "The Rise of Fully Homomorphic Encryption" (2022) 20 Queue 39; M Corrales Compagnucci and others, "Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?" (2019) 3 European Pharmaceutical Law Review 144.

[1091] M Gomez-Barrero and others, "Multi-Biometric Template Protection Based on Homomorphic Encryption" (2017) 67 Pattern Recognition 149.

[1092] P Drozdowski and others, "On the Application of Homomorphic Encryption to Face Identification" 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2019, 1-5.

[1093] C Gentry, "A Fully Homomorphic Encryption Scheme" (2009) PhD thesis, Stanford University https://crypto.stanford.edu/craig/craig-thesis.pdf. For a simpler overview of the technological development of homomorphic encryption, see DJ Wu, "Fully Homomorphic Encryption: Cryptography's Holy Grail" (2015) 21 XRDS: Crossroads, The ACM Magazine for Students 24.

[1094] eu-LISA, "Enabling Seamless Travel to the European Union" (2022) 34.

The Institute of Electronics and Electrical Engineers (IEEE) is a body which develops standards and protocols concerning electronics and communications. The IEEE developed a standard for biometric privacy for which it claims that a biometric system which conforms to this standard does not incur either GDPR or US equivalent privacy requirements by using homomorphic encryption in which there is no need to store keys in a central database.[1095] This means that the biometric recognition system is never able to decrypt the biometric data. Homomorphic encryption has been mentioned as a method for enhancing the privacy of individuals whose biometric data are processed for the EES in a report by eu-LISA.[1096]

A number of critical points can be raised in relation to encryption, especially the techno-reductionist idea of it being the holy grail. There are a number of reasons why encryption methods such as those mentioned above may not be the solution even to those aspects of privacy and data protection which they claim to resolve. First of all, new research sometimes reveals that an encryption method may have previously undetected weaknesses.[1097] There may appear a new method of decryption (or attack) that was not taken into consideration by the authors of the encryption methods. In general, experts can be wrong in their calculations. Therefore, the claims of irreversibility and revocability achieved with no loss of performance[1098] should be taken with caution. The second reason bloom filters or homomorphic encryption may not represent the "holy grail" in terms of biometric data protection is that the technical papers do not understand or consider all the legal aspects concerning the protection of fundamental rights. As much as legal experts lack technical knowledge, so it is true that technological experts may have a narrow, simplistic understanding of the law. It may not be the case that all aspects of fundamental rights to privacy and data protection are exhaustively covered by these encryption methods, not to mention the implications for other fundamental rights.

[1095] IEEE 2410-2021, "IEEE Standard for Biometric Privacy" https://standards.ieee.org/ieee/2410/7746/.

[1096] eu-LISA, "Biometric Technologies in Identity Management and Verification" (2022) 21.

[1097] For example, Gomez-Barrero and others comment in their paper that the previous method of encryption may have faults: "While the irreversibility property of the system has been confirmed, it is shown that the initial scheme is vulnerable to cross-matching attacks. In [7] it has been demonstrated that suggested key-spaces are of insufficient size enabling brute-force cross-matching attacks. In addition, it has been shown that the irreversibility property of Bloom filter-based transforms depends on the nature of biometric data". M Gomez-Barrero and others, "Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters" (2016) 370–371 Information Sciences 18, 19.

[1098] Christoph Busch and others, "A Response to the European Data Protection Supervisor 'Misunderstandings in Biometrics' by the European Association for Biometrics" (2021) 11 IET Biometrics, 79, 84.

5.7. Conclusion: Kerkhoff's Principle

Auguste Kerkhoff was a 19th century cryptographer who stated that an information system should be designed in such a way that it is secure even if everything, apart from the key, is public knowledge. It means that the system is protected by encryption, not by hiding from others the way it operates. This is a valid privacy principle in relation to EU information systems and the way these should process biometric data.

To answer the main research question of the thesis, from the analysis presented in this chapter, it follows that encryption as a privacy enhancing tool can improve the privacy and data protection rights of individuals, but it is not the holy grail of fundamental rights protection. Therefore, the hypothesis can be considered to be only partially proven. Encryption must be a necessary component of the processing of biometric data, but it is not sufficient to provide the full measure of privacy and data protection rights that any individual, including migrants and asylum seekers, is entitled to in the sphere of EU law.

A number of conclusions can be drawn from the analysis in this final substantive chapter of the thesis. First, it could be argued that there already exists a right to encryption in EU law, as a right under privacy and data protection. In contrast, it could also be argued that public authorities can require their own right to have any personal data decrypted, in accordance with the existing framework for the human right to privacy. This tension between the right to encryption and the potential obligation to leave a backdoor is still not definitively resolved in the sphere of law.

Turning to more practical recommendations, the processing of biometric data should adhere to already existing international standards on biometric recognition and protection of the biometric template. A way forward is to embed technical standards in the legal text and, of course, to adjust the practical aspects of biometric systems to these standards. Clear references to the methods by which biometric data are protected are necessary in higher level legislative sources, such as the Eurodac Regulation and the Interoperability Regulations. The changes proposed here cannot be adequately made through delegated acts. The problems raised are fundamental rights problems and not mere technical issues. What is more, technical standards themselves do not equate to the protection of fundamental rights but can be considered only a necessary element. It would nevertheless be useful to incorporate the concepts of irreversibility and renewability into EU biometric law, given the importance of biometric data and the benefits these concepts may bring.

Encryption methods such as bloom filters and homomorphic encryption should be used in biometric information systems in the EU, even though this may lead to new legal uncertainties. As previously mentioned, encryption methods could enable biometric recognition with the use of anonymous data which seems beneficial for the privacy and data protection of individuals. However, the question then is how such anonymous data processing is regulated, since the whole of the data protection legal framework rests on the fact that personal data are being processed. Even if homomorphic encryption delivers on its promise, it is an open question whether such anonymous biometric recognition should be left completely unregulated, and if not, which framework would protect fundamental rights.

The proliferation of technical requirements and jargon in law is unavoidable but has significant drawbacks. It makes the law less understandable, more isolated from its other parts, and more reliant on narrow expert knowledge. It is unlikely that a layperson can understand their rights in relation to biometric data processing. The rules and principles need to remain broad and flexible in their application, as is the current virtue of the privacy and data protection legal framework. The successful protection of fundamental rights of migrants and asylum seekers in biometric applications still rests on reasonable rules and reasonable people applying those rules, with the guiding principle of human dignity.

Chapter 6: Conclusions and a Look to the Future.

6.1. Conclusions

This part contains the conclusions of each chapter along with the general conclusion.

Chapter 1 concluded that legal biometric terminology should be better aligned with ISO/IEC biometric vocabulary. The analysis showed that EU legal norms have consistently confused the term authentication with verification and that certain other important terms for understanding biometrics as a legal phenomenon are missing. It is particularly important for the law to have a proper, better understanding of biometric categorisation, a concept which shows that not all use of biometric technologies involves the processing of biometric data, and the notion of biometric data itself, which is not adequately defined in EU law. In concrete terms, ISO/IEC biometric vocabulary should be used in legal terminology. EU legislation should stop using the deprecated notion of authentication and instead refer to biometric verification. The most problematic issue is biometric categorisation, which currently is not considered to be either a type of biometric recognition in the sense of ISO standards nor does it represent the processing of biometric data in the meaning of EU law. Nevertheless, a policy choice needs to be made on whether to include biometric categorisation as a notion in EU law. The AI Act already defines this term, though not in terms of processing biometric data. The second chapter analysed the elements that make up EU biometric law. Most importantly, this chapter aimed to resolve how to properly interpret the definition of biometric data, but also how the definition could be improved. According to the analysis, biometric data as the law stands should be interpreted to represent sensitive personal data in the meaning of Article 9(2) GDPR both when they concern biometric verification and biometric identification. Biometric categorisation involves the processing of personal data, not biometric data, as the law stands. The definition of biometric data could be significantly improved, however. The term biometric recognition should be used instead of the less precise notions of allowing and confirming identification, and the characteristics mentioned in the definition should be simplified to refer to behavioural and biological characteristics.

Chapter 2 presented a systematisation of the rules that make up EU biometric law, which includes provisions of the LED, EUDPR and the AI Act. A critical analysis of provisions of the GDPR and of the AI Act related to biometrics resulted in a number of conclusions. Each component of the definition of biometric data was analysed and a conclusion drawn that the definition could be simplified without any loss of clarity. For example, instead of referring to physical, physiological or behavioural characteristics, it would be better to refer simply to

human characteristics. Furthermore, "allowing and confirming identification" should be replaced with the more precise term of "biometric recognition". This would have the same meaning but would avoid confusion as to whether the current definition relates to both identification and verification. It was concluded that the current definition is narrow, excluding, for example, photographs from being considered as biometric data unless the photographs are processed by specific technical means for the purpose of biometric identification or verification. However, it was also considered that there are good reasons for keeping a narrow definition of biometric data in order not to overly burden any processing of photographs with the requirements for the processing of biometric data.

One of the crucial results of the analysis in this thesis concerned the relationship between the two mentions of biometric data in the GDPR, namely whether Articles 4(14) and 9(1) GDPR contain different conceptions of biometric data or if there is only a single definition. This is vitally important for understanding biometric law. If there are two definitions of biometric data, with only one type of biometric data being considered sensitive personal data, this greatly determines the conditions for processing biometric data. However, the analysis of the wording of the provisions as well as an analysis of the legislative history and intentions of the legislators led to the conclusion that the proper understanding of biometric data should be that all biometric data are sensitive, meaning that the processing of biometric data must conform to the conditions of Article 9(1) GDPR (and the corresponding articles in the LED and EUDPR). This research revealed that the EU legislator and the Court are not aware of the confusion created by these different ways of understanding of biometric data. In short, this thesis has explained how the concept of biometric data should be interpreted as the law stands, at the same time adding recommendations on how the definition of biometric data could be improved.

Further, it was argued that the ECHR exhibits decisive influence on EU biometric law, and this was demonstrated by the analysis of the ECHR, Convention 108 and the case law of the ECtHR related to biometrics. Finally, Chapter 2 examined the application of biometric law in case studies on Clearview AI and Worldcoin biometric practices. This has shown that the already existing legal framework systematised as EU biometric law can be successfully used to protect the privacy of individuals in the context of modern technologies, such as AI and facial recognition.

Chapter 3 was tasked with defining EU biometric law but in the more specific circumstances of EU migration and asylum. In the first part of the chapter, a critical analysis of EU biometric

case law (concerning migration) was conducted, and the conclusion drawn that the CJEU uses the framework of privacy and data protection to resolve cases concerning the processing of biometric data. However, the approach of the Court was determined to be inconsistent with certain facts that are important for biometrics. For example, it was shown that in *A, B and P* the Court held that the processing of ten fingerprints is a proportionate measure, while previously in *Schwarz* the Court ruled that the processing of two fingerprints is proof that the measure of limiting privacy and data protection does not go beyond what is necessary to meet the objective of general interest. Moreover, the Court may rephrase the question received from a national court, as it did in *Willems*. In this way, it avoided answering whether a national measure which requires remote national biometric databases goes beyond what is necessary, since the Court had previously stated that storing biometric data only locally, on the document itself, satisfies the proportionality principle (*Schwarz*).

The second part of Chapter 3 constructed a model of so-called biometric parameters, representing the building blocks of any biometric system, and which can be used to assess a biometric system through the lens of EU biometric law as established in this thesis. This was done in the case study of the Eurodac information system, by considering its main parameters of length and place of storage, access to biometric data, the purpose of processing, and other parameters which were defined in the course of this section. This model may allow any biometric system to be assessed by a checklist of factors which would enable any practitioner, or deployer of a biometric system, to judge whether a biometric system satisfies the legal requirements of EU (biometric) law. The final part of Chapter 3 examined the interoperability of EU biometric systems, and in particular the concept of the biometric template. It was concluded that the biometric template is and should be regarded as biometric data, despite the examined arguments to the contrary.

Chapter 4 analysed the fundamental rights of biometrics. First, it was concluded that privacy and data protection are the most important fundamental rights for the regulation of the use of biometric data in the EU. The Court uses these two rights together to assess biometrics. The first part explored the reasons of how and why privacy in particular, and later also data protection, were the fundamental rights that emerged as crucial for the legal framing of biometrics. However, it was further argued that there are other fundamental rights which are affected by the use of biometric technologies. First, human dignity is infringed by the forced fingerprinting of vulnerable people, including children, for enrolment into Eurodac. An important insight raised in this thesis is that the legal requirement to provide fingerprints, which

exists in EU law as well as national laws, effectively changes the meaning of the right to asylum. If a person refuses to provide fingerprints, their request for international protection may be denied, despite the fact that the person in question may satisfy all the requirements of international law to be recognised as a refugee. In this way, the definition of refugee is changed and expanded by EU biometric law, which adds the requirement that to be recognised as a refugee the individual has to provide fingerprints.

Finally, the fundamental right to non-discrimination was analysed as a possible legal avenue for limiting the negative effects of biometrics. This was done by studying facial recognition in particular. However, the conclusion reached was that non-discrimination, unlike privacy, is difficult to successfully apply in the use of biometrics, due to the legal discrimination framework which is hard to prove. Despite this, the analysis yielded a number of practical recommendations and insights. In order to reduce algorithmic bias, algorithms need to be state-of-the-art and have to be trained on large and representative datasets, which should be made a legal requirement. The appropriate understanding of bias and discrimination should be arrived at by examining whether biometric technologies reduce the biases that already exist, instead of striving to achieve biometric technologies with no bias at all, which is not possible in any circumstances. The final insight is that, when it comes to applying biometric algorithms, there is a trade-off between fairness and accuracy, which requires a policy choice of what matters most.

In sum, the previous chapters answered how biometric technologies are regulated in EU law and in migration and asylum in particular, what the biometric template is and which fundamental rights are affected by the use of biometric technologies and the extent to which they are affected. This allowed for the final chapter which corresponds to the main hypothesis. The conclusion of Chapter 5 is that there are encryption methods which can protect biometric templates and therefore significantly reduce the negative effects of biometrics on privacy and data protection. It confirmed that there are already rules in place which can be interpreted as a legal basis for the encryption of biometric data. These methods are in particular bloom filters and homomorphic encryption. Chapter 5 explained how these methods work and discussed the legal implications of these methods by examining them with regard to their effects on pseudonymity and anonymity of personal data. It was also added that the irreversibility and revocability of biometric templates should be defined as legal terms. Irreversibility should be a standard feature of biometric data, which would prevent biometric data from revealing, for example, the original photograph of the face from which the biometric data were processed.

The revocability of biometric data would allow the issuing of new biometric identities if the previous biometric data were stolen or compromised in another manner. It was suggested that there might even be a right to encryption of personal data as an emerging right within the framework of data protection. This would mean that encryption should be understood as a necessary condition for the processing of biometric data. However, it was shown that at the same time there is an emerging tendency of public authorities to prohibit encryption. Public authorities may be unable to access personal or biometric data they find crucial for security and law enforcement if certain encryption methods are applied. This leads, the thesis concluded, to a privacy and encryption dilemma between an emerging right to encryption and reasons for there to be an obligation to decrypt data when required by public authorities. Therefore, it was finally concluded that encryption is one of many privacy enhancing tools, but it is not the holy grail of privacy and data protection. There are limits to encryption for a number of reasons. For example, it may be the case that encryption methods have a flaw not previously detected, or that a new technology renders a certain encryption method obsolete. For these reasons, the main hypothesis was thus only partially supported by the analysis of Chapter 5 given that encryption is a necessary, but not a sufficient, element of privacy and data protection in the context of EU biometric law.

6.2. A Look into the Future of Biometric Law

Nobody knows what the future holds. Past events are a reliable indicator of the future, except in those rare but fundamental events which nobody expects to happen, as much as nobody expected the Spanish inquisition. Judging by the historical developments, biometrics are going to become an even more important element of law, crucial for identification, control and security. And yet this trajectory is not a destiny. A single event, for example the reaction to the September 11 attacks, triggered a wave of changes which resulted in the introduction of biometric technologies in migration control. The following decades shifted towards prioritising security over human rights. The migration crisis in Europe, which has never completely tapered off, resulted in further limitations of the fundamental rights and freedoms of migrants caused by the use of modern technologies, such as biometrics, to protect borders and territories. The apex of this securitisation of refugee and migration law was perhaps reached by the interoperability of EU information systems and the addition of facial recognition capabilities to extant migration systems which relied on fingerprinting. The AI Act, as has been shown in this thesis, represents a concession to security concerns and the use of biometric surveillance over privacy.

Yet, there are signs that technologies have reached their negative societal limits. The interoperability of EU systems continually appears to be a few years away from full functionality. The AI Act, even before becoming applicable, has recently been criticised by those who were previously the greatest force behind the push for allowing in the AI Act the most intrusive of biometric practices. It is true that interoperability has been marred by technical difficulties, and that the AI Act is now seen as a potential hindrance to economic growth, more than these two are seen as problems for the privacy and data protection of individuals. However, this shows that an atmosphere of securitisation can quickly change to one of deregulation, and back again. These material sources of law are governed by the fear, intuition and instinct of political leaders and of the political masses, more than by a rational and legal analysis. Nevertheless, the law is here, available to properly frame the problems that biometrics cause migrants as limitations of fundamental and human rights. The lines which limit the use of biometrics have to be drawn and cannot simply rely on the technical limitations of biometrics. Law and fundamental rights are the best canvas for drawing these lines. Biometrics are just another tool that humans have invented, along with the hammer or pencil. Biometrics must be used to serve the interests of human individuals and societies. The message to legislators and courts is that, in the future, biometrics should be measured by the yardstick of human rights, where human dignity should be the basic unit of measure.

Bibliography and Other Sources Used in the Research

Bibliographic Sources

- Agamben G., *Homo sacer: Suverena moć i goli život* (Multimedijalni institut, 2006).
- Almada M., N Petit N., "The EU AI Act: A Medley of Product Safety and Fundamental Rights?" EUI RSC Working Paper 2023/59.
- Bačić Selanec N., Petrić D., "Migrating with Dignity: Conceptualising Human Dignity Through EU Migration Law", (2021) 17(3) European Constitutional Law Review, 498–516.
- Barocas S., Selbst AD, "Big Data's Disparate Impact" (2016) 104(3) California Law Review, 671–732.
- Berlin I., "Two Concepts of Liberty". In I Berlin (ed.), *Four Essays On Liberty* (Oxford University Press, 1969).
- Blasi Casagran C., "Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU" (2021) 21 Human Rights Law Review 433.
- Borgesius FZ, "Discrimination, Artificial Intelligence, and Algorithmic Decision-making", Council of Europe, 2018.
- Borgesius FZ, "Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence" (2020) 24 International Journal of Human Rights 1572.
- Bose P. et al., "On the False-Positive Rate of Bloom Filters" (2008) 108 Information Processing Letters 210.
- Busch C. et al., "A Response to the European Data Protection Supervisor 'Misunderstandings in Biometrics' by the European Association for Biometrics" (2021) 11 IET Biometrics 79.
- Buolamwini J., Gebru T., "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81(1) Proceedings of Machine Learning Research.

- Bygrave LA, L Tosoni L., “Article 4(15). Data Concerning Health” in C Kuner et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020). ISBN 978–0–19–882649–1.
- Byrne WH, Olsen HP, “Doctrinal Legal Science: A Science of Its Own? (pp. 1–25) (2024). University of Copenhagen. MOBILE Working Paper Series No. 36.
- Chiara PG, “Towards a right to cybersecurity in EU law? The challenges ahead”, Computer Law & Security Review, Volume 53, 2024.
- Corrales Compagnucci M. Et al., “Homomorphic Encryption: The ‘Holy Grail’ for Big Data Analytics and Legal Compliance in the Pharmaceutical and Healthcare Sector?” (2019) 3 European Pharmaceutical Law Review 144.
- Costello C., *The Human Rights of Migrants in European Law* (Oxford University Press, 2016).
- Creeger M., “The Rise of Fully Homomorphic Encryption” (2022) 20 Queue 39.
- Darwin C., *On the Origin of Species* (general editor David Quammen, Sterling, 2008).
- Drozdowski P. et al., “On the Application of Homomorphic Encryption to Face Identification” 2019 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2019, pp. 1-5.
- Duić D., Petrašević T., “Data Protection and Cybersecurity : Case-Law of Two European Courts,” EU and comparative law issues and challenges series (Faculty of Law, Josip Juraj Strossmayer University of Osijek 2023).
- Dupré C., *The Age of Dignity: Human Rights and Constitutionalism in Europe* (Bloomsbury Publishing 2016).
- Emeriau M., “Learning to Be Unbiased: Evidence from the French Asylum Office” (2022) 67 American Journal of Political Science 1117.
- Foucault M., *Rođenje biopolitike* (Sandorf i Mizantrop, 2016).

- Galton F., “Eugenics: Its Definition, Scope, And Aims”, (July 1904) 10(1) The American Journal of Sociology <https://galton.org/essays/1900-1911/galton-1904-am-journ-soc-eugenics-scope-aims.html> accessed 28 May 2025.
- Galton F., *Hereditary Genius: An Inquiry Into Its Laws and Consequences* (1869).
- Galton F., *Finger Prints* (MacMillan, 1892) 195 <https://galton.org/books/finger-prints/galton-1892-fingerprints-1up.pdf> accessed 28 May 2025.
- Gentry C., “A Fully Homomorphic Encryption Scheme” (2009) PhD thesis, Stanford University <https://crypto.stanford.edu/craig/craig-thesis.pdf> accessed 28 May 2025.
- Georgieva L., Kuner C., “Article 9. Processing of Special Categories of Personal Data’ in C Kuner et al. (eds.) *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), 376. ISBN 978–0–19–882649–1.
- Guild E., “Unreadable Papers? The EU’s First Experiences with Biometrics: Examining Eurodac and the EU’s Borders” in Juliet Lodge (ed), *Are You Who You Say You Are? The EU and Biometric Borders* (Wolf Legal Publishers, 2007).
- Guild E., “The Europeanisation of Europe’s Asylum Policy,” International Refugee Law (2017) 18(3-4).
- Goldner Lang I., “‘Laws of Fear’ in the EU: The Precautionary Principle and Public Health Restrictions to Free Movement of Persons in the Time of COVID-19” (2021) 14 European Journal of Risk Regulation 141.
- Goldner Lang I., “Croatia and EU Asylum Law: Playing on the Sidelines or at the Centre of Events?” In V Stoyanova and E Karageorgiou (eds.), *The New Asylum and Transit Countries in Europe during and in the Aftermath of the 2015/2016 Crisis* (Brill, 2018).
- Goldner Lang I., Nagy B., “External Border Control Techniques in the EU as a Challenge to the Principle of Non-Refoulement” (2021) 17(3) European Constitutional Law Review.
- Gomez-Barrero M. et al., “Unlinkable and Irreversible Biometric Template Protection Based on Bloom Filters” (2016) 18 Information Sciences, 370–371.

- Gomez-Barrero M. et al., “General Framework to Evaluate Unlinkability in Biometric Template Protection Systems” (2018) 13 IEEE Transactions on Information Forensics and Security 1406.
- Gomez-Barrero M. et al. “Multi-Biometric Template Protection Based on Homomorphic Encryption” (2017) 67 Pattern Recognition 149.
- Gonzàlez Fuster G., "Fighting for Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection" (2014) 2, Birkbeck L. Rev.
- Hacker P., “Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law” (2018) 55 Common Market Law Review 1143.
- De Hert P., Bouchagiar G., “Visual and Biometric Surveillance in the EU. Saying ‘No’ to Mass Surveillance Practices?” Information Polity (2022), 27(2), 193–217.
- De Hert P., Bouchagiar G., “Facial Recognition, Visual and Biometric Data in the US. Recent, Promising Developments to Regulate Intrusive Technologies”, Brussels Privacy Hub, Working Paper 7(29)(2021b).
- Hill TE., “In Defence of Human Dignity: Comments on Kant and Rosen”, Understanding Human Dignity (British Academy 2013).
- Van Hoecke M., “Legal Doctrine: Which Method(s) for What Kind of Discipline?” In Mark van Hoecke (ed), *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* (Hart Publishing, 2011) 1–18.
- Jasserand C.A., “Avoiding Terminological Confusion between the Notions of ‘Biometrics’ and ‘Biometric Data’: An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective”. *International Data Privacy Law, 6*(1) (2016). https://doi.org/10.1093/idpl/ipv020, 66-67.
- Jasserand C.A., “Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data’ (2016) European Data Protection Law, 2 Rev. 297.

- Jasserand-Breeman C.A., “Reprocessing of Biometric Data for Law Enforcement Purposes” (Thesis fully internal (DIV), University of Groningen 2019).
- Kak A., Introduction, in A Kak, ed., “Regulating Biometrics: Global Approaches and Urgent Questions” AI Now Institute, 1 September 2020
- Van Klink B., Taekema HS, “On the Border: Limits and Possibilities of Interdisciplinary Research” in Bart van Klink, Hester Sanne Taekema (eds), *Law and Method: Interdisciplinary Research into Law* (Mohr Siebeck, 2011) 7–32.
- Kindt E., *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Science & Business Media, 2013).
- Kindt E., “A First Attempt at Regulating Biometric Data in the European Union” in Amba Kak (ed), *Regulating Biometrics: Global Approaches and Open Question* (AI Now Institute, 2020).
- Kindt E., “Having Yes, Using No? About the New Legal Regime for Biometric Data” Computer Law & Security Review: The International Journal of Technology Law and Practice (2017).
- Kindt E., “Biometric Data Processing: Is the Legislator Keeping Up or Just Keeping Up Appearances” in G González, R Van Brakel, and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (Elgar, 2022).
- Kleinberg J. et al., “Algorithmic Fairness” (2018) 108 AEA Papers and Proceedings.
- Kleinberg J. et al., “Discrimination in The Age of Algorithms” (National Bureau of Economic Research 2019) https://doi.org/10.3386/w25548.
- Kokott J., Sobotta C., “The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR” International Data Privacy Law, volume 3, issue 4, November 2013, pp. 222–228.
- Kontak M., “Biometric Borders Envisaged by Frontex: Fundamental Rights in the Backseat” European Papers, vol. 9, no 2, 2024, 621-640.
- Kuner C. et al. (eds.) (2020) *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press, 209. ISBN 978–0–19–882649–1.

- Lawson R., “Atlas Shrugged: An Analysis of the ECtHR Case Law Involving Issues of EU Law Since Opinion 2/13” European Papers, vol. 9, no 2, 2024, pp. 647-671.
- Lenaerts K., Gutierrez Fons J., “To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice” (EUI AEL 2013/09, Distinguished Lectures of the Academy).
- Macklin R., “Dignity Is a Useless Concept” (2003) 327 BMJ 1419.
- Marnau N., C Sorge C., “From Law to Engineering: A Computer Science Perspective on Privacy and Data Protection’ in G González, R Van Brakel, and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law* (2022 Elgar).
- McCrudden C., “Human Dignity and Judicial Interpretation of Human Rights” (2008) 19 European Journal of International Law.
- Molnár T., “The Impact of ECtHR Case-law on the CJEU’s Interpreting of the EU’s Return Acquis: More Than It First Seems?’ Hungarian Journal of Legal Studies, volume 62, issue 4, 2022, 273 https://doi.org/10.1556/2052.2022.00354.
- Moraru M., “The EU Fundamental Right to Asylum: In Search of Its Legal Meaning and Effects”. In S Iglesias Sánchez and M González Pascual (eds.), Fundamental Rights in the EU Area of Freedom, Security and Justice (Cambridge University Press, 2021).
- Moreno-Lax V., “Mutual (Dis-)Trust in EU Migration and Asylum Law: The ‘Exceptionalisation’ of Fundamental Rights”. In S Iglesias Sánchez and M González Pascual (eds.), Fundamental Rights in the EU Area of Freedom, Security and Justice (Cambridge University Press, 2021).
- Mukharjee S., *The Gene: An Intimate History* (Penguin, 2016).
- Ozkul D., “Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe” 2023 University of Oxford, Refugee Studies Centre.
- Palmiotto F., “When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis”, German Law Journal (2024) 25(2):210-236.

- F Palmiotto F., N Menéndez González N., “Facial Recognition Technology, Democracy and Human Rights” Computer Law & Security Review, volume 50, 2023, 105857, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2023.105857.
- Paolucci F., “From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights” in Natalia Menéndez González and Giuseppe Mobilio (eds), *Facial Recognition Technology* (Springer, 2024) (forthcoming) <https://ssrn.com/abstract=4929132> accessed 28 May 2025.
- Van der Ploeg I, “The Illegal Body: `Eurodac' and the Politics of Biometric Identification”. Ethics and Information Technology (1999) 1, 295–302.
- Ramji-Nogales J., Schoenholtz AI, Schrag PG, *Refugee Roulette: Disparities in Asylum Adjudication and Proposals for Reform* (NYU Press 2011).
- Rathgeb C. et al., “On Application of Bloom Filters to Iris Biometrics” (2014) 3 IET Biometrics 207.
- Riedl M.A., “Notes Biometric Borders and Minors’ Rights: A Critical Analysis of European Migration Management under the New Eurodac Regulation” (2024) University of Twente Student Thesis.
- Rodriguez PA, “Human Dignity as an Essentially Contested Concept” (2015) 28 Cambridge Review of International Affairs 743.
- Rosen M., “Dignity: The Case Against”. In C McCrudden (ed.), *Understanding Human Dignity* (British Academy, 2013).
- Russell S., Norvig P., A*rtificial Intelligence: A Modern Approach* (4th Edition, Global Edition, Pearson, 2022).
- Rutherford A., *Control: The Dark History and Troubling Present of Eugenics* (WW Norton & Company, 2022).
- Schneier B., “Inside Risks: The Uses and Abuses of Biometrics” (1999) 42 Communications of the ACM 136.
- Shurson J., “A European Right to End-to-End Encryption?” (2024) Computer Law & Security Review 55 106063 2024.

- Sumer B., 'The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?' (2024) 10 *European Data Protection Law Review* 150 https://doi.org/10.21552/edpl/2024/2/6.

- De Terwangne C., "Council of Europe Convention 108+: A Modernised International Treaty for the Protection of Personal Data", Computer Law & Security Review, volume 40, 2021, 105497, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105497.

- De Terwangne C., "Privacy and Data Protection in Europe: The Council of Europe's Convention 108+ and the European Union's GDPR" in G González, R Van Brakel and P De Hert (eds), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics* (Elgar, 2022), pp. 10-35.

- Tinière R., "The Use of ECtHR Case Law by the CJEU: Instrumentalisation or Quest for Autonomy and Legitimacy?" European Papers, vol. 8, no. 1, 2023, pp. 323-330, 325 ISSN 2499-8249 - doi: 10.15166/2499-8249/654.

- Tzanou M., *The Fundamental Right to Data Protection Normative Value in the Context of Counter-Terrorism Surveillance* (Hart 2017).

- Valdivia A., Serrajòrdia JC, Swianiewicz A., "There Is an Elephant in the Room: Towards a Critique on the Use of Fairness in Biometrics" (2022) 3 AI and Ethics 1407.

- Vavoula N., *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (BRILL 2022).

- Vavoula N., "Interoperability of EU Information Systems: The Deathblow to the Rights to Privacy and Personal Data Protection of Third-Country Nationals?" (2020) 26 European Public Law 131.

- Vavoula N., "Consultation of EU Immigration Databases for Law Enforcement Purposes: A Privacy and Data Protection Assessment" (2020) 22 European Journal of Migration and Law 139.

- Warren SD, Brandeis LD, "The Right to Privacy" (1890) 4 Harvard Law Review 193.

- Wu DJ, "Fully Homomorphic Encryption: Cryptography's Holy Grail" (2015) 21 XRDS: Crossroads, The ACM Magazine for Students 24.

Legislation

- Charter of Fundamental Rights of the European Union [2012] OJ C326/393 (CFR).
- Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services OJ L 373, 21.12.2004.
- Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ L180.
- Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation [2000] OJ L 303/16.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) PE/32/2022/REV/2 OJ L 333.
- Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) [2006] OJ L 204/23.
- EU Commission, Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES) C/2019/1280 OJ L 57 (EES Implementing Decision 2019/329).
- EU Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final 2012/0011 (COD).
- EU Commission, "Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Regulation (EU) 2017/2226 and Regulation (EU) 2016/399 as regards a progressive start of operations of the Entry/Exit System" 567 final 2024/0315(COD).

- Consolidated version of the Treaty on the Functioning of the European Union OJ C 326, 26.10.2012, p. 47–390 (TFEU).
- Consolidated version of the Treaty on European Union [2012] OJ C326/1 (TEU).
- EU 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 210/1.
- Council of Europe (CoE), Consultative Committee of the Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No. 108] (Strasbourg 2013) T-PD(2013)06 <https://rm.coe.int/consultative-committe-of-the-convention-for-the-protection-of-individu/16806945c7> accessed 28 May 2025.
- CoE, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
- CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS, No. 108, 28 January 1981, Strasbourg (Convention 108).
- CoE, Convention 108 + Convention for the protection of individuals with regard to the processing of personal data <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 28 May 2025.
- CoE, Amending the Protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data CM/Del/Dec(2018)128/5.
- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L 385/1.
- Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation) Interinstitutional File: 2012/0011(COD) 2014 <https://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf> accessed 28 May 2025.

- Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Written debriefing of trilogue on 24 November ST 14461 2015 INIT <https://www.consilium.europa.eu/en/documents/public-register/public-register-search/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentLanguage=EN&ImmcIdentifier=ST%2014461%202015%20INIT> accessed 28 May 2025.

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 (Data Protection Directive - DPD).

- Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast) [2013] OJ L 180/60.

- 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 [2016] OJ L119/89 (Law Enforcement Directive - LED).

- Pravilnik o obradi biometrijskih podataka NN 122/2020 (Croatian Ordinance on the processing of biometric data).

- Pravilnik o načinu prikupljanja podataka, tehničkim uređajima za prikupljanje podataka, sadržaju i korisnicima operativnih zbirki podataka koje vodi granična policija te rokovima čuvanja NN 102/2018 (Ordinance on the method of data collection, technical devices for data collection, content and users of operational data collections maintained by the border police and on the retention periods).

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 General Data Protection Regulation [2016] OJ L119 (GDPR).

- 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 - AI Act) [2024] OJ L2024/1689.

- Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement PE/70/2019/REV/1 [2019] OJ L188/67.

- Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 PE/33/2019/REV/1 OJ L 295, 14.11.2019.

- Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification) OJ L 77, 23.3.2016.

- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA PE/30/2019/REV/1 OJ L 135, 22.5.2019.

- 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 PE/31/2019/REV/1 OJ L 135, 22.5.2019.

- Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes [2017] OJ L327/20.

- Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints [2013] OJ L180/1.

- 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 L295/39 (European Data Protection Regulation - EUDPR).

- Regulation (EU) 2018/1860 on the use of the Schengen Information System for the return of illegally staying third-country nationals.

- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks PE/35/2018/REV/1 [2018] OJ L312/14.

- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L 312/56.

- Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders PE/20/2024/REV/1 [2024] OJ L 2024/1356; Regulation (EU) 2024/1351 of the European Parliament and of the Council of 14 May 2024 on asylum and migration management PE/21/2024/REV/1 [2024] OJ L 2024/1351.

- Regulation (EU) 2024/1348 of the European Parliament and of the Council of 14 May 2024 establishing a common procedure for international protection in the Union and repealing Directive 2013/32/EU PE/16/2024/REV/1 [2024] OJ L 2024/1348.

- Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of “Eurodac” for the comparison of biometric data [2024] OJ L2024/1358 (Eurodac 2024 Regulation).

- Zakon o obradi biometrijskih podataka NN 127/19 (The Croatian Act on the Processing of Biometric Data).
- Zakon o provedbi Opće uredbe o zaštiti podataka NN 42/2018 (Croatian Act on the Implementation of the GDPR).
- Zakon o nadzoru državne granice NN 83/18, 27/16, 114/22, 151/22 (Act on State Border Control).
- Zakon o međunarodnoj i privremenoj zaštiti NN 70/15, 127/17, 33/23, 17/25 (Act on International and Temporary Protection).
- Zakon o strancima NN 133/20, 114/22, 151/22 (Aliens Act),

Case Law

- Case C-377/98 Netherlands v Parliament and Council ECLI:EU:C:2001:523.
- Case C-36/02 Omega ECLI:EU:C:2004:614.
- Case T-194/04 Bavarian Lager ECLI:EU:T:2007:334.
- Case C-524/06 Huber ECLI:EU:C:2008:724.
- Case C-236/09 Test-Achats ECLI:EU:C:2011:100.
- Case C-617/10 *Åkerberg Fransson* ECLI:EU:C: 2013:105.
- Case C-291/12 *Schwarz* ECLI:EU:C:2013:670.
- Case C-291/12 *Schwarz* ECLI:EU:C:2013:401, Opinion of AG Mengozzi.
- Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238.
- Case C-446/12 *Willems* ECLI:EU:C: 2015:238.
- Opinion 2/13 ECLI:EU:C:2014:2454.
- Case C-362/14 *Schrems I* ECLI:EU:C: 2015:650.
- Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C: 2016:970.
- Opinion 1/15 ECLI:EU:C:2017:592.

- Joined cases C-511/18 *Quadrature du Net* ECLI:EU:C:2020:791, paras 187-189.
- Case C-70/18 *A, B and P* ECLI:EU:C:2019:823.
- Case C-311/18 *Schrems II* ECLI:EU:C: 2020:559.
- Joined Cases C 322/19 and C 385/19 *The International Protection Appeals Tribunal and Others* ECLI:EU:C:2021:11.
- Case C-18/19 *WM v Stadt Frankfurt am Main* ECLI:EU:C:2020:130, Opinion of Advocate General Pikamäe.
- Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* ECLI:EU:C: 2022:491.
- Case C-709/20 *The Department for Communities in Northern Ireland* ECLI:EU:C:2021:602.
- Case C-205/21 *Ministerstvo na vatreshnite raboti* ECLI:EU:C:2023:49.
- Case C-634/21 *Schufa Holding* ECLI:EU:C:2023:957.
- Case C-61/22 *RL v Landeshauptstadt Wiesbaden* ECLI:EU:C: 2024:251.
- Case C-118/ 22 *NG v Ministerstvo na vatreshnite raboti* ECLI:EU:C:2024:97.
- Case C-80/23 *Ministerstvo na vatreshnite raboti* ECLI:EU:C: 2024:991.
- *Big Brother Watch and Others v. UK*, App. Nos. 58170/13, 62322/14 and 24960/15 (ECtHR 25 May 2021).
- *Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium v Belgium* (Merits) App. no. 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64) (ECtHR, 23 July 1968).
- *Timishev v Russia*, App. nos. 55762/00 and 55974/00 (ECtHR, 13 December 2005).
- *DH and Others v the Czech Republic*, App. no. 57325/00 (ECtHR, 13 November 2007).
- *I v. Finland,* App. no. 20511/03 (ECtHR, 17 October 2008).
- *S and Marper v UK,* App. No. 30562/04 and 30566/04 (ECtHR, 4 December 2008).

- *Rotaru v Romania*, App. no. 28341/95 (ECtHR 4 May 2000).
- *MK v France,* App. no. 19522/09 (ECtHR, 18 April 2013).
- *Peruzzo and Martens v Germany*, App. nos. 7841/08 and 57900/12 (ECtHR, 4 June 2013).
- *Dembele v Switzerland*, App. no. 74010/11 (ECtHR, 17 February 2014).
- *Biao v Denmark,* App. no. 38590/10 (ECtHR, 24 May 2016).
- *Škorjanec v Croatia,* App. no. 25536/14 (ECtHR 28 June 2017).
- *Trajkovski and Chipovski v North Macedonia*, App. nos. 53205/13 and 63320/13 (ECtHR,13 February 2020).
- *Gaughran v UK,* App. no .45245/15 (ECtHR, 13 June 2020).
- *Glukhin v Russia*, App. no.. 11519/20 (ECtHR, 4 July 2023).
- *Podchasov v. Russia,* App. no. 33696/19 (ECtHR 13 May 2024).
- *Wa Baile v Switzerland*, App. nos. 43868/18 and 25883/21 (ECtHR, 20 May 2024).
- *R (Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058.
- Rechtbank Den Haag, *Syri* ECLI:NL:RBDHA:2020:1878.
- Canadian Federal Court, *Barre v Canada* 2022 FC 1078.

Other Sources

- AFAR project website <https://www.hertie-school.org/en/research/research-directory/afar> accessed 28 May 2025.
- Article 29 Working Party (A29WP), "Opinion 2/2012 on facial recognition in online and mobile services" (2012) 00727/12/EN WP 192, Regulation (EU) 2024/1689.
- A29WP, "Opinion 3/2012 on Developments in Biometric Technologies" (2012) 00720/12/EN WP193.

- A29WP, “Opinion 4/2007 on the concept of personal data” (2007) 01248/07/EN WP 136.
- A29WP, “Working Document on Biometrics” (2003) WP 80.
- A29WP, “Opinion 03/2013 on purpose limitation” (2013) 00569/13/EN WP 203.
- A29WP, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679” (2018) 17/EN WP251rev.01.
- A29WP, “Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is ‘Likely to Result in a High Risk’ for the purposes of Regulation 2016/679” 17/EN WP 248 (2017).
- A29WP, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (2014) 844/14/EN WP 217”.
- AZOP, <https://azop.hr/sedam-novih-upravnih-novcanih-kazni-u-iznosu-od-169-000-eura/> accessed 28 May 2025.
- Border Violence Monitoring Network (BVMN) “Input by Civil Society Organisations to the EUAA Asylum Report 2024 by the Border Violence Monitoring Network” <https://euaa.europa.eu/sites/default/files/2024-02/border_violence_monitoring_network.pdf> accessed 28 May 2025.
- Busch C., “Biometric Data Interchange Standards and ICAO 9303 Relevance” presentation, available at <https://www.christoph-busch.de/files/Busch-ICAO-39794-NFIQ2-210419.pdf> accessed 28 May 2025.
- Biden White House, “Blueprint for an AI Bill of Rights” (2022) <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/> accessed 28 May 2025.
- Choi T., “Biometrics Use by Canadian Border Agency Increasing. Maybe It Already Has” BiometricUpdate.com (January 25, 2022) <https://www.biometricupdate.com/202201/biometrics-use-by-canadian-border-agency-increasing-maybe-it-already-has> accessed 28 May 2025.
- Commission nationale de l’Informatique et des Libertés (CNIL) Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI.

- CNIL, Entry into force of the European AI Regulation: the first questions and answers from the CNIL (2024) <https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil> accessed 28 May 2025.
- Comissão Nacional de Proteção de Dados (CNDP) DELIBERAÇÃO/2024/137 <https://www.cnpd.pt/media/imub4o4i/pt-sa-decision-worldcoin_temporary-limitation-of-processing_20240325.pdf> accessed 28 May 2025.
- Council of Europe, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data" (2005) <https://rm.coe.int/16806840ba> accessed 28 May 2025.
- Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [Ets No. 108] Draft Explanatory Report (2016) <https://rm.coe.int/convention-for-the-protection-of-individuals-with-regard-to-automatic-/16806b6ec2> accessed 28 May 2025.
- Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data "Guidelines on Facial Recognition" (2021).
- Collinson P., "How an EU Gender Equality Ruling Widened Inequality" The Guardian (14 January 2017) <https://www.theguardian.com/money/blog/2017/jan/14/eu-gender-ruling-car-insurance-inequality-worse> accessed 28 May 2025.
- Consultative Committee on Convention 108, Guidelines on Facial Recognition 108 T-PD(2020)03rev4 5.
- Draghi M., Report for the EU Commission "The future of European competitiveness."
- ECtHR, "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention on the Prohibition of Discrimination" (31 August 2024).
- Engel C., Linhardt l., Schubert M., "Code Is Law: How COMPAS Affects the Way the Judiciary Handles the Risk of Recidivism" (2024) Artificial Intelligence and Law.
- European Council on Refugees and Exiles (ECRE), "Reforming EU Asylum Law: The Final Stage" (2023) <https://ecre.org/wp-content/uploads/2023/08/Policy-Parper-

Reforming-EU-Asylum-Law-the-Final-Stage-August-2023.pdf> accessed 28 May 2025.

- European Data protection Board (EDPB), Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR, Version 1.1 (2024) <https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-112024-use-facial-recognition-streamline_en> accessed 28 May 2025.

- EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement (2022) <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en> accessed 28 May 2025.

- EDPB "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default" Version 2.0 (2020).

- EDPB, 'Guidelines 3/2019 on processing of personal data through video devices' Version 2.0 (2020).

- EDPB 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak' (2020).

- 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)" (2021).

- EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022).

- EDPS (European Data Protection Supervisor), Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council Concerning the Visa Information System (VIS) and the Exchange of Data Between Member States on Short Stay-Visas (COM (2004)835 final).

- EDPS, "Opinion on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions" (2006/C 313/13).

- EDPS, “Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)” (2011).
- EDPS, “Reflection Paper on the Interoperability of Information Systems in the Area of Freedom, Security and Justice” (2017).
- EDPS “Guidelines 01/2025 on Pseudonymisation” (2025).
- European Digital Rights “European Commission adoption consultation: Artificial Intelligence Act Brussels” (2021) <https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf> accessed 28 May 2025.
- eu-LISA, “Single Programming Document 2024–2026” Document 2022-408 REV 4.
- eu-LISA, “Single Programming Document 2022–2024 European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice Single Programming Document 2022–2024 2020-323 Rev 2 (2021).
- eu-LISA, “Eurodac 2023 Annual Report December 2024” www.eulisa.europa.eu/Publications/Reports/Eurodac%20Statistics%20Report%202023.pdf.
- eu-LISA, “Technology Brief, Biometric Technology, Part 2. What Added Value Does Eu-Lisa Bring Through Biometrics?” (2024).
- eu-LISA “Enabling Seamless Travel to the European Union” (2022).
- eu-LISA ‘Biometric Technologies in Identity Management and Verification’ (2022).
- European Law Institute Guidelines on the Application of the Definition of an AI System in the AI Act: ELI Proposal for a Three-Factor Approach Response of the ELI to the EU Commission's Consultation (2024).
- Europol and ENISA Joint Statement “On lawful criminal investigation that respects 21st Century data protection” (2016)

- EU Commission, “Commission Staff Working Document Impact Assessment on establishing a framework for interoperability between EU information systems” SWD/2017/0473 final - 2017/0351 (COD).

- EU Commission, “Report from the Commission to the European Parliament and the Council on the State of Play of Preparations for the Full Implementation of the Interoperability Regulations in Accordance with Article 78(5) of Regulation (EU) 2019/817 and Article 74(5) of Regulation (EU) 2019/818” COM(2024) 293 final.

- EU Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Protecteu: A European Internal Security Strategy” com(2025) 148 final.

- European Parliament, Parliamentary question, 005624/2018 <https://www.europarl.europa.eu/doceo/document/E-8-2018-005624_EN.html> accessed 28 May 2025.

- European Court of Auditors, “Special Report No 20/2019: EU Information Systems Supporting Border Control – A Strong Tool, but More Focus Needed on Timely and Complete Data”.

- Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy (FIDELITY) <https://cordis.europa.eu/project/id/284862/factsheet> accessed 28 May 2025.

- Fundamental Rights Agency (FRA), “Facial recognition technology: fundamental rights considerations in the context of law enforcement” (2019).

- Fundamental Rights Agency (FRA), “Under Watchful Eyes – Biometrics, EU IT-systems and Fundamental Rights” (2018).

- FRA, “Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac” (2015).

- FRA, “Article 3 - Right to integrity of the person”, <https://fra.europa.eu/en/eu-charter/article/3-right-integrity-person> accessed 28 May 2025.

- FRA, “Opinions Biometrics”, <https://fra.europa.eu/en/content/fra-opinions-biometrics> accessed 28 May 2025.
- FRA, “Border Control at External Land Borders and Fundamental Rights – Practical Guidance” (2022).
- FRA, “Data Quality and Artificial Intelligence – Mitigating Bias and Error to Protect Fundamental Rights” (2019).
- FRA ‘Handbook on European data protection law - 2018 edition.’
- Frontex, Technology Foresight on Biometrics for the Future of Travel (European Border and Coast Guard Agency, 2022) www.frontex.europa.eu.
- Goldner Lang I., “Pushbacks against the Child’s Best Interests” VerfBlog, 2022/1/07, <https://verfassungsblog.de/pushbacks-against-the-childs-best-interests/> accessed 28 May 2025.
- Global Campus of Human Rights, <https://www.gchumanrights.org/preparedness/how-is-chatgpt-regulated-by-the-eu-ai-act-reflections-on-higher-education/#:~:text=ChatGPT%20does%20not%20classify%20as,chatGPT%20in%20their%20AI%20system> accessed 28 May 2025.
- Guide to the Case-Law of the of the European Court of Human Rights, Data protection, 2020 <https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0> accessed 28 May 2025.
- Grother P., others, “Face Recognition Vendor Test (FRVT) Part 7” (National Institute of Standards and Technology (US) 2021) <https://pages.nist.gov/frvt/reports/travel/frvt_travel_report.pdf> accessed 28 May 2025.
- Grother P., “Face Recognition Vendor Test (FRVT) Part 8” (National Institute of Standards and Technology 2022) <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8429.ipd.pdf> accessed 28 May 2025.

- Grother P., M Ngan M., Hanaoka K., “Face Recognition Vendor Test Part 3: Demographic Effects” (19 December 2019) NIST publication, 54 <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> accessed 28 May 2025.
- Hellenic Data Protection Authority (HDPA), Decision 35/2022 Ref. No. 1809.
- Hersey F., “Pakistani Political ‘Hecklers’ Threatened with Blocked Biometric ID, Bank Accounts” *BiometricUpdate.com* (August 22, 2022) <https://www.biometricupdate.com/202208/pakistani-political-hecklers-threatened-with-blocked-biometric-id-bank-accounts> accessed April 29, 2025.
- HRW, “New Evidence That Biometric Data Systems Imperil Afghans” (Human Rights Watch, March 30, 2022) <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans> accessed April 29, 2025.
- HRW, “UN Shared Rohingya Data Without Informed Consent” (Human Rights Watch, June 15, 2021) <https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent> accessed April 29, 2025.
- IEEE 2410-2021, IEEE Standard for Biometric Privacy <https://standards.ieee.org/ieee/2410/7746/> accessed 28 May 2025.
- ISO/IEC 2382-37:2022(en) Information technology — Vocabulary — Part 37: Biometrics <https://www.iso.org/committee/313770.html> accessed 28 May 2025.
- ISO/IEC 19795-10:2024(en) Information technology — Biometric performance testing and reporting Part 10: Quantifying biometric system performance variation across demographic groups.
- International Civil Aviation Organization (ICAO), Doc 9303, Machine Readable Travel Documents Part 1 — Introduction ISBN 978-92-9265-291-3 <https://www.icao.int/publications/Documents/9303_p1_cons_en.pdf> accessed 28 May 2025.
- Kashmir Hill, ‘Eight Months Pregnant and Arrested After False Facial Recognition Match” The New York Times 6 August 2023 <https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html> accessed 28 May 2025.

- Keung N., “Are These Two Photos of the Same Person? Canada’s Controversy over Asylum-Seekers and ‘Photo Matching’” *Toronto Star* (21 January 2022) <https://www.thestar.com/news/canada/are-these-two-photos-of-the-same-person-canada-s-controversy-over-asylum-seekers-and/article_2edca377-85ce-57af-9f40-4aff6cda8293.html> accessed 28 May 2025.

- Kollias F., “Suspicion Machines Methodology” (Lighthouse Reports, 6 March 2023) <https://www.lighthousereports.com/suspicion-machines-methodology/> accessed 28 May 2025.

- McLaughlin M., Castro D., “The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist”, Information Technology and Innovation Foundation | ITIF (January 27, 2020) <https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms> accessed 28 May 2025.

- Ngan ML, Grother P., “Face Recognition Vendor Test (FRVT) – Performance of Automated Gender Classification Algorithms” (NIST, April 20, 2015) <https://www.nist.gov/publications/face-recognition-vendor-test-frvt-performance-automated-gender-classification> accessed 28 May 2025.

- Niinistö S., Report for EU Commission “Safer Together Strengthening Europe’s Civilian and Military Preparedness and Readiness.”

- NIST (National Institute of Standards and Technology), “Face Technology Evaluations - FRTE/FATE” <https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate> accessed 28 May 2025.

- Note on interviews conducted in the course of the research. Expert interviews were held with representatives of Croatian Ministry of Interior and Croatian Data Protection Agency (AZOP). These interviews were semi-structured. Written questions were provided before the interview. A note on privacy and rights was also provided to the subjects. Interviews involved questions concerning the use of biometrics or processing of biometric data. Conducting the interviews was beforehand approved by the Ethics Committee of the Faculty of Law. The author expresses thanks to the experts who

participated, including to Anamarija Mladinić, Head of the Sector for EU, International Cooperation, and Legal Affairs at the Croatian Data Protection Authority (AZOP).

- Peers S., "Biometric Data and Data Protection Law: The CJEU Loses the Plot' EU Law Analysis (17 April 2015) <https://eulawanalysis.blogspot.com/2015/04/biometric-data-and-data-protection-law.html> accessed 28 May 2025.
- Pinker S., "The Stupidity of Dignity" (The New Republic, May 28, 2008).
- Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, <https://rm.coe.int/progress-report-on-the-application-of-the-principles-of-convention-108/1680744d81> accessed 28 May 2025.
- Rathgeb C, Breitinger F., Busch C., "Alignment-Free Cancelable Iris Biometric Templates Based on Adaptive Bloom Filters," 2013 International Conference on Biometrics (ICB) (IEEE 2013) https://doi.org/10.1109/icb.2013.6612976.
- Secure Access Control over Wide Area Network (SWAN) <https://www.ntnu.edu/iik/swan/publications> accessed 28 May 2025.
- Science for Humanity: Human Presence, Movement & Heartbeat Detection System (MDS) <https://s4h.be/wp-content/uploads/2020/12/Science-for-Humanity-Frontex-booklet.pdf>> accessed 28 May 2025.
- "Stop All the Clocks", a poem by WH Auden.
- TrUsted Revocable Biometric IdeNtitiEs (Turbine) <https://cordis.europa.eu/project/id/216339> .
- Thales's website, <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history> accessed 28 May 2025.
- Veale M., F. Zuiderveen Borgesius FZ, "Demystifying the Draft EU Artificial Intelligence Act" arXiv:2107.03721 https://doi.org/10.48550/arXiv.2107.03721.
- "Why Most Published iBorderCtrl Research Findings Are Likely to Be False" <https://iborderctrl.no/blog:ioannides>accessed 28 May 2025.

- Y Yang Y. et al., “Automated Decision-Making and Artificial Intelligence at European Borders and Their Risks for Human Rights” (*arXiv.org*, October 8, 2024) <https://arxiv.org/abs/2410.17278> accessed 28 May 2025.

Note on Author and Published Works

Matija Kontak graduated from the Faculty of Law in Zagreb. During his studies he participated in the Willem Vis Moot and in the work of the Law Clinic. After that, he obtained the title of Master of Laws (*cum laude*) at the Faculty of Law of Radboud University in the Netherlands. During his studies in the Netherlands, he participated in the Future Tech Law Moot and in the Lab for New Justice, which developed a cryptocurrency on a blockchain for settling legal disputes. As the best student in the Lab for New Justice, he received a paid internship at the legal technology company Jur AG. Since 2022, he has been living again in Croatia, in Zagreb, and works at the Faculty of Law in Zagreb as an assistant at the Department of European Public Law. He is a researcher and member of Algorithmic Fairness for Asylum Seekers and Refugees (AFAR) project and the Horizon project Protecting Irregular Migrants in Europe (PRIME).

Published papers:

- "Biometric Borders Envisaged by Frontex: Fundamental Rights in the Backseat" European papers, 9 (2024), 2; 621-640.
- "Eurodac, biometrija i algoritmi: utjecaj tehnologije na ljudska prava migranata" in *Migracije na rubu Europe: trendovi, politike i izazovi*, Klempić Bogadi, Sanja; Gregurović, Snježana; Mlinarić, Dubravka (ur.);Zagreb: Institut za istraživanje migracija, 2024. str. 117-128.
- "The Application of Public Policy and Public Security Reasons for Justifying Restrictions on Free Movement of Capital in the EU" Zagrebačka pravna revija, 10/2021 (2021), 2; 150-166;
- "Modern Tools to Lower the Costs of Disputes: Digitalisation and the New Venues of Online Dispute Resolution" Harmonius, 1/2021 (2021), 1; 113-132.
- "Evaluation of the EU Screening Mechanism and the Question of Reciprocity with China" , Croatian yearbook of European law & policy, 17/2021 (2021), 17; 203-235.