UNIVERSITA' COMMERCIALE "LUIGI BOCCONI"

PhD SCHOOL

PhD program in Legal Studies

Cycle: 37°

Disciplinary Field (code): IUS-08

Constitutional Safeguards in the Age of AI. A Study on the Fundamental Rights Impact Assessment of Facial Recognition Technology

Advisor: Prof. Oreste POLLICINO

PhD Thesis by

Federica PAOLUCCI

ID number: 3157480

Year 2025

A mia madre

AKNOWLEDGMENTS

Before delving into the core of this thesis, I wish to express my deepest gratitude. This PhD journey has marked one of the most challenging periods of my life, and I would not have been able to persevere without the unwavering support of each person mentioned here. My heartfelt thanks go to all of you.

My utmost gratitude goes to Professor Oreste Pollicino, whose energy, creativity, and vision constantly pushed me beyond my limits. His faith in me, especially when I lacked it in myself, was fundamental. I am also sincerely thankful to my reviewers, Professor Erik Longo and Professor Simona Demková, for taking the time to read my thesis and provide thoughtful guidance throughout the process. I am particularly indebted to Professor Marco Bassini and Professor Giovanni De Gregorio for their invaluable support and mentorship. Being part of their team has been one of the most enriching academic experiences of this journey. Professor Eleanor Spaventa deserves special thanks for her intellectual guidance, her dedication, and for encouraging me to broaden my understanding of the European fundamental rights framework. To the Constitutional Law group, in particular Professor Marta Cartabia, Professor Davide Paris, and Professor Davide Zecca, thank you for your constant inspiration, not only in research but also in your creativity and passion for teaching.

Nothing would have been possible without my family and friends. I am especially grateful to my brother Luca, my best friend and soulmate. Your calm, strength, and constant support have been my safe harbour. To my father and grandmother: people from the Marche region, reserved and discreet, yet never failing to offer unwavering support in times of hardship. Thank you to Stefano, for always believing in me.

A person is nothing without her friends, and I am truly lucky. In the darkest moments, I found not just colleagues, but true friends who brightened even the greyest Milanese days with coffee, glasses of wine, laughter, and tears. Each one has been an essential piece of this journey. I want to thank Marco, Umberto, Maria Antonia, Rosalba, Maria, Valeria, Flavia, and Pietro for their friendship.

I have not forgotten where I come from. I am deeply grateful to my non-academic friends, both old and new, who patiently listened to my thesis-induced breakdowns (and not only), before, during, and after. Special thanks to Carola, for being there even when I wasn't able to be myself; to Laura, for sharing meltdowns and moments of mutual chaos, with a touch of sprinkle; to Giorgia, for being a quiet and constant presence; to Mariangela and Elia, for the laughter and for helping me let go of the past; to Michele, for his unique and meaningful closeness; and to Hillary, for her lightness of spirit and for always seeing the good in people and things.

I am deeply grateful to Bocconi University for welcoming me and providing the strong wings I needed to carry out my research and this project in particular. My thanks extend to all the staff, especially Marta Menin.

This thesis, and everything I do, is dedicated to my mother, Mara, who taught me that kindness and gratitude matter more than anything else. She witnessed the beginning of this journey, but did not wait long enough to see its completion. I hope she would be proud.

TABLE OF CONTENT

TABLE OF CONTENT ..... **I**

ABSTRACT ..... **IV**

TABLE OF ABBREVIATIONS ..... **VI**

TABLE OF CASES ..... **VIII**

TABLE OF LEGISLATION AND OFFICIAL DOCUMENTS ..... **XVI**

I PART ..... **XXIV**

1. INTRODUCTION **1**

1.1 OBJECTIVES OF THE RESEARCH **1**

1.1.1 *BACKGROUND OF THE RESEARCH: FACIAL RECOGNITION TECHNOLOGY BETWEEN OLD AND NEW CHALLENGES* 1
1.1.2 CONSTITUTIONAL LAW IN THE AGE OF AI 3
1.1.3 OBJECTIVES AND RESEARCH QUESTIONS 9

1.2 METHODOLOGY **11**

1.2.1 BEHIND THE CHOICE OF FRT: A CASE STUDY IN RIGHTS AND RISKS 13
1.2.2 THE LEGAL FRAMEWORK 15
1.2.3 THE TERRITORIAL SCOPE 17
1.2.4 ELEMENTS OF INTERDISCIPLINARITY 17

1.3 STRUCTURE OF THE WORK **18**

1.3.1 PART ONE 18
1.3.2 PART TWO 19

2. THE REGULATION OF ARTIFICIAL INTELLIGENCE: **20**

AN EXISTENTIAL CHALLENGE **20**

2.1 INTRODUCTION **20**

2.2 WHAT IS AI? **24**

2.2.1 CONCEPTUAL FOUNDATIONS OF AI 26
2.2.2 WHAT AI IS NOT 28
2.2.3 TECHNICAL FOUNDATIONS 30
2.2.3.1 The 'souls' of AI *31*
2.2.3.2 Symbolic and sub-symbolic AI *32*
2.2.3.3 Machine learning and deep learning *33*
2.2.3.4 What about FRT? *36*

2.3 FROM AUTOMATION TO AUTONOMY **37**

2.3.1 THE POWER OF AUTONOMY: NEW UNPRECEDENTED CHALLENGES 43

2.4 THE ARTIFICIAL INTELLIGENCE ACT **49**

2.4.1 OBJECTIVES OF THE REGULATION: BETWEEN PRODUCT SAFETY AND FUNDAMENTAL RIGHTS 50
2.4.2 MATERIAL AND TERRITORIAL SCOPE 53
2.4.3 METHOD: THE RISK-BASED APPROACH 55
2.4.4 PROHIBITED RISK AI SYSTEMS 59
2.4.5 HIGH RISK AI SYSTEMS 60
2.4.6 LIMITED RISKS 65
2.4.7 REQUIREMENTS FOR HIGH-RISK SYSTEMS 66
2.4.8 OBLIGATIONS FOR HIGH-RISK SYSTEMS 72

2.4.9 OBLIGATIONS FOR PROVIDERS OF HIGH-RISK AI SYSTEMS 73
2.4.10 OBLIGATIONS FOR DEPLOYERS OF HIGH-RISK AI SYSTEMS 74
2.4.10.1 Fundamental Rights Impact Assessment (FRIA) *75*
2.4.11 HARMONISED STANDARDS 78
2.4.12 GOVERNANCE AND ENFORCEMENT 81
2.4 CONCLUSION 84
3. THE REGULATION OF FACIAL RECOGNITION TECHNOLOGY 87
3.1 INTRODUCTION 87
3.2 THE CONTEXT 89
3.2.1 LAW ENFORCEMENT USE OF FRT: A TAXONOMY 91
3.2.2 FROM TRADITIONAL FORMS OF SURVEILLANCE TO FRT: LOOKING FOR A NEW PARADIGM 94
3.3 THE TECHNICAL FRAMEWORK 99
3.4 THE FUEL OF FRT: BIOMETRIC DATA 103
3.4.1. SPECIAL CATEGORIES OF PERSONAL DATA: THE GDPR PARADIGM ON BIOMETRIC DATA 104
3.4.2. SPECIAL CATEGORIES OF PERSONAL DATA: THE LED PARADIGM ON BIOMETRIC DATA 108
3.4.3 NON-LAW ENFORCEMENT USE OF BIOMETRIC DATA: THE CASE OF THE DIGITAL IDENTITY WALLET 112
3.5 THE REGULATION OF FRT IN THE AI ACT 116
3.5.1 THE AI ACT LEX SPECIALIS 118
3.5.2 ISSUES AND DE IURE CONDITO *PERSPECTIVES* 124
3.6 TOWARD A COMPREHENSIVE LEGAL FRAMEWORK FOR FRT 128
3.6.1 THE GDPR FRAMEWORK 130
3.6.2 THE LED FRAMEWORK 132
3.6.3 THE AI ACT FRAMEWORK 135
3.6.4 INTEGRATED OBLIGATIONS ACROSS THE GDPR, LED, AND AI ACT 137
3.7 CONCLUSION 141
II PART 143
4. FUNDAMENTAL RIGHTS IMPACT ASSESSMENT 144
4.1 INTRODUCTION 144
4.2 A PREMISE: THE PROTECTION OF FUNDAMENTAL RIGHTS IN THE EU 148
4.2.1 THE HORIZONTAL EFFECT OF FUNDAMENTAL RIGHTS 153
4.3 IMPACT ASSESSMENTS AS VESSELS OF RISKS: A TAXONOMY 160
4.3.1 IMPACT ASSESSMENTS IN THE INTERNATIONAL CONTEXT 165
4.4 THE FUNDAMENTAL RIGHTS IMPACT ASSESSMENT 170
4.4.1 THE ACTORS 172
4.4.2 TIME AND MODALITIES 172
4.4.3 KEY ELEMENTS 173
4.4.4 PROCEDURAL OBLIGATIONS 174
4.4.5 DATA PROTECTION IMPACT ASSESSMENTS: FRIEND OR FOE? 175
4.4.6 IMPACT ASSESSMENTS: DRAWING PARALLELS 176
4.4.7 THE OTHER ASSESSMENTS UNDER THE AI ACT 180
4.4.8 CRITICAL ANALYSIS OF THE FRIA 184
4.5 MUCH ADO ABOUT METHODOLOGY 186
4.5.1 FRIA: BORROWING A METHODOLOGY? 191
4.5.2 UTILITY WITH THE AI ACT 195

4.6 CONCLUSION 197

5. THE FRIA IN PRACTICE: APPLYING A NORMATIVE FRAMEWORK TO FACIAL RECOGNITION 199

5.1 INTRODUCTION 199

5.2 FRIA: BUILDING A MODEL FOR FACIAL RECOGNITION TECHNOLOGY 202

5.2.1 ELABORATION OF THE MODEL 203
5.2.2 ALL RIGHTS ARE EQUAL, BUT SOME ARE MORE AT RISK 207

5.3 FRIA FOR FRT 209

5.3.1 FUNDAMENTAL RIGHT'S CHECKLIST 214
5.3.2 WHICH FUNDAMENTAL RIGHTS ARE AFFECTED? 217
5.3.2.1 Case analysis: Glukhin v. Russia – A practical application of FRIA 218

5.4. TEST: ART. 8 CFREU, DATA PROTECTION 224

5.4.1 CLUSTER 1: TRAINING AND MODELING – ARE THESE PERSONAL DATA? 230
5.4.2 CLUSTER 2: THE USE OF PUBLICLY AVAILABLE DATA 234
5.4.3 CLUSTER 3: DATA RETENTION AND ERASURE 238
5.4.3.1 The right to erasure: who wants to live forever? 240
5.4.3.2 Data retention: it's now or never? 244

5.4.4 CHILLING EFFECTS 249

5.5 CONCLUSION 253

6. EFFECTIVE REMEDIES: "WHATEVER IT TAKES" FOR THE PROTECTION OF FUNDAMENTAL RIGHTS 255

6.1 INTRODUCTION 255

6.2 LEGAL FRAMEWORK: THE RIGHT TO AN EFFECTIVE REMEDY 257

6.2.1 THE EUROPEAN LEGAL FRAMEWORK 258
6.2.1.1 Applicability of the right 261
6.2.1.2 Limitations 262
6.2.1.3 The role of MS in ensuring effective judicial protection 262

6.3 THE RIGHT TO AN EFFECTIVE REMEDY IN THE DIGITAL AGE 264

6.4 THE REMEDIES UNDER THE AI ACT 269

6.4.1 ANOTHER ONE BITES THE DUST? 270

6.5 AGENCY: *UBI SOCIETAS, IBI IUS?* 277

6.6 (JUDICIAL) AUTHORITY: *QUID IURIS?* 282

6.6.1 DIVERGING STANDARDS OF SCRUTINY 284
6.6.2 'IN SUBORDINE': AT LEAST A QUASI-JUDICIAL OVERSIGHT 288

6.7 "IT'S A THOUGH CALL: THEY ARE SO DIFFERENT": THE ITALIAN CASE .. 290

6.8 CONCLUSION 294

7. 297

CONCLUDING REMARKS 297

7.1 INTRODUCTION 297

7.2 *DE IURE CONDENDO*: A BLUEPRINT FOR THE FUTURE 300

REFERENCES 303

BIBLIOGRAPHY AND ONLINE RESOURCES 303

ABSTRACT

This thesis explores the regulation of Facial Recognition Technology (FRT) as a lens through which to examine the constitutional and fundamental rights challenges posed by Artificial Intelligence (AI). Positioned at the intersection of innovation and public authority, FRT is emblematic of the wider tensions AI generates between security imperatives and rights guarantees. Its deployment in law enforcement and public surveillance underscores acute risks to privacy, data protection, freedom of expression and assembly, and, crucially, access to effective remedies.

Central to this inquiry is the Fundamental Rights Impact Assessment (FRIA), introduced by Reg. (EU) 2024/1689, the Artificial Intelligence Act, as a mechanism for embedding rights considerations into the lifecycle of high-risk AI systems. This thesis conceptualises the FRIA not merely as a compliance obligation but as a normative tool capable of operationalising constitutional safeguards. Applied to the case of biometric systems, particularly FRT, the FRIA is shown to address structural risks such as algorithmic bias, surveillance overreach, and chilling effects on democratic participation. By linking *ex ante* legal analysis to context-specific harms, the FRIA model developed in this study promotes a shift from reactive to preventive governance, contributing to a thicker model of digital constitutionalism.

Through an in-depth review of the European Union's regulatory landscape, the thesis evaluates the interaction between the AI Act, the General Data Protection Regulation (GDPR), and the Law Enforcement Directive (LED). It underscores the fragmented and reactive nature of current frameworks, particularly in their ability to address the opacity, accountability, and societal impact of FRT. Case studies, in particular based on the case law of the Court of Justice of the European Union and of the European Court of Human Rights, and legal analysis reveal critical gaps in procedural safeguards, judicial oversight, and the provision of effective remedies for individuals affected by the deployment of biometric technologies.

Ultimately, the study argues that the governance of FRT reveals deeper tensions between EU harmonisation efforts and the procedural autonomy of Member States. These tensions are especially visible where jurisdictional boundaries are blurred and regulatory

fragmentation persists. While the AI Act's *lex specialis* provisions represent a step forward, their limited reach leaves unaddressed several of the systemic and rights-related concerns associated with biometric technologies. The thesis calls for a recalibrated regulatory approach, one that treats impact assessments not as bureaucratic checklists but as vehicles for reinforcing accountability, democratic legitimacy, and the substantive protection of fundamental rights.

Finally, by framing FRT as a litmus test for AI regulation, the thesis underscores its potential to propose a model for FRIA that eventually aims at balancing innovation and fundamental rights in the digital era. The findings contribute to the growing discourse on AI regulation by providing an in-depth examination of FRT as a unique lens for understanding the constitutional, regulatory, and societal dimensions of emerging technologies.

KEYWORDS: Facial recognition technology; Artificial Intelligence; AI Act; Biometric data; Privacy; Data protection; Fundamental Rights Impact Assessment (FRIA); Effective remedies; Constitutional law; Digital constitutionalism.

TABLE OF ABBREVIATIONS

ACHR	American Convention on Human Rights
ADM	Automated Decision Making
AEPD	Agencia Española de Protección de Datos
AG	Advocate General
AI	Artificial Intelligence
AIA	Canada's Algorithmic Impact Assessment
CAI	Committee on Artificial Intelligence
CCTV	Closed Circuit Television
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
DG-CNECT	Directorate-General for Communications Networks, Content and Technology
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DSA	Digital Services Act
EC	European Commission
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union

FRA	European Agency for Fundamental Rights
FRAIA	Fundamental Rights and Algorithms Impact Assessment (the Netherlands)
FRIA	Fundamental Rights Impact Assessment
FRT	Facial Recognition Technology
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
HLEG	High-Level Expert Group on Artificial Intelligence
HRIA	Human Rights Impact Assessment
HUDERIA	Human Rights Democracy and Rule of Law Impact Assessment
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commission Officer
LED	Law Enforcement Directive
ML	Machine Learning
MS	Member States
OECD	Organisation for Economic Co-operation and Development
QMS	Quality Management System
RBI	Real time Biometric Identification Systems
SA	Supervisory Authority
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights

UK	United Kingdom
UN	United Nations
US	United States of America

TABLE OF CASES

CASES

Court of Justice of the European Union:

ECJ*, Erich Stauder v City of Ulm,* Case 29/69, 12 November 1969.

ECJ, Comet *BV v Produktschap voor Siergewassen,* C- 45/76, 6 December 1976.

ECJ, ewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland, C-33/76, 6 December 1976.

ECJ, Comet *BV v Produktschap voor Siergewassen,* C- 45/76, 6 December 1976.
ECJ*, Erich Stauder v City of Ulm,* Case 29/69, 12 November 1969.

ECJ, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermitte,* C-11/70, 17 December 1970.

ECJ*, J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities,* C-4/73, 14 May 1974.

ECJ, *B.N.O. Walrave and L.J.N. Koch v Association Union cycliste internationale, Koninklijke Nederlandsche Wielren Unie and Federación Española Ciclismo,* C-36/74, 12 December 1974.

ECJ, *Gabrielle Defrenne v Société anonyme belge de navigation aérienne Sabena,* C-43/75, 8 April 1976.

ECJ, *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen*, Case 14/83, 10 April 1984.

ECJ, *Andrea Francovich and Danila Bonifaci and others v Italian Republic,* Joined cases C-6/90 and C-9/90, 19 November 1991.

ECJ, *Pierre Corbiau v Administration des Contributions*, C-24/92, 16 February 1993.

CJEU (GC), *Werner Mangold v Rüdiger Helm,* C-144/04, 22 November 2005.

CJEU (GC), *Graham J. Wilson v Ordre des avocats du barreau de Luxembourg,* C-506/04, 19 September 2006.

CJEU (GC), *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, Joined cases C-402/05 P and C-415/05, 3 September 20028.

CJEU (GC), *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy,* Case C-73/07, 16 December 2008.

CJEU (4th Sec.), *Rosalba Alassini v Telecom Italia SpA, Filomena Califano v Wind SpA, Lucia Anna Giorgia Iacono v Telecom Italia SpA, and Multiservice Srl v Telecom Italia SpA,* Joined cases C-317/08, C-318/08, C-319/08 and C-320/08, 18 March 2010.

CJEU (GC), *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen,* Joined Cases C-92/09 and C-93/09, 9 November 2010.

CJEU, (GC), *Stefano Melloni v Ministerio Fiscal,* C-399/11, 26 February 2013.

CJEU (Fourth Chamber), C-291/12, *Michael Schwarz v Stadt Bochum*, 17 October 2013.

CGUE, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, 13 May 2024.

CJEU (GC), *Digital Rights Ireland and Seitlinger and Others*, Joined C-293/12 and C- 594/12, 8 April 2014.

CJEU (Third Chamber), *Smaranda Bara and Others v Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF*), C-201/14*,* 1 October 2015.

CJEU (GC), *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14, 6 October 2015.

CJEU (GC), *European Parliament and European Commission v Council of the European Union*, Joined Cases C-124 and 125/13, 1 December 2015.

CJEU (GC), Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen, Joined Cases C-404/15 and C-659/15 PPU, 5 April 2016.

CJEU (GC), *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others,* 21 Joined C-203/15 and C-698/15, 21 December 2016.

CEJU (Third Chamber), *Peter Puškár contro Finančné riaditeľstvo Slovenskej republiky e Kriminálny úrad finančnej správy,* C-73/16, 2017.

CJEU (Grand Chamber), *Associação Sindical dos Juízes Portugueses v Tribunal de Contas,* Case C-64/16, 27 February 2018.

CJEU (GC), *IR v JQ.,* C-68/17, 11 September 2018.

CJEU (GC), *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.,* C-414/16, 17 April 2018.

CJEU (GC), *GC and Others*, C-136/17, 24 September 2019.

CJEU (GC), *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés,* C-507/2017, 24 September 2019.

CJEU (GC), *Miasto Łowicz and Prokurator Generalny*, Joined Cases C-558/18 and C-563/18, 26 March 2020.

CJEU (GC), *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others,* C-623/17, 6 October 2020.

CJEU (GC), *La Quadrature du Net and Others v Premier ministre and Others*, Joined C-511/18, C-512/18, and C-520/18, 6 October 2020.

CJEU (GC), *Commission v. Poland (Disciplinary regime for judges)*, Case C-791/19, 15 July 2021.

CJEU (Opinion AG), *Ligue des droits humains ASBL v Conseil des ministers,* C-817/19, 27 January 2022.

CJEU (GC), *Ligue des droits humains ASBL v Conseil des ministers,* C-817/19, 21 June 2022.

CJEU (Opinion AG), *Ministerstvo na vatreshnite raboti*, C-205/21, 30 June 2022.

CJEU (Opinion AG), *TU, RE v Google LLC,* C-460/20, 7 April 2022.

CJEU (GC), *TU, RE v Google LLC,* C-460/20, 8 December 2022.

CJEU (Fifth Chamber), C-205/2021, *V.S. v. Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost,* 26 January 2023.

CJEU (GC), *Meta Platforms Inc and Others v Bundeskartellamt,* C-252/21, 4 July 2023.

CJEU (I Chamber), *OQ v Land Hessen*, C-634/21, 7 December 2023.

CJEU (GC), C-118/2022, *NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti*, 30 January 2024.

CJEU (GC), *K.L. v X sp. z o.o.,* C-715/2020, 20 February 2024.

CJEU (GC), *RU v Landeshauptstadt Wiesbaden*, no. C-61/2022, 21 March 2024.

CJEU (GC), *La Quadrature du Net (et al.) v. Premier ministre et Ministre de la Culture,* C-470/21, 30 April 2024.

CJEU (GC), *C.G. v Bezirkshauptmannschaft Landeck,* C- 548/2021*,* 4 October 2024.

Colombia:

República de Colombia Corte Constitucional, Ruling T-323/2024.

European Court of Human Rights:

ECtHR [GC], *Klass and Others v Germany*, App no. 5029/71, 6 September 1978.

ECtHR [GC], *X and Y v the Netherlands*, n. 8978/80, 26 March 1985.

ECtHR [GC], *Huvig v. France*, No. 11105/84, 24 April 1990.

ECtHR [GC], *Rotaru v. Romania*, no. 28341/95, 4 May 2000.

ECtHR [IV Sec.,], *Kennedy v. UK*, no. 26839/05, 18 May 2010.

ECtHR [GC], *S. and Marper v. the United Kingdom*, nos. 30562/04 and 30566/04, 4 December 2008.

ECtHR [GC], *El-Masri v. "the former Yugoslav Republic of Macedonia",* no. 39630/09, 13 December 2012.

ECtHR [GC], *Zakharov v. Russia*, no. 47143/ 06, 4 December 2015.

ECtHR [III Sec.], *Novikova and Others v. Russia*, nos. 25501/07, 26 April 2016.

ECtHR [IV Sec.], *Szabò and Vissy v. Hungary*, no. 37138/ 14, 12 January 2016.

ECtHR [I Sec.], *Gaughran v. The United Kingdom*, App no 45245/15, 3 June 2020.

ECtHR (GC), *Big Brother Watch v. U.K.*, App. no. 58170/13, 62322/14, 24960/15, 25 May 2021.

ECtHR [GC], *Centrum för Rättvisa v. Sweden*, no. 35252/08, 25 May 2021.

ECtHR [I Sec.], *Biliński v. Poland*, Application No. 13278/20, 30 April 2022.

ECtHR [GC], *Synakiewicz and others v. Poland,* Application Nos. 46453/21, 8076/22, 9988/22, 15928/22, 23 May 2022.

ECtHR [III Sec.] *Glukhin v. Russia,* no. 11519/20, 2023, 4 July 2023.

ECtHR [III Sec.], *Podchasov v. Russia,* no.33696/19, 21 June 2021.

France

Trib. Adm. de Marseille, n. 1901249, 3 February 2020.

Germany

Bundesverfassungsgericht, Beschluss vom 01. Juni 2006–1 BvR 2293/03 (Federal Constitutional Court, Decision of 1 June 2006–1 BvR 2293/03).

Italy

Italian Constitutional Court, no. 34 of 1973.

Italian Constitutional Court, no. 170 of 1984.

Italian Constitutional Court, no. 232 of 1989.

Italian Constitutional Court, no. 348 of 2007.

Italian Constitutional Court, no. 349 of 2007.

Italian Cost. Court, no. 336 of 2008.

Italian Constitutional Court, no. 269 of 2017.

Italian Constitutional Court, no. 170 of 2023.

Italian Council of State, Third Section, decision no. 7891 of November 25, 2021.

Supreme Court of Cassation (SS. UU.), no. 2737/2006, 29 novembre 2005.

Supreme Court of Cassation (SS. UU.), no. 30347/2007, 12 luglio 2007.

United Kingdom:

Court of Appeal, The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058, 11 August 2020.

United States of America:

Katz v United States 389 US 347 (1967).

SANCTIONS

Federal Trade Commission

Federal Trade Commission, Everalbum, Inc., also d/b/a Ever and Paravision, decision and order docket no. c-4743/2021.

French Data Protection Authority

CNIL, Deliberation of the restricted committee N° SAN-2022-019 of 17 October 2022.

Information Commission Officer (ICO)

Information Commission Officer (ICO), Order against Serco Limited UK, 23 February 2024.

Italian Data Protection Authority

Italian DPA (Garante), Order no. 551/2017, 21 December 2017, doc. no. 7496252.

Italian DPA, Injunction Order against Clearview AI - 10 February 2022, Register of Measures, No. 50 of 10 February 2022.

Italian DPA, 30 March 2023, Register of Measures, No. 112 of 30 March 2023.

Italian DPA, Measure of 11 January 2024, Register of Measures, No. 5 of 11 January 2024.

Italian DPA, Measure of 22 February 2024, Decisions no. 105, 106, 107, 108 and 109.

Italian DPA, Register of Measures, No. 755 of 2 November 2024, doc. web no. 10085455.

Swedish Data Protection Authority

IMY (Swedish DPA), DI-2020-2719, 11 February 2021.

TABLE OF LEGISLATION AND OFFICIAL DOCUMENTS

LEGISLATION

European Union:

Charter of Fundamental Rights of the European Union OJ C 364/1 2000.

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

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, 2021 O.J. (L 172) 79.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC.

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

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) 2018/1139 and (EU)

2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

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.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, no longer in force.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment, later amended by Directive 2014/52/EU of the European Parliament and of the Council of 16 April 2014, amending Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment.

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.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, 2018 O.J. (L 303) 69.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC.

Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (Eu) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final.

Council of Europe:

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Convention 108+ for the protection of individuals with regard to the processing of personal data, 2018.

Council of Europe (CoE), Framework Convention on artificial intelligence, human rights, democracy and the rule of law, published on 17 May 2024, Council of Europe Treaty Series - No. 225.

Italy

Law No. 137 of 9 October 2023, which converted into law, with amendments, the Decree-Law No. 105 of 10 August 2023.

Provisions and powers delegated to the Government regarding artificial intelligence (1146-A), 19 marzo 2025 N. 1 (DDL on Artificial Intelligence).

OFFICIAL DOCUMENTS

European Union:

Commission of the European Communities, Green Paper Promoting a European Framework for Corporate Social Responsibility, 2001.

Communication from the Commission Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM/2010/0573 final. The quotes come from the same text.

Commission Staff Working Paper. Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC(2011) 567 final. The paper is also part of the Smart Regulation in the European Union, COM(2010) 543 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation: Joining forces to make better laws, COM/2021/219 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strategy to strengthen the application of the Charter of Fundamental Rights in the EU, Brussels, 2.12.2020.

European Commission, 'Communication on Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe' COM (2016) 288 final, 5 (hereafter European Commission, 'Communication on Online Platforms and the Digital Single Market').

European Commission Proposal for a 'Regulation of the European Parliament and of the Council laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers' COM(2010) 83 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', Brussels, 2.12.2020, COM(2020) 711 final.

European Commission, 'White Paper on Artificial Intelligence: a European approach to excellence and trust', 19 February 2020.

European Commission, 'ANNEX to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)', published 4 February 2025, C(2025) 884 final.

European Parliament, Directorate General for Internal Policies, Citizen's Rights and Constitutional Affairs, *Justice, Freedom and Security, Implementation of the EU Charter of Fundamental Rights and its impact on EU Home Affairs Agencies, Frontex, Europol and the European Asylum Support Office,* + 2011.

European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for an Artificial Intelligence Act, COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), Amendment 168.

European Parliament (2024) 'Harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, Proposal for a regulation', in the Draft report curated by Brando Benifei and Dragoş Tudorache, IMCO-LIBE committees, 13.6.2022.

European Parliament (2024) Briefing Updating the European digital identity framework; Explanatory Memorandum of the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (Eu) No 910/2014.

Explanatory Memorandum to the Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, {Sec(2021) 167 Final} - {Swd(2021) 84 Final} - {Swd(2021) 85 Final}.

Explanatory Memorandum published within the proposal for a Regulation of the European Parliament and of the Council, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21.4.2021, COM(2021) 206 final.

Mario Draghi, 'The Future of European Competitiveness' (*European Commission*, 2024).

European Data Protection Board:

EDPB, ‘Guidelines 3/2019 on processing of personal data through video devices’, 29 January 2020.

EDPB, ‘Guidelines 07/2020 on the concepts of controller and processor in the GDPR’, 7 July 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, 2021.

EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26 April 2023.

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), 24 May 2024.

EDPB, ‘Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models’, 17 December 2024.

Council of Europe:

Committee on Artificial Intelligence (CAI), ‘Outline Of HUDERIA Risk And Impact Assessment Methodology’, CAI-BU(2022)03, 17 May 2022.

Committee on Artificial Intelligence (CAI), ‘Methodology for the Risk and Impact Assessment of Artificial Intelligence Systems from the Point of View of Human Rights, Democracy and the Rule of Law (HUDERIA Methodology)’, Strasbourg, 28 November 2024, CAI(2024)16rev2.

Italian DPA:

Italian Data Protection Authority (DPA), ‘Guidelines on Biometric Recognition and Graphometric Signature Annex A to the Garante’s Order of 12 November 2014’ (2014).

European Agency for Fundamental Rights (FRA):

European Agency for Fundamental Rights (FRA), 'Challenges and opportunities for the implementation of the Charter of Fundamental Rights Opinion of the European Union Agency for Fundamental Rights', Opinion 4/2018, 24 September 2018.

European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019.

Fundamental Rights Agency and Council of Europe, *Fundamental rights of refugees, asylum applicants and migrants at the European borders*, 2020.

European Agency for Fundamental Rights (FRA), 'Getting the Future Right – Artificial Intelligence and Fundamental Rights,' 2020.

European Union Agency for Fundamental Rights (FRA), 'Bias in algorithms - Artificial intelligence and discrimination', 2022.

European Agency for Fundamental Rights, 'GDPR in practice – Experiences of data protection authorities', 2024.

Future of privacy forum:

Future of Privacy Forum, 'AI Governance behing the Scenes. Emerging Practices for AI Impact Assessments', 2024.

OECD:

Organization for Economic Co-operation and Development (OECD), AI Principles, 2019.

National Institute of Standards and Technology:

NIST, 'Face Recognition Technology Evaluation (FRTE)', 2024.

United Kingdom:

ICO, ‘Data Protection Impact Assessment Canva’, 28.11.2023.

United Nations:

United Nations High Commissioner for Human Rights, ‘Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests’, 24 June 2020, UN Doc. A/HRC/44/24.

United Nations Human Rights Office of the High Commissioner, ‘Taxonomy of Human Rights Risks Connected to Generative AI Supplement to B-Tech’s Foundational Paper on the Responsible Development and Deployment of Generative AI’, 2024.

Working Party 29:

Working Party 29, ‘Opinion 4/2007’, WP136 (2007).

WP 29, ‘Opinion 1/2010 on the concepts of “controller” and “processor”’, 00264/10/EN, WP 169, 16 February 2010.

WP29, ‘Advice paper on special categories of data (“sensitive data”)’ (2011).

Working Group 29, ‘Opinion 3/2012 on developments of biometric technologies’, 27 April 2012, 00720/12/IT WP193.

Working Party Article 29, ‘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’ (4 October 2017).

I PART

1. INTRODUCTION

SUMMARY: 1.1 Objectives of the research; 1.1.1 Background of the research: facial recognition technology between old and new challenges; 1.1.2 Constitutional law in the age of AI; 1.1.3 Objectives and research questions. – 1.2 Methodology; 1.2.1 Behind the choice of FRT: A case study in rights and risks; 1.2.2 The legal framework; 1.2.3 The territorial scope; 1.2.4 Elements of interdisciplinarity. – 1.3 Structure of the work; 1.3.1 Part one; 1.3.2 Part two.

1.1 Objectives of the research

1.1.1 *Background of the research: facial recognition technology between old and new* challenges

Facial recognition technology (FRT) represents one of the most contentious applications of artificial intelligence (AI). By enabling the identification of individuals through the automated processing of biometric data, FRT collapses the boundaries between the body and data, the private and the public, the visible and the surveilled.[1] Its integration into law enforcement practices does not merely raise issues of legality or proportionality: it unsettles the foundational principles of constitutional democracy, i.e., accountability, individual autonomy, and the limits of state power. [2]

This thesis investigates these transformations by examining the deployment of FRT in public spaces as a lens through which to analyse how AI reconfigures the exercise of power in contemporary society.[3] It engages with a broader shift identified by scholars such as Paul Nemitz as the "the age of AI", "in which high technology increasingly colonises every aspect of life".[4]

At such turn in society and history, decisions with legal consequences are increasingly delegated to AI systems. This shift is not neutral. It institutionalises new asymmetries of knowledge and control and displaces the normative architecture through which democratic orders have traditionally mediated authority.

---

[1] European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019.

[2] The topic will be further expanded in Chapter 3, para. §3.2.1.

[3] Oreste Pollicino, 'Regolazione e Innovazione Tecnologica Nell'"ordinamento Della Rete"' [2025] Rivista AIC 1.

[4] Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180089.

Constitutional law, at its core, exists to constrain power and secure fundamental rights through principles of legality, transparency, and redress. [5] It establishes the boundaries within which power, whether wielded by the state, corporations, or other actors, can be exercised, ensuring that it does not infringe upon individual rights or the principle of democracy.[6] Yet technologies like FRT challenge its operative assumptions. They obscure causal chains of decision-making, enable preventive forms of control, and render oversight reactive rather than anticipatory.[7] This thesis argues that legal systems must confront these structural shifts by reimagining the tools available to govern high-risk AI. In this context, the Fundamental Rights Impact Assessment (FRIA), introduced by the Reg. (EU) 2024/1689, Artificial Intelligence Act (AI Act, hereafter),[8] is not simply a procedural innovation it is a potential site for constitutional resistance, as will be dissected in the following pages.

While there is a growing body of literature examining the intersection of constitutional law and private powers in cyberspace, what is increasingly referred to as 'digital constitutionalism',[9] this research shifts the focus to public authority and the specific responsibilities of state actors in the governance and use of digital technologies.[10]

[5] Oreste Pollicino, 'Potere Digitale' in Marta Cartabia and Marco Ruotolo (eds), *Potere e Costituzione. Enciclopedia del diritto: i tematici* (Treccani 2023).

[6] Annibale Carena, 'Le Nuove Tendenze Del Diritto Costituzionale' [1931] Annali di scienze politiche 248.

[7] Oreste Pollicino and Pietro Dunn, *Intelligenza Artificiale e Disinformazione* (Egea 2024).

[8] 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) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

[9] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Bloomsbury Publishing 2021); Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022); Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2022); Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' [2021] International Journal of Constitutional Law; Giovanni De Gregorio, 'The Normative Power of Artificial Intelligence' (2023) 30 Indiana Law Journal; Francisco de Abreu Duarte, Giovanni De Gregorio and Angelo Golia, 'Perspectives on Digital Constitutionalism' (2023) ; Angelo Golia jr, 'The Contribution of Societal Constitutionalism to the Legal Theory of Digital Society: Framing and Perspectives' [2024] Diritto pubblico.

[10] Without downplaying or trivialising the consequences of the private sector's control over these technologies – an issue more closely tied to the development of AI itself – the role of the state is central in determining how and when these systems are implemented and introduced to the market. This research focuses precisely on these decisions, examining how the deployment of AI in specific contexts must occur within a framework of non-negotiable guarantees to prevent violations of rights. It is important to emphasize that these are decisions only the state – or more specifically, the legislator – can make, taking responsibility for such choices while acting following the law, respecting the established constitutional guarantees, and reinforcing such safeguards where necessary.

This is because the adoption of advanced AI systems, such as FRT, by public authorities requires strengthened constitutional scrutiny to ensure these technologies do not undermine fundamental rights, the rule of law, or democratic accountability. To stay true to its mission of constraining power and safeguarding fundamental rights, constitutional law must now adapt to the challenges posed by automated systems, which increasingly mediate decisions and interactions between individuals and institutions.[11]

States, therefore, play a pivotal role in striking a delicate balance between harnessing the potential of such technologies and upholding the right to privacy and other fundamental rights, especially when pervasive technologies like FRT are in place.[12]

On these premises, this thesis adopts FRT as a lens through which broader governance challenges were explored within the EU's regulatory framework.[13] By critically analysing the regulation of FRT under the AI Act and related legal instruments, it evaluates whether current safeguards sufficiently address the risks posed by such systems while balancing innovation with fundamental rights. Situating FRT as both a technological and constitutional issue, this thesis contributes to the ongoing discourse on responsible AI governance that upholds democracy, the rule of law, and fundamental rights.

1.1.2 Constitutional law in the age of AI

What was once regarded as a speculative or even dystopian concern has now become a pressing issue in the realm of legal governance.

The advent of AI in almost every aspect of human life might open a 'new cycle of constitutionalism'[14] aimed at creating a balance between competing strengths and powers, especially those of the public sector, which are further amplified by the use of this technology. AI's integration into critical domains, e.g. law enforcement, compels constitutional law to reassess the protection of fundamental rights. AI technologies such

[11] Erik Longo, *Giustizia Digitale e Costituzione: Riflessioni Sulla Trasformazione Tecnica Della Funzione Giurisdizionale* (FrancoAngeli 2023).

[12] European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', id.

[13] Arya Priya, 'Case Study Methodology of Qualitative Research: Key Attributes and Navigating the Conundrums in Its Application' (2021) 70 Sociological Bulletin 94.

[14] As a general remark and a methodological note, the reference to the cycle of constitutionalism is to be found in Giuseppe Morbidelli, 'La Costituzione' in Lucio Pegoraro and others, *Diritto pubblico comparato* (G Giappichelli Editore 2016). Nonetheless, Pollicino used the framework of phases and cycles to describe the evolution of regulatory and governance approaches towards digital regulations. Specifically, Oreste Pollicino, 'Potere Digitale', *Potere e Costituzione* (Treccani 2023).

as biometric identification, automated decision-making, and surveillance shift this constitutional focus, posing new and unprecedented challenges in the balancing of powers and rights.[15] Thus, like other disruptive technologies before it, AI has transitioned from being governed by a liberal, innovation-first regulatory approach to one that demands significant oversight and control. However, unlike previous technological advancements, this shift has occurred at an unprecedented speed.[16]

Furthermore, the rapid integration of AI into both public and private sectors has left little room for reactive legislation, forcing lawmakers to act preemptively. In contrast to other fields where regulation lagged behind widespread adoption, AI regulation has had to evolve in real time, especially as its applications in surveillance and decision-making have triggered immediate concerns about civil liberties.[17]

Thus, the purpose of this section is to illustrate why constitutional law plays a pivotal role in shaping the societal impact of AI. Indeed, constitutional law plays a pivotal role in limiting the exercise of power and ensuring the protection of fundamental rights within a democratic society.[18] Its primary function is to set the boundaries within which political and governmental powers can operate, ensuring that they remain accountable to the people and cannot infringe upon individual liberties.[19]

This principle is deeply rooted in the liberal revolutions of the 18th century, where thinkers like John Locke and Montesquieu advocated for the separation of powers and the establishment of legal limits on state authority.[20] The foundational documents of this era, such as the U.S. Constitution and the Declaration of the Rights of Man and of the

[15] Els J Kindt, 'The Criteria for the Correct "Balancing of Rights"' in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013).

[16] Nathalie A Smuha, 'From a "Race to AI" to a "Race to AI Regulation": Regulatory Competition for Artificial Intelligence' (2021) 13 Law, Innovation and Technology 57.

[17] See Section 2.2.2.

[18] Dieter Grimm, 'Conditions for the Emergence and Effectiveness of Modern Constitutionalism' in Dieter Grimm (ed), *Constitutionalism: Past, Present, and Future* (Oxford University Press 2016) <https://doi.org/10.1093/acprof:oso/9780198766124.003.0002> accessed 21 September 2024.

[19] Cf. in particular, Cesare Pinelli, 'Legal Certainty and the Tasks of Jurists' [2019] Diritto pubblico; Roberto Bin and Giovanni Pitruzzella, *Diritto Costituzionale* (Giappichelli 2015).

[20] "The end of law is not to abolish or restrain, but to preserve and enlarge freedom. For in all the states of created beings capable of laws, where there is no law, there is no freedom. For liberty is to be free from restraint and violence from others; which cannot be where there is no law: and is not, as we are told, a liberty for every man to do what he lists. But a liberty to dispose and order freely as he lists his person, actions, possessions, and his whole property within the allowance of those laws under which he is, and therein not to be subject to the arbitrary will of another, but freely follow his own", John Locke, *Due trattati sul governo e altri scritti politici / di J. Locke. Patriarca / di R. Filmer ; a cura di L. Pareyson* (3. ed. accresciuta, UTET 1982).

Citizen, codified the idea that power must be subject to legal constraints to prevent tyranny and authoritarianism.[21]

In the course of the 20th century, constitutional law further evolved to provide the necessary legal frameworks that ensured political power remained an emanation of the sovereign people, rather than an unchecked force that could operate with impunity.[22] It is within this tradition that constitutional law has continued to function as the guardian of democratic values and individual freedoms, ensuring that no authority, whether public or private, can overstep its bounds without facing legal scrutiny.[23] Importantly, constitutional law is not static; it adapts to meet new challenges as societies evolve.[24] Historically, this has included addressing the rise of supra-national powers,[25] mass communication, and the expansion of global trade. Today, its role extends beyond limiting state power to also curbing the growing influence of private entities, particularly in the digital age, where technological advancements blur the traditional boundaries between public and private authority.[26]

In this context, constitutional law functions as both a shield and a guide. It shields individuals and communities from the overreach of both governmental and non-governmental actors, and it provides a framework for integrating emerging technologies, like AI, into democratic societies without compromising fundamental rights. This dual role is vital in a world where AI technologies introduce unprecedented forms of power that transcend traditional governance structures. As emphasized in scholarly discourse, constitutional law must ensure that these technologies operate within the principles of transparency, accountability, and the rule of law.[27]

---

[21] Giuseppe Franco Ferrari, *I diritti nel costituzionalismo globale: luci e ombre / Giuseppe Franco Ferrari* (Prima edizione pubblicata in Italia, Mucchi Editore 2023); William Schabas and United Nations General Assembly, *The Universal Declaration of Human Rights: The Travaux Préparatoires / [Edited by] William A. Schabas, OC MRIA.* (1st ed., University Press 2013).

[22] 'Lo Stato', in Roberto Bin, *Diritto costituzionale / Roberto Bin, Giovanni Pitruzzella* (Ventitreesima edizione, G Giappichelli 2022).

[23] Marta Cartabia, 'Prefazione', *I diritti in azione* (Società editrice il Mulino, Spa 2009).

[24] Ex multis, Gunther Teubner, Constitutional Fragments: Societal Constitutionalism and Globalization (1st edn, OUP Oxford 2012); Tania Groppi, Menopeggio: La democrazia costituzionale nel XXI secolo / Tania Groppi. (Società editrice il Mulino Spa 2020).

[25] Giuseppe Martinico and Oreste Pollicino, *The Interaction Between Europe's Legal Systems: Judicial Dialogue and the Creation of Supranational Laws* (Edward Elgar 2012).

[26] Oreste Pollicino, 'The Quadrangular Shape of the Geometry of Digital Power(s) and the Move towards a Procedural Digital Constitutionalism' (2023) 29 European Law Journal; De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (n 5).

[27] Marta Cartabia, *I diritti in azione: Universalità e pluralismo dei diritti fondamentali nelle Corti europee* (Società editrice il Mulino 2009); Augusto Barbera, 'Ordinamento Costituzionale e Carte Costituzionali'

As anticipated, AI presents novel and complex challenges that amplify the very dangers constitutional law has always sought to prevent: the unchecked use of power and the potential for abuse. In this context, AI introduces unprecedented forms of decision-making and control that operate autonomously or semi-autonomously, often without transparency or accountability, and that shortens the distance between citizens and the State.[28]

This peculiarity has often been described in the literature using metaphors like the "panopticon," resembling the surveillance structure envisioned by Jeremy Bentham, where individuals are constantly monitored without knowing when or by whom they are being watched.[29] Another metaphor, popularized during the COVID-19 pandemic,[30] is the concept of the "Age of Surveillance Capitalism",[31] which refers to the commodification of personal data by large corporations and the use of surveillance to predict and influence behaviour. However, these metaphors, while insightful, are somewhat partial in their scope. Both the "panopticon" and "surveillance capitalism" emphasize the unilateral nature of observation, where power is concentrated in a singular entity, and individuals are passive subjects being watched. In contrast, with AI, the dynamics of surveillance are far more complex and decentralised.[32]

AI systems not only monitor but also actively interact with individuals, through predictive algorithms, recommendations, and decision-making processes. The relationship is no longer one-directional; individuals unwittingly participate in their surveillance by providing data through daily interactions with AI-driven platforms, which

[2010] Quaderni costituzionali; Antonio Ruggeri, 'Carte Internazionali Dei Diritti, Costituzione Europea, Costituzione Nazionale: Prospettive Di Ricomposizione Delle Fonti in Sistema' (2007).

[28] Andrea Simoncini and Samir Suweis, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale' [2019] Rivista di filosofia del diritto 87.

[29] Jeremy Bentham, *Panopticon o La Casa d'ispezione* (Marsilio 1997); Thomas McMullan, 'What Does the Panopticon Mean in the Age of Digital Surveillance?' *The Guardian* (23 July 2015) <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham> accessed 3 May 2020.

[30] For an analysis of the specific matters that the global pandemic provoked by the COVID-19 virus, see Arianna Vedaschi and Chiara Graziani, 'New Dynamics of the "Post-COVID-19 Era": A Legal Conundrum' (2023) 24 German law journal 1612.

[31] "Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data", Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019* (Profile Books 2019).

[32] Frank Pasquale, 'Watching (and Improving) the Watchers', *The black box society. The secret algorithms that control money and information.* (Harvard University Press 2015).

then use that data to inform and influence future behaviours and patterns.[33] This mutual entanglement of humans and AI systems complicates the traditional "watcher" and "watched" dynamic, making it less about observation alone and more about the co-creation of control and influence in the digital ecosystem.[34]

This metaphor[35] has been used to highlight the pervasive and invisible control that AI technologies, particularly in surveillance and data monitoring, can exert over individuals, creating a system where power is centralized, and privacy is significantly diminished. Specifically, there is the risk of what may be described as a new form of digital authoritarianism, where control over information, services, and even legal outcomes can be delegated to machines.

In this respect, Max Weber's concept of rational-legal authority, which emerged as part of the liberal revolutions, underscores the importance of power being exercised within a system of laws, where legal frameworks constrain the actions of both the state and private actors.[36] AI, by its nature, challenges this balance by introducing technologies that can make decisions that deeply affect individuals ranging from who gets approved for a loan to determining a person's guilt in criminal matters. Without robust legal constraints, the risk of AI being used to bypass established safeguards, such as due process and the right to equality, becomes a significant threat.

As noted by scholarly analysis,[37] the advent of AI introduces a new dimension to digital power, in which private actors, empowered by AI, can wield quasi-sovereign authority over critical aspects of public life. The automation of decisions that deeply affect individual rights, such as freedom of expression, privacy, and due process, requires that

---

[33] This evolution has been already analysed by Lyon with respect to the intersections between society and technology. David Lyon, *The Culture of Surveillance: Watching as a Way of Life* (Kindle, Wiley 2018).

[34] This aspect has also been commented on as "an erosion of privacy", or, in the words of the Korean philosopher Byung-Chul Han, *Psychopolitics: Neoliberalism and New Technologies of Power* (Verso Books 2017). Byung-Chul Han, "The neoliberal regime transforms subjects into projects. As projects, individuals constantly police, manage, and enhance themselves. They exploit themselves on behalf of the system". Specifically, Byung-Chul Han highlights that the digital era introduces a new form of dominance, where control is exerted not through physical force but through data and information. For a critique and an analysis of the computer-human relationship respectively: Pasquale, 'Watching (and Improving) the Watchers' (n 34); Batya Friedman and others, 'The Watcher and the Watched: Social Judgments About Privacy in a Public Place' (2006) 21 Human-Computer Interaction 235.

[35] On the role of metaphors shaping the judicial protection of fundamental rights on the Internet, see Alessandro Morelli and Oreste Pollicino, 'Metaphors, Judicial Frames, and Fundamental Rights in Cyberspace' (2020) 68 The American Journal of Comparative Law 616.

[36] Max Weber, *Diritto; a cura di Werner Gephart e Sigfried Hermes ; edizione italiana a cura di Massimo Palma* (Donzelli Editore 2016).

[37] Pollicino, 'Potere Digitale' (n 3).

constitutional law intervene to set boundaries and ensure that AI systems do not infringe on fundamental rights. As mentioned above, constitutional law has always functioned as a safeguard, ensuring that no entity, whether governmental or private, can exercise unchecked power.[38] In the case of AI, this role becomes even more central: to devise new legal mechanisms that avert the dangers posed by algorithmic governance, ensuring that rights are respected.[39]

Therefore, as society progresses into the digital era, where AI is increasingly woven into the fabric of everyday life, constitutional law's role as a safeguard against the concentration of power becomes even more vital. Particularly, constitutional law has a renewed role in addressing these asymmetries.[40] It must continue to fulfil its historical function of limiting power, but it must now extend its reach to encompass new forms of technological authority. Clearly, AI systems, which make decisions that affect fundamental rights must be subject to the same constitutional scrutiny as any other form of power.[41]

However, history reminds us of that legality alone is no safeguard for justice. As observed by Cartabia and Lupo,

> "during the totalitarian regimes of the 1920s and 1930s, a vast number of shameful and atrocious crimes were committed through the law, not despite the law. […] The rule of law was formally respected, at least from a procedural point of view. Alas, from a substantive point of view, the content of the 'laws' passed […] were at odds with the most basic sense of justice."[42]

This observation offers a powerful reminder: at critical times, one should reflect not only on the legality *per se* of the actions, but the assessment should involve a clear

[38] Marco Ruotolo, 'La Sicurezza Nel Gioco Del Bilanciamento' (2009) 49 Astrid rassegna.

[39] Sofia Ranchordás, 'The Invisible Citizen in the Digital State: Administrative Law Meets Digital Constitutionalism' in J De Poorter, C Oirsouw and G van der Schyff (eds), *European yearbook of constitutional law* (2024).

[40] Karen Yeung, 'Constitutional Principles in a Networked Digital Society' (Social Science Research Network, 3 March 2022).

[41] As Simoncini and Longo note, the increasing reliance on AI in areas like predictive policing, biometric surveillance, and automated legal judgments calls for constitutional frameworks to ensure that rights are not undermined by the black-box nature of algorithmic decision-making. Andrea Simoncini and Erik Longo, 'Fundamental Rights and the Rule of Law in the Algorithmic Society' in Hans-W Micklitz and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021).

[42] Marta Cartabia and Nicola Lupo, 'The Constitutional Court', *The Constitution of Italy* (Bloomsbury Publishing Plc 2022).

articulation of the substantive not negotiable values. Indeed, constitutional exist exactly to illustrate the limits of formal legal compliance: in this context, this quote is deemed particularly helpful to underscore the necessity of assessing not only how a system operates, but *why*, *where*, and *in what context* it is deployed.

In this light, this thesis proposes a *normative* reading of the Fundamental Rights Impact Assessment introduced under Article 27 of the AI Act. The FRIA should not be understood as a mere procedural requirement or bureaucratic formality. Rather, it must evolve into a constitutional tool, a mechanism that enables the legal system to interrogate the legitimacy of AI deployments in context, with attention to the structural risks they pose to dignity, agency, and democratic participation. This perspective reframes FRIA not only as a compliance mechanism, but as a vehicle for normative scrutiny and rights-based governance in the AI age.

Thus, closing this premise and moving forward with the presentation of the context on which this thesis builds on, the presentation hereby conducted had the aim to address the role of constitutional law in addressing the asymmetries of power introduced by AI systems, and links the context with the research questions which are examined *infra*.

1.1.3 Objectives and research questions

This thesis sets out to investigate how the regulation of facial recognition technology reflects broader constitutional and fundamental rights challenges posed by AI.

To this end, the analysis begins by contextualising FRT within the European regulatory landscape, with particular attention to the recently enacted AI Act. While the AI Act introduces a risk-based framework for AI governance,[43] the application of its provisions to high-risk technologies like FRT remains fragmented, especially when these systems are used by public authorities for surveillance and law enforcement purposes, being divided into prohibited practices and high-risk ones. What is at stake is the capacity of FRT to fundamentally reshape the exercise of public power, raising concerns over mass surveillance, discriminatory practices, and the erosion of individual autonomy.

Against this backdrop, the thesis adopts a dual objective. First, it critically examines the risks posed by facial recognition technology– including surveillance overreach, privacy violations, and discrimination – while situating these concerns within broader

[43] See, *infra,* §2.4.3.

constitutional principles such as proportionality, necessity, and democratic accountability. Second, it reinterprets the Fundamental Rights Impact Assessment as a normative tool that public authorities must use not only to assess the technical risks of AI systems, but to evaluate whether the legal and institutional context of their deployment aligns with the requirements of fundamental rights protection.[44]

In contrast to existing approaches, which tend to focus on technical parameters and quantifiable thresholds of risk,[45] this thesis contends that a FRIA must begin by asking whether the regulatory and governance framework itself is constitutionally adequate. It must interrogate whether the normative environment in which FRT is deployed, including authorisation procedures, judicial oversight, and redress mechanisms, provides sufficient guarantees against arbitrariness, opacity, and systemic harm. A FRIA that merely scrutinises system design or performance, while overlooking the broader legal architecture, fails to meet its function as a constitutional safeguard.

Therefore, rather than treating rights as fixed, abstract categories akin to a 'periodic table of elements', this thesis proposes a methodology that views rights as context-dependent constructs. The aim is to develop a process of recognition that identifies and assesses the specific issues affecting the enjoyment of rights in practice.[46] This approach requires a careful examination of how rights are triggered, impacted, and potentially violated by the deployment of FRT, particularly in sensitive contexts such as law enforcement.

Hence, while Chapter 5 lays the groundwork for this discussion by examining the broader range of rights at stake, Chapter 6 focuses on the right to an effective remedy as both a substantive and procedural cornerstone of fundamental rights protection in the governance of FRT. Substantively, this right provides individuals with actionable mechanisms to protect their rights when infringed by the deployment of FRT. Procedurally, it requires that FRT be embedded within a framework that upholds judicial safeguards, particularly the principles of fair trial and effective judicial remedies. This

[44] See, *infra,* Chapter 4.

[45] Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 Computer Law & Security Review 106020; Donatella Casaburo and Irina Marsh, 'Ensuring Fundamental Rights Compliance and Trustworthiness of Law Enforcement AI Systems: The ALIGNER Fundamental Rights Impact Assessment' [2024] AI and Ethics.

[46] Marta Cartabia, 'Universality of Rights in the Era of "New Rights"' [2009] Quaderni costituzionali.

dual focus ensures that individuals not only have clear and accessible avenues for redress but also that any use of FRT aligns with the broader principles of justice and accountability required in democratic systems.[47]

This research thus advances a qualitative, context-sensitive approach to FRIA, centred on three key questions: what is the constitutional threshold at which a right is considered effectively at risk? What legal and institutional elements shape that risk in a given deployment scenario? And how can a FRIA methodology ensure that the public actor's decision-making process is not only lawful in form, but substantively compatible with the fundamental rights framework of a democratic society? How does the deployment of FRT impact fundamental rights, particularly in high-risk contexts such as law enforcement? What mechanisms are necessary to operationalise the principle of effective remedies in the governance of FRT? How can this reconceptualised framework for FRT governance offer broader insights into the regulation of AI systems in public governance?

1.2 Methodology

A research method identifies how the research will be conducted in practice. The biggest challenge lied, then, in developing the most suitable method to answer the research question. The chosen method has been designed to answer precisely the questions asked, but, at the same time, the method had an influence on the way the research questions are formulated.[48]

That being said, legal research is usually classified, on the basis of the method used, as doctrinal or socio-legal (also known as non-doctrinal or empirical), where the former examines the 'law as it is' and the latter observes the relationship between law and society.[49] For this thesis, the primary focus is on normative legal methodology, treating the law as an objective and structured framework. This approach is essential for

[47] Simona Demková, *Automated Decision-Making and Effective Remedies : The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023); Kathleen Gutman, 'The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?' (2019) 20 German Law Journal 884; Matteo Bonelli, 'Effective Judicial Protection in EU Law: An Evolving Principle of a Constitutional Nature' (2019) 12 Review of European Administrative Law 35.

[48] Patrick Dunleavy, Authoring a PhD: How to plan, draft, write and finish a doctoral thesis or dissertation (Bloomsbury Publishing, 2003); in part. 18 – 26.

[49] Amrit Kharel, 'Doctrinal Legal Research' (2018) SSRN.

interrogating the alignment between existing legal norms and AI, particularly FRT as argued before.

This research then follows a normative method, meaning that it considers the law a normative and objective fact. Even though questions about the protection of fundamental rights are addressed through socio-legal methods, for the purposes of this research, meaning to understand how law can better address the novelties presented above, this thesis relies on a legal methodology. That does not exclude attention to the societal implications of, i.e., better-enforcing rights against AI uses; however, it is beyond the scope of this research to unpack the sociological matters.[50] The focus is on understanding and critiquing legal frameworks rather than on broader sociological impacts, which are acknowledged but not exhaustively addressed.

To situate the research within a robust human rights framework, the thesis draws on Griffin's conceptualisation of human rights as rooted in agency and dignity, which underpins the protection of self-determination.[51] This approach is balanced by Beitz's functional perspective on human rights, particularly relevant for examining state sovereignty and the justification for international intervention.[52] Together, these perspectives provide a critical lens for evaluating the governance of FRT in the European Union (EU) and, to some extent, in the Italian context, especially in analysing the AI Act implementing actions and the compatibility with the existing national legal framework.[53]

By integrating doctrinal rigour with fundamental rights theory, this methodology enables a structured critique of AI governance frameworks assuming a normative approach to human rights. The goal is to bridge theoretical insights and practical challenges, providing actionable recommendations for aligning regulatory frameworks with the principles of transparency, accountability, and rights protection.

[50] In this regard, this project relies on the contribution of FRA, 'Annex II: Examples of theoretical assessment of harm and significant impact of AI or automated decisions' (2020).

[51] James Griffin, 'Human Rights: Questions of Aim and Approach' (2010) 120 Ethics 741; James Griffin, *On Human Rights* (OUP Oxford 2009).

[52] Charles R Beitz, 'Normativity' in Charles R Beitz (ed), *The Idea of Human Rights* (Oxford University Press 2009); Charles R Beitz, 'International Concern' in Charles R Beitz (ed), *The Idea of Human Rights* (Oxford University Press 2009).

[53] See, *infra,* Chapter 6.

1.2.1 Behind the choice of FRT: A case study in rights and risks

While facial recognition is a prominent form of biometric identification, the broader category of these systems encompasses technologies such as fingerprint scanning, iris recognition, and voice analysis.[54] These systems share a common feature: they rely on unique physiological or behavioural characteristics to identify individuals.[55] However, their applications and risks vary significantly.[56] For instance, while fingerprint recognition is often used in controlled environments such as workplace access, facial recognition's deployment in public spaces makes it particularly susceptible to misuse and raises complex constitutional questions about proportionality, necessity, and accountability. Moreover, FRT's use in law enforcement raises significant concerns about the potential of illegitimate mass surveillance and latent infringements of fundamental rights. For instance, in its first ruling concerning the use of FRT by law enforcement, the ECtHR held that using FRT to analyse CCTV footage and social media images for identifying a protester violated fundamental rights, underlining the risks that this technology poses especially in the context where democratic freedoms are already under stress.[57]

FRT is particularly significant among biometric technologies because of its unique intersection of accessibility, scalability, ubiquity, and definitely its impact on public and private life.[58] Unlike fingerprint or iris recognition, which often require close physical interaction with a device, FRT operates passively, identifying individuals at a distance, even without their knowledge or consent. This ability makes it uniquely suited to mass surveillance, enabling unprecedented monitoring of public spaces in real-time and

[54] Zichang Tan and Guodong Guo, 'Face Recognition Research and Development' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024); Imane Badri and Mhamed Sayyouri, 'Face Recognition: A Mini-Review' in Saad Motahhir and Badre Bossoufi (eds), *Digital Technologies and Applications* (Springer Nature Switzerland 2023).

[55] See, *infra,* Chapter 3.

[56] Els J Kindt, 'The Risks Involved upon the Use of Biometric Data and Biometric Systems' in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013).

[57] ECHR (III Sec.), *Glukhin v. Russia,* id.

[58] Els J Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, vol 12 (Springer Netherlands 2013); Monika Zalnieriute and Rita Matulionyte (eds), 'The Cambridge Handbook of Facial Recognition in the Modern State', *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024); Natalia Menéndez González, *The Impact of Facial Recognition Technology Empowered by Artificial Intelligence on the Right to Privacy* (Routledge 2022); Giuseppe Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative* (ITA 2021).

retroactively through vast troves of collected data.[59] These characteristics significantly elevate the stakes for privacy, autonomy, and the relationship between state power and individual freedoms, especially when deployed in the law enforcement sector.[60]

Due to its far-reaching implications for fundamental rights, FRT has drawn increasing regulatory scrutiny. In August 2024, the EU AI Act entered into force, creating a new regulatory framework for AI systems, including biometric identification technologies. While the Regulation represents a significant step forward in addressing the risks associated with FRT, gaps remain, particularly in its application to law enforcement. Despite the critical role of FRT in sensitive contexts such as law enforcement, there has been limited research evaluating how the AI Act governs its use, its impact on fundamental rights, and the specific mechanisms required to address these issues in law enforcement, where such considerations are particularly pressing. This thesis seeks to fill this gap by examining the governance of FRT as a lens through which to explore broader constitutional and regulatory challenges posed by AI in the modern era.[61]

What makes FRT particularly relevant is its dual role in public and private ecosystems. On one hand, public authorities rely heavily on FRT for purposes such as border control, law enforcement, and public safety. Its deployment in these contexts raises significant concerns about proportionality, necessity, and accountability, particularly when used for mass surveillance or to monitor protestors, as underscored by the ECtHR. On the other hand, private actors play a critical role in the FRT ecosystem. Companies often develop the underlying algorithms and systems, providing the technical expertise and infrastructure that public bodies may lack. Furthermore, these systems frequently rely on datasets sourced from private platforms, such as social media networks, where users' images are collected and analysed, often without explicit consent.[62]

[59] Whence the distinction made by the AI Act between real-time biometric identification systems, which are deemed as 'prohibited AI practices', and therefore only usable under specific exceptions, *infra* Chapter 3, and remote biometric identification systems, which are instead classified as 'high risk'.

[60] By 2021, at least 11 out of 27 EU Member States were actively deploying FRT in criminal investigations. FPSM Ragazzi and others, 'Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the European Parliament' (Greens/EFA 2021); Gizem Gültekin-Várkonyi, 'Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation' (2024) 13 Internet Policy Review.

[61] See, i*nfra,* §3.5.

[62] See, *infra,* §5.3.1.

All of these points of concern are reasons motivating the relevance and necessity of this research topic. At the same time, FRT questions are rooted in fundamental rights challenges that are the starting points to reflect on and structure the research.

1.2.2 The legal framework

This thesis seeks to critically examine the governance of facial recognition as a focal point for understanding broader constitutional, regulatory, and fundamental rights concerns arising in the age of AI. The investigation is anchored in the context of law enforcement, where the deployment of FRT raises profound questions about the balance between security, privacy, and accountability.

The primary legal framework for this analysis is the European Union's (EU) regulatory architecture, particularly the AI Act, which represents a landmark attempt to regulate AI systems, including FRT. However, FRT, especially in the law enforcement sector, engages a complex web of fundamental rights protections, starting with the right to data protection enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (CFREU).[63] This right is deeply interconnected with Article 7 CFREU, which safeguards privacy, emphasising the need to protect individuals from disproportionate and intrusive surveillance. Additionally, the deployment of FRT in public spaces implicates the right to freedom of assembly and association (Article 12, CFREU) and raises potential concerns about non-discrimination (Article 21, CFREU), particularly when the underlying AI systems exhibit biases that disproportionately target specific groups or communities.

Complementing the CFREU, the European Convention on Human Rights (ECHR) provides another cornerstone of this thesis.[64] Article 8 ECHR establishes the right to respect for private and family life, while Article 11 protects the right to freedom of assembly and association. Notably, the European Court of Human Rights (ECtHR) has issued judgments that emphasise the obligations of states to strike a balance between surveillance technologies and the protection of these rights.

These decisions, alongside the jurisprudence of the Court of Justice of the European Union (CJEU), have shaped the fundamental rights framework governing AI and FRT,

[63] Charter of Fundamental Rights of the European Union OJ C 364/1 2000.
[64] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

providing critical interpretative guidance on the scope and limitations of lawful surveillance.

Beyond the foundational rights, secondary EU legislation offers operational tools for regulating FRT. The EU's 2016 data protection reform package introduced two key instruments: the General Data Protection Regulation (GDPR),[65] which governs data protection in general contexts, and the Law Enforcement Directive (LED),[66] which applies specifically to law enforcement activities. Both frameworks establish principles of transparency, necessity, and proportionality, but their adequacy in addressing the unique challenges posed by FRT remains contested, so much so that precisely with the AI Act, a *lex specialis* was drawn up for the regulation of this specific group of technologies that has elements of all three regulatory frameworks.[67]

Moreover, as mentioned, these instruments intersect with the jurisprudence of the ECtHR and CJEU, as well as national courts, which have increasingly emphasised the need to balance technological innovation with fundamental rights protections. The analysis of the courts' decisions will serve especially crucial to conduct that act of visibility and recognition that is central to the FRIA. [68]

A significant aim of the thesis is to evaluate how the regulatory frameworks address the need for effective remedies and safeguards against the misuse of FRT, particularly in contexts where the technology operates in real-time and targets individuals in public spaces. The analysis also seeks to understand the role of procedural autonomy, the harmonisation objectives of the EU, and Member States' sovereignty claims in shaping the governance of these technologies. These dynamics are especially pronounced in areas such as data retention, judicial oversight, and the procedural frameworks for remedies, which sit at the intersection of constitutional tensions and technological innovation.

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

[66] 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.

[67] See, *infra,* Chapter 3.

[68] See, *infra,* Chapter 4 and 5.

1.2.3 The territorial scope

As evidenced by the above, this research primarily focuses on the European legal framework governing FRT and its implications for fundamental rights, with particular attention to the legislative and jurisprudential developments within the EU and the Council of Europe. The EU's AI Act, GDPR and LED serve as key instruments in this analysis, while the case law of the CJEU and the ECtHR provides critical guidance on the interpretation and application of fundamental rights in the context of technological governance.

In addition to this overarching European focus, this thesis examines the specific case of Italy, with a particular emphasis on the country's approach to the implementation of the above framework, especially the AI Act, and its compatibility with the existing norms. Italy offers a compelling case study due to its jurisprudential history and regulatory developments concerning the use of surveillance technologies, including wiretapping and other methods that intersect with FRT. These practices highlight the tension between security imperatives and fundamental rights, particularly privacy and due process, which are central to the thesis's focus on constitutional safeguards.[69]

At the same time, the research acknowledges the transnational nature of FRT and AI governance, recognizing that these technologies often transcend jurisdictional boundaries. While the primary focus remains on Europe and Italy, relevant comparative perspectives are incorporated where appropriate. For instance, the thesis contrasts the European framework with the United States' approach to AI governance, particularly in balancing innovation with fundamental rights protection. Combining an in-depth analysis of the European legal framework with a focus on Italy and selected comparative insights, this research aims to provide a nuanced understanding of the governance challenges posed by FRT.

1.2.4 Elements of interdisciplinarity

This research primarily examines the governance of facial recognition technology (FRT) from a legal perspective, focusing on its implications for fundamental rights and constitutional principles.

[69] See Chapters 5 and 6, *infra.*

However, fully understanding the governance of FRT and its implications requires engaging with the technical aspects of the technology itself. Therefore, the legal and constitutional analysis is complemented by an exploration of relevant technological aspects.[70] This includes an examination of the underlying functioning of AI systems, the specific technical processes involved in FRT, such as image capture, pattern recognition, and dataset training, and the risks associated with these processes, such as biases and inaccuracies. These technical insights, discussed in Chapters 2 and 3, provide a basis for understanding how the deployment of FRT affects fundamental rights and shapes regulatory challenges. By integrating legal and technical perspectives, this work aims to provide a comprehensive understanding of the governance issue posed by FRT and propose actionable solutions grounded in both constitutional principles and technical realities.

1.3 Structure of the work

While the previous sections have already highlighted the key aspects of the present work, the following subsections will give a more detailed overview of the content of the dissertation's Chapters.

1.3.1 Part one

The first part, comprising Chapters 2 and 3, provides the broader context and theoretical framework necessary to understand the regulatory challenges posed by artificial intelligence, particularly in the application of biometric identification systems. Chapter 2 lays the foundation by examining the legal and constitutional dimensions of AI, framing it as both a transformative technological force and a complex regulatory agenda. It explores how emerging technologies reshape traditional notions of governance, fundamental rights, and the rule of law, situating these issues within the European Union's regulatory approach, with a specific focus on the AI Act's risk-based framework. Chapter 3 builds on this foundation by delving into the specifics of biometric systems, particularly facial recognition technology. This chapter examines the technical and social implications of biometric technologies, emphasising their rapid adoption and associated risks. It critically analyses the interplay between the GDPR, the LED, and the AI Act, assessing

[70] See Chapter 2 and 3, *infra.*

how these legal frameworks address the unique challenges posed by facial recognition systems.

1.3.2 Part two

The second part of the thesis, comprising Chapters 4, 5, and 6, transitions from the general regulatory context to a detailed examination of fundamental rights and the mechanisms intended to safeguard them. Chapter 4 introduces the concept of FRIA, positioning them as central to the governance of high-risk AI systems under the AI Act. It evaluates the theoretical and practical issues of embedding FRIA into existing legal and procedural frameworks, drawing comparisons with other regulatory tools to identify best practices. Chapter 5 applies the FRIA framework specifically to the governance of biometric systems, analysing their profound implications for fundamental rights, including privacy, freedom of expression, and data protection. This chapter scrutinizes the systemic risks posed by these technologies and assesses whether the AI Act sufficiently mitigates these concerns. Chapter 6 then focuses on the right to an effective remedy in the context of high-risk AI systems such as facial recognition. It critiques the AI Act's provisions on remedies, with particular attention to transparency, access to justice, and the balance of power between judicial and administrative oversight. This chapter argues that the fragmented nature of the current regulatory framework leaves significant gaps in the protection of fundamental rights, particularly in scenarios where the opacity and scale of AI systems intensify accountability challenges. Chapter 7 concludes.

From this structure, the research aims to offer both a comprehensive understanding of the constitutional and regulatory challenges posed by AI and a focused critique of how these issues play out in the governance of biometric technologies. This dual approach highlights the tension between technological innovation and rights protection, advocating for a robust regulatory framework that effectively safeguards fundamental rights in the digital age.

2. THE REGULATION OF ARTIFICIAL INTELLIGENCE: AN EXISTENTIAL CHALLENGE

SUMMARY: 2.1 Introduction. – 2.2 What is AI?; 2.2.1 Conceptual foundations of AI; 2.2.2 What AI is not; 2.2.3 Technical foundations of AI; 2.2.3.1 The 'souls' of AI; 2.2.3.2 Symbolic and sub-symbolic AI; 2.2.3.3 Machine learning and deep learning; 2.2.3.4 What about FRT?. – 2.3 From automation to autonomy; 2.3.1 The power of autonomy: new unprecedented challenges. – 2.4 The Artificial Intelligence Act; 2.4.1 Objectives of the Regulation: between product safety and fundamental rights; 2.4.2 Material and territorial scope; 2.4.3 Method: the risk-based approach; 2.4.4 Prohibited risk AI; 2.4.5 High Risk AI systems; 2.4.6 Limited risks; 2.4.7 Requirements for high risk systems; 2.4.8 Obligations for high risk systems; 2.4.9 Obligations for providers of high-risk systems; 2.4.10 Obligations for deployers of high risk systems; 2.4.10.1 Fundamental rights impact assessment (FRIA); 2.4.11 Harmonised standards; 2.4.12 Governance and enforcement; 2.5 Conclusion.

2.1 Introduction

The regulation of AI represents one of the most pressing existential challenges of the modern age.[71] As AI systems continue to mediate human experiences, whether in curating news, diagnosing medical conditions, or making legal judgments, regulating their use becomes an urgent concern for not just technologists, but also policymakers, legal experts, and society at large, positioning it as a cornerstone of the global economy and democratic governance.[72]

From a purely legal perspective, it must be acknowledged that AI is considered by the Regulation (EU) 2024/1689 a product and, as such, is subject to regulatory frameworks like any other manufactured good.[73] However, differently from apples, cars, and shoes,

[71] Oreste Pollicino and others (eds), *La Disciplina Dell'intelligenza Artificiale* (Giuffrè Editore 2025).

[72] Mario Draghi, 'The Future of European Competitiveness' (*European Commission*, 2024) <https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en> accessed 3 December 2024.

[73] See the Explanatory Memorandum to the Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, {Sec(2021) 167 Final} - {Swd(2021) 84 Final} - {Swd(2021) 85 Final}, in part. §2, on the legal basis. See, also, Gabriele Mazzini and Salvatore Scalzo, 'The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts' (2 May 2022) <; Marco Almada and Nicolas Petit, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (18 October 2023).

AI is a peculiar product: its capabilities often transcend traditional notions of goods or services. AI systems, particularly those that operate autonomously, introduce unique risks that demand dedicated regulatory approaches.[74] These risks include their opacity, scalability, and profound societal impacts, which blur the lines between innovation, accountability, and protecting fundamental rights.[75]

Therefore, understanding what AI truly is, is a profound challenge: its nature is not fixed or organic; it evolves continuously, adapting to new datasets, algorithms, and societal demands.[76] This fluidity renders AI fundamentally different from traditional products: it is not merely a tool but a system capable of learning, making decisions, and influencing human lives in ways that are often opaque.[77] The difficulty in defining AI and understanding what it is tied to its transformative potential, which, as some have noted, represents "a revolution that has few parallels in history".[78]

Floridi encapsulates this challenge with his counterfactual approach, suggesting that it is more practical to avoid rigid definitions of AI and instead assert, "I recognise it when I see it."[79] This perspective highlights the elusiveness of AI as a concept and the inadequacy of traditional definitional frameworks. AI forces us to grapple with deeper philosophical questions: What does it mean to possess intelligence? Can a machine truly understand, or does it merely mimic understanding? If intelligence is inherently human or animal, does extending the term to machines anthropomorphise them, thereby obscuring their true function as artefacts of human design?[80]

---

[74] European Commission, 'White Paper on Artificial Intelligence: a European approach to excellence and trust', 19 February 2020.

[75] Oreste Pollicino, '"Getting the Future Right – Artificial Intelligence and Fundamental Rights". A view from the European Union Agency for Fundamental Rights' [2021] BioLaw Journal - Rivista di BioDiritto 7; Erik Longo, 'La ricerca di un'antropologia costituzionale della società digitale' (2023) 5 Rivista italiana di informatica e diritto 147.

[76] Giovanni Sartor, *L'intelligenza artificiale e il diritto* (Giappichelli, 2022); Francesca Lagioia and Giovanni Sartor, 'Artificial Intelligence in the Big Data Era: Risks and Opportunities', *Legal Challenges of Big Data* (Edward Elgar Publishing 2020); Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20170355.

[77] Henrik Palmer Olsen and others, 'What's in the Box? The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration' (Social Science Research Network 2019) SSRN Scholarly Paper ID 3402974.

[78] Erik Longo and Andrea Pin, 'Oltre Il Costituzionalismo? Nuovi Principi e Regole Costituzionali per l'era Digitale' [2023] Diritto pubblico comparato ed europeo. Auth. Trasl.

[79] Luciano Floridi, *Etica Dell'intelligenza Artificiale: Sviluppi, Opportunità, Sfide* (Raffaello Cortina Editore 2022). Auth. Trasl.

[80] Luciano Floridi, 'Present: AI as a New Form of Agency, Not Intelligence' in Luciano Floridi (ed), *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities* (Oxford University Press 2023).

The term "intelligence" itself has traditionally been associated with humans or, to some extent, animals.[81] Assigning it to machines fosters anthropomorphic narratives, suggesting that AI systems are akin to living beings with cognitive capacities. However, AI is fundamentally different: its processes, while seemingly intelligent, are mechanical, statistical, and devoid of consciousness. John McCarthy, one of the pioneers of AI, sought to provide clarity by defining AI as:

> "the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not need to confine itself to biologically observable methods."[82]

Even the frequent invocation of the term "oracle" to describe AI systems reflects a broader tendency to imbue them with quasi-mystical authority.[83] Like the oracles of antiquity, AI systems are often perceived as providing definitive answers to human questions, derived from data that even their developers may not fully understand. While evocative, this characterisation risks exaggerating AI's capabilities, fostering a false sense of its omnipotence and autonomy.[84]

Treating AI as an autonomous actor capable of independent decision-making risks shifting accountability away from the human creators, developers, and users who ultimately design and operate these systems.[85]

---

[81] "An entity is intelligent if it has an adequate model of the world (including the intellectual world of mathematics, the understanding of its own purposes and other mental processes), if it is capable of answering a wide variety of questions based on that model, if it can draw additional information from the external world when necessary, and if it can perform in the external world the tasks required by its purposes and permitted by its physical capabilities", John McCarthy and others, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955' (2006) 27 AI Magazine 12.

[82] John McCarthy, 'What Is Artificial Intelligence?' [2007] Formal Stanford.

[83] On the mystification of generative AI, read Francesco Paolo Levantino, 'Generative and AI-Powered Oracles: "What Will They Say about You?"' (2023) 51 Computer Law & Security Review 105898.

[84] Instead, as Giusella Finocchiaro aptly notes, this portrayal reinforces the perception that AI systems possess an intrinsic authority as if they are capable of deciphering complexities and rendering judgments that surpass human understanding.[84] Such narratives amplify the mystique surrounding AI, complicating efforts to regulate it with the necessary balance of scepticism and pragmatism. Critically, this perception risks distorting our approach to AI's legal and ethical governance.Giusella Finocchiaro, *Intelligenza Artificiale. Quali Regole?* (Il mulino 2024).

[85] Joanna J Bryson, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford University Press 2020); Christopher Beha, 'Opinion | A.I. Isn't Genius.

This distinction is crucial for safeguarding the integrity of legal systems and upholding fundamental principles of justice, especially in scenarios where AI's decisions significantly affect individual rights and societal values. Recognising AI's autonomy in a technical sense must not come at the cost of eroding human responsibility. As underlined by Pollicino, stressing the value of the concept of autonomy in this context,

> "The pervasive presence of AI is thus opening up a new phase characterised by the increasing dominance of automation, the main new factor of which is to be found in the fact that human supervision is often reduced to mere supervision and control of the result that is actually produced by the 'machine'. In other words, the transition from an algorithmic society to one shaped by AI represents a profound change in the way the state positions itself and interacts with its citizens and in the way more or less complex situations are regulated. […] It is essential, especially from the perspective of constitutional law, to define precise guidelines on when and how human involvement should take place."[86]

Therefore, regulations should aim to balance the capabilities of autonomous systems with robust mechanisms to ensure transparency, traceability, and ethical accountability, creating a space and posing at its centre the human being and its added value throughout the AI-chain.

To this end, this chapter examines how AI's characteristics, such as its opacity, scalability, and autonomy, intersect with the AI Act. While providing an exhaustive definition of AI falls outside the scope of this thesis, a foundational understanding is necessary to engage with the unique challenges its applications pose across various sectors. Subsequently, the discussion of AI will be narrowed down to a specific goal, namely that of understanding the framework in which the challenges, the risks of FRT, as well as the necessary fundamental rights safeguards, in the specific sector of law enforcement. In this sense, the chapter is structured like a funnel, gradually narrowing down the topic. Therefore, particular emphasis is placed on how the Regulation seeks to

---

We Are.' *The New York Times* (26 December 2024) <https://www.nytimes.com/2024/12/26/opinion/ai-genius-art.html> accessed 3 December 2024.

[86] Oreste Pollicino, 'Regolare l'Intelligenza Artificiale: La Lunga via Dei Diritti Fondamentali' in Oreste Pollicino and others (eds), *La disciplina dell'intelligenza artificiale* (Giuffrè Editore, 2025). Text translated by the author.

mitigate risks while balancing innovation with the protection of fundamental rights. This chapter undertakes a critical examination of the AI Act's structure, objectives, and limitations, focusing on its implications for constitutional law and the protection of fundamental rights – a prodromic to understand the risks specifically related to FRT. By disentangling myths from realities, this analysis aims to provide a nuanced understanding of AI while laying the foundation for a governance framework that addresses legal and ethical challenges, ensures alignment with democratic principles, and effectively safeguards fundamental rights in an era of rapid technological advancement.

2.2 What is AI?

When we explain to a child what an apple is, we show them an image of the fruit, let them taste its juice, and connect its form to its benefits, its sweetness, its nourishing properties, and even the idea that "an apple a day keeps the doctor away." This simple, tangible approach allows the child to relate the concept of an apple to its physical characteristics and its role in their life. However, how do we explain what AI is? Unlike tangible objects, AI resists simple visual or experiential definitions. Philosophers, as mentioned earlier, propose a counterfactual approach: AI is something you "recognise when you see it," as it diverges fundamentally from other computational tools humanity has created.[87] Among its unique features is to be recalled its ability to analyse vast quantities of data at unparalleled speed and precision, adapting to evolving circumstances without needing explicit human instructions.

Understanding AI begins with grappling with its lack of a universally accepted definition. Among the most referenced descriptions is that of the Organisation for Economic Co-operation and Development (OECD),[88] on which the EU based the creation of its understanding of AI system:

> "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for

[87] 'What's the Difference Between AI and Regular Computing? | Royal Institution' (12 December 2023) <https://www.rigb.org/explore-science/explore/blog/whats-difference-between-ai-and-regular-computing> accessed 3 December 2024.

[88] Organization for Economic Co-operation and Development (OECD), AI Principles, 2019. See, also, Karen Yeung, 'Recommendation of the Council on Artificial Intelligence (OECD)' (2020) 59 International Legal Materials 27.

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."[89]

This definition was also referenced by the CoE within its Framework Convention on Artificial Intelligence.[90] At its core, AI's defining characteristic is its autonomy: [91] its ability to function without explicit human instructions, learning from data to adapt and optimise its behaviour, rather than merely executing a set of predefined steps as traditional computing systems do.[92] This unique capacity to analyse vast amounts of data and dynamically adjust to changing conditions distinguishes AI from conventional IT systems.[93]

Nonetheless, this definition offers little insight into what AI truly is, since it indeed focus on AI system, not AI itself. To address the question posed in the title of this paragraph, it is necessary to take a step back. Therefore, the following sections will explore the conceptual origins of AI and delve into its technical features.

[89] AI Act, Art. 3, no. 1). See also the 'Guidelines on the definition of an artificial intelligence system established by AI Act', published by the European Commission, Feb. 2025.

[90] Council of Europe (CoE), Framework Convention on artificial intelligence, human rights, democracy and the rule of law, published on 17 May 2024, and open for signatures since 5 September 2024, Council of Europe Treaty Series - No. 225.

[91] A different definition was provided by the High Level Expert Group on AI (AI HLEG, set up by the European Commission) in its report on the development of a European strategy on AI, which preceded the Proposal for a Regulation: Artificial intelligence (AI) systems are software (and possibly hardware) systems developed by human beings that, given a complex goal, operate in the physical or digital dimension by perceiving their environment by acquiring data, interpreting the collected structured and unstructured data structures, reasoning about knowledge or processing information, derived from this data, and deciding on the best actions to take in order to achieve the given goals. AI systems can use symbolic rules or learn a numerical model, and can also adapt their behaviour by analysing how the environment is affected by their previous actions. High-Level Expert Group on Artificial Intelligence (AI HLEG), Ethics Guidelines For Trustworthy AI, 08 April 2019. For a comment see Nathalie A Smuha, 'The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence' (2019) 20 Computer Law Review International 97.

[92] Lilian Edwards, 'Expert Opinion: Regulating AI in Europe' (2022), Ada Lovelace Institute, <https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/> accessed 3 December 2024.

[93] It is important to note that the majority of AI systems are designed to perform only a limited range of tasks, often focusing on specific functions such as pattern recognition (e.g., classifying objects in images, identifying individuals using biometric data, or analysing sentiments and attitudes), language translation, filtering unwanted content (such as spam, violence, or explicit material), or selecting targeted information (like social media content curation). Some systems, however, integrate multiple capabilities. For instance, autonomous vehicles must not only identify objects in their surroundings but also plan routes and navigate independently to reach their destinations. See Mireille Hildebrandt, *Smart Technologies and the End (s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2015).

2.2.1 Conceptual foundations of AI

The origins of AI[94] as a technological discipline date back to the mid-20th century, particularly with the publication of Alan Turing's seminal 1950 paper, Computing Machinery and Intelligence.[95] This foundational work marked the dawn of modern AI. Around the same time, Norbert Wiener, one of the pioneers of cybernetics, was learning about how the brain appears to function and began theorizing how machines could mimic these processes. Wiener's groundbreaking ideas on feedback loops and control systems laid the groundwork for thinking about intelligent machines that could respond and adapt, much like the human brain.[96]

Nonetheless, long before AI became a subject of legal and regulatory focus, it captivated the human imagination through art and film. Stanley Kubrick's 2001: A Space Odyssey (1968) was the first major cinematic work to explore AI's transformative potential, notably through the character of HAL 9000. This was followed by other iconic works such as Blade Runner, The Matrix, Bicentennial Man, and Her, each addressing unique aspects of AI, from the philosophical questions of consciousness and autonomy to emotional intelligence and human-robot relationships.

In literature, Isaac Asimov's Three Laws of Robotics introduced in the 1930s have had a lasting influence on both science fiction and actual legal discussions, especially about the relationship between human categories, like liability, and technology.[97]

As AI transitioned from speculative fiction to a tangible and influential technology, its impact on the human experience became undeniable.[98] AI functions as a powerful information intermediary, filtering, curating, and distributing content, which not only influences what information individuals receive but also how they perceive reality.[99]

---

[94] Luciano Floridi, 'Passato: L'origine Dell'intelligenza Artificiale', *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide* (Raffaello Cortina Editore 2022).

[95] Alan M Turing, 'Intelligenza Meccanica, a Cura Di G. Lolli, [1994], Boringhieri, Torino.

[96] Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine* (MIT press 2019).

[97] Asimov's laws were even referenced in the European Parliament Resolution of 16 February 2017, which recommended civil law regulations on robotics and AI. These cultural representations of AI have shaped societal perceptions and raised ethical questions long before AI began to impact daily life and regulatory frameworks, as also observed by Henry A Kissinger, Eric Schmidt and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (Hachette UK 2021).

[98] For an historical evolution of AI, see Sartor (n 80).

[99] Henry A Kissinger, Eric Schmidt and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (Hachette UK 2021). Specifically, the authors observed that AI is set to impact a huge transformation on the human

Scholars Stuart Russell and Peter Norvig, in their seminal work, distinguish AI approaches along two key dimensions: whether they focus on thinking versus acting, and whether their goal is to replicate human capabilities or achieve optimal rationality beyond human limitations.[100] This framework highlights the dual aspirations of AI research. On one hand, some approaches aim to simulate human cognitive processes, replicating how humans think and reason. On the other, there are systems designed to optimise performance and achieve precise outcomes without emulating human thought patterns. For instance, the former may involve AI models that mirror human problem-solving processes, while the latter prioritises efficiency, as seen in systems optimising supply chains or diagnosing medical conditions.[101]

A critical distinction lies between AI and traditional computational techniques such as algorithms. While algorithms operate through predefined, step-by-step instructions to achieve specific results, AI systems are marked by their autonomy and adaptability.[102] This distinction becomes especially evident in machine learning (ML), a subset of AI that allows systems to learn from data and refine their behaviour over time.[103] AI, in this sense, represents a shift from static rule-based operations to dynamic, data-driven decision-making.[104]

Despite its advancements, defining AI remains an elusive endeavour, reflecting its interdisciplinary nature and continuous evolution. Scholars debate whether cognitive terms such as "intelligence," "reasoning," or "understanding," originally developed to describe human mental processes, are appropriate for artificial systems.[105]

---

experience dialysed by renovations in the field of decision making, decision making, scientific discovery, education and learning and information intermediary.

[100] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th US ed, Pearson Education 2021).

[101] Serena Quattrocolo, 'Approaching the Unknown: Some Preliminary Words' in Serena Quattrocolo (ed), *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion* (Springer International Publishing 2020).

[102] As underlined by Sartor, "it is therefore important to remember that algorithms, as procedures susceptible to automatic application, have a field of use that extends beyond AI systems, covering every computer system". Sartor (n 80).

[103] Zhi-Hua Zhou, *Machine Learning* (Springer Nature 2021); Ethem Alpaydın, *Machine Learning* (MIT Press Essential Knowledge series 2016).

[104] Teresa Rodríguez de las Heras Ballell, 'Legal Challenges of Artificial Intelligence: Modelling the Disruptive Features of Emerging Technologies and Assessing Their Possible Legal Impact' (2019) 24 Uniform Law Review 302.

[105] Luciano Floridi, 'Present: AI as a New Form of Agency, Not Intelligence' in Luciano Floridi (ed), *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities* (Oxford University Press 2023); Floridi, *Etica Dell'intelligenza Artificiale: Sviluppi, Opportunità, Sfide* (n 8); Luciano Floridi, 'AI as

Furthermore, the legal implications of defining AI add another layer of complexity. For instance, the AI Act, as mentioned, adopts a functional and purpose-driven approach, focusing on the risks and societal impacts of AI applications.[106] However, AI is not a singular field but a convergence of diverse techniques and applications that intersect with almost every aspect of society. Its transformative potential and inherent complexities call for nuanced understanding, not only in technical research but also in regulatory efforts.

Given the complexity and vast scope of AI research, the following section aims to clarify some fundamental concepts and key aspects of AI. While not exhaustive, these elements are intended to provide a foundational understanding of the technical dimensions of AI.

2.2.2 What AI is not

First and foremost, we should clarify what AI is not.

The term 'algorithm' is often used interchangeably with AI, particularly in expressions such as 'algorithmic governance,'[107] or, even, 'algorithmic society.'[108] While algorithms are foundational to AI, they are not exclusive to it and serve a much broader range of applications in computing.[109] From simple procedures, like sorting lists or finding the greatest common divisor, to highly complex processes, such as encryption, voice

Agency Without Intelligence: On ChatGPT, Large Language Models, and Other Generative Models' (2023) 36 Philosophy & Technology 15.

[106] Michał Araszkiewicz, Grzegorz J Nalepa and Radosław Pałosz, 'The Artificial Intelligence Act. Taking Normative Imbalances Seriously' (*Internet Policy Review*) <https://policyreview.info/articles/news/artificial-intelligence-act-taking-normative-imbalances-seriously/1817> accessed 3 December 2024.

[107] The term is used by Danaher to mean "a system in which algorithms are used to collect, collate and organise the data on which decisions are typically made and to assist in how that data is processed and communicated through the relevant *governance* system", (emphasis added), John Danaher, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29 Philosophy & Technology 245.

[108] Marc Schuilenburg and Rik Peeters, *The Algorithmic Society: Technology, Power, and Knowledge* (Routledge 2020); Jack M Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2017) 51 UCDL rev. 1149.

[109] An algorithm, in its simplest form, is a step-by-step procedure or set of rules designed to perform a specific task. Traditional algorithms execute instructions that are explicitly defined by humans to produce a deterministic output. For instance, a basic algorithm might involve calculating the shortest route between two points or applying rules to classify emails as spam or non-spam. See also Anthony Elliott, *Making Sense of AI: Our Algorithmic World* (John Wiley & Sons 2021).

recognition, or financial forecasting, algorithms are essential to every computational system, whether or not it involves AI.[110]

This distinction is not easy to grasp, especially, in legal terms. In this sense, the Italian Council of State articulated the following definition:

> "The common and general notion of algorithm brings to mind a finite sequence of instructions, well-defined and unambiguous so that they can be mechanically executed and such as to produce a given result; however, if the notion is applied to technological systems, it is inescapably linked to the concept of automation, that is to say, to systems of action and control capable of reducing human intervention, the degree and frequency of which depend on the complexity and accuracy of the algorithm that the machine is called upon to process. What is different is artificial intelligence, in which the algorithm contemplates machine learning mechanisms and creates a system that does not merely apply software rules and pre-set parameters (as the traditional algorithm does) but, on the contrary, constantly elaborates new criteria of inference between data and makes efficient decisions based on such elaborations, according to a process of machine learning."[111]

This definition, even if ambiguous in some parts, is useful to draw a line between AI and algorithms. These latter ones are typically understood as a finite sequence of well-defined, unambiguous instructions that can be mechanically executed to produce a specific result. In this sense, they operate predictably and are tied closely to automation processes that aim to reduce human intervention, with their performance shaped by the complexity and precision of the programmed instructions, without being fully autonomous and able to infer information[112]

---

[110] Sartor (n 5); Arno R Lodder, 'Algorithms: What, How, and Particularly Why?' (Social Science Research Network 2019) SSRN Scholarly Paper ID 3392869 <https://papers.ssrn.com/abstract=3392869> accessed 3 December 2024.

[111] Italian Council of State, Third Section, decision no. 7891 of November 25, 2021, §9.1. The text was translated by the author of this thesis.

[112] Frank Pasquale, 'A Rule of Persons, Not Machines: The Limits of Legal Automation' (2019) 87 George Washington Law Review 1.

By contrast, AI systems transcend these traditional algorithmic boundaries. While AI systems still rely on algorithms, they incorporate mechanisms such as machine learning, enabling them to develop and refine new criteria for inference directly from data.[113] For this reason, as will be explained *infra,* one of the most important and distinguishing features of AI is indeed the ability to infer, enabling autonomous learning. Unlike traditional algorithms, which rigidly apply pre-defined rules, AI systems dynamically adapt their behaviour by learning from their inputs.

2.2.3 Technical foundations

Therefore, a critical starting point in understanding AI is distinguishing it from the broader concept of algorithms. While all AI systems are underpinned by algorithms and structured, step-by-step computational procedures, not all algorithms qualify as AI.

The core of AI systems lies in learning algorithms: sophisticated computational methods designed to adapt and improve over time.[114] Whereas traditional algorithms[115] follow static, predefined rules, these learning algorithms process vast datasets to develop algorithmic models capable of predicting outcomes, recognising patterns, or making decisions autonomously.[116] For example, a neural network tasked with classifying images does not simply apply fixed instructions.[117] Instead, it employs a learning algorithm to adjust the weights of its connections iteratively, refining its performance in identifying objects like animals, faces, or sentiments. This process of optimisation and self-adjustment allows the system to adapt to new data and contexts, enhancing its predictive accuracy and utility. The inner workings of such models, particularly in the case of deep learning, can become opaque, giving rise to what is known as the "black-box" problem.[118]

---

[113] Sabina Leonelli, 'What Distinguishes Data from Models?' (2019) 9 European Journal for Philosophy of Science 22.

[114] Russell and Norvig (n 103).

[115] Those algorithms, which are still considered highly effective, operate deterministically, producing outputs based on predefined rules and inputs. See the analysis conducted by Shuyao Zeng, Yanming Zhao and Shaobin Li, 'Comparison Between the Traditional and Deep Learning Algorithms on Image Matching', *2022 IEEE/ACIS 22nd International Conference on Computer and Information Science (ICIS)* (2022) <https://ieeexplore.ieee.org/document/9882428> accessed 3 December 2024.

[116] Olsen and others (n 6); Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2972505 <https://papers.ssrn.com/abstract=2972505> accessed 3 December 2024; Lodder (n 38).

[117] Zhou (n 106).

[118] Sartor (n 80).

This refers to the difficulty, even for the system's creators, in understanding the exact mechanisms or logic that led to a specific decision or prediction. This opacity has been indicated as the difficulty in achieving and granting a right to an explanation of the decisions produced by and, or via automated decision-making systems,[119] due to the significant challenges for accountability, trust, and regulatory oversight in the deployment of AI systems.

2.2.3.1 The 'souls' of AI

Given these premises, AI can be broadly categorized into two paradigms: cognitive (or 'strong') AI and engineering (or 'weak') AI.[120]

Cognitive AI aims to replicate human intelligence, striving to create machines capable of 'thinking' and reasoning like humans. This approach, often associated with speculative visions of AI, has largely remained confined to science fiction and theoretical research.[121] Engineering AI, by contrast, focuses on achieving practical outcomes, prioritising functionality over mimicry of human cognition. This pragmatic approach has driven the development of most modern AI systems, which excel at solving specific problems efficiently without attempting to replicate human thought processes. Examples include IBM's Deep Blue, which defeated the world chess champion in 1997, and DeepMind's AlphaGo, which mastered the game of Go.[122]

This distinction is indeed well encapsulated by Floridi who notes that "successful AI concerns the replacement, not replication, of human intelligence."[123] This pragmatic

[119] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking For' (LawArXiv 2017) preprint <https://osf.io/97upg> accessed 3 December 2024; Ljubiša Metikoš and Jef Ausloos, 'The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act' (Social Science Research Network, 6 August 2024) <https://papers.ssrn.com/abstract=4996173> accessed 3 December 2024; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243; S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law <https://ora.ox.ac.uk/objects/uuid:6c90bb41-093c-417b-852a-7716054e44bb> accessed 3 December 2024.

[120] Oreste Pollicino and Pietro Dunn, 'IA e Valori Democratici' in Oreste Pollicino and Pietro Dunn, *Intelligenza Artificiale e Disinformazione* (Egea 2024).

[121] Quattrocolo (n 104); Sartor (n 80); Finocchiaro (n 88).

[122] Albert-László Barabási and Marton Parafasi, *Network Science* (Cambridge University Press 2016); Zhou (n 31).

[123] Floridi, 'Present' (n 84).

orientation underscores the field's focus on outcomes, emphasising the utility of AI systems rather than their alignment with human cognitive attributes.

Therefore, excluding the real presence of cognitive AI – at least at the state of the art – and devoting our attention to the sole engineering one, it is to further distinguish between 'symbolic' vs. 'subsymbolic' AI. These two major methodological approaches refer to the way AI is set to learn and are described as follows.

2.2.3.2 Symbolic and sub-symbolic AI

Symbolic AI dominated the early years of AI development. This approach is based on formal logic and rule-based systems, where human experts manually curate and encode knowledge into "if-then" rules.[124] For instance, a system might be programmed to conclude that "if an object has four legs and a back, then it is likely a chair."

These systems are generally transparent and predictable, making them relatively easy to understand and explain. They are particularly well-suited to structured problems like chess or basic arithmetic. However, symbolic AI has significant limitations. Its reliance on manually crafted rules means it struggles with unstructured,[125] complex, real-world data.

Due to the limitations of symbolic learning, subsymbolic AI emerged in the 90s. Instead of relying on predefined rules, subsymbolic AI uses data-driven methods to learn patterns and relationships directly from data. In essence, sub-symbolic AI is characterised by the fact that it uses large databases to automatically extract specific information and *patterns* from them, so as to learn from them and thus be able to reproduce 'intelligent' behaviour.[126] As the following table shows, AI – more technically, from now on, when the term AI is used, it is meant sub-symbolic AI – is then to be considered an umbrella term that contains various forms of learning and analysing data through non-traditional

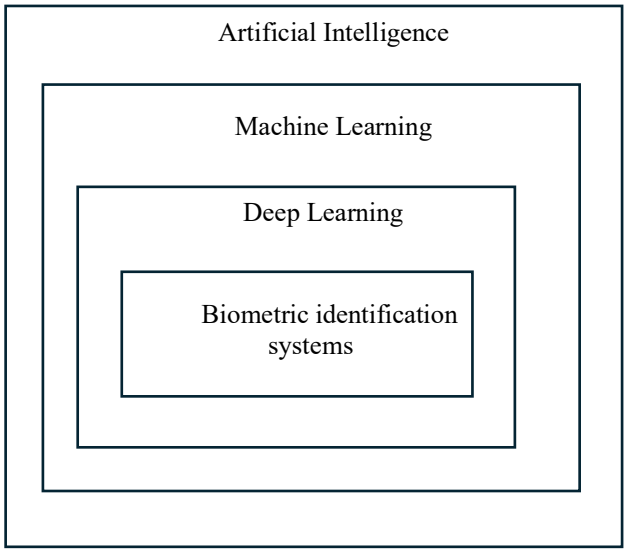
[124] Marta Garnelo and Murray Shanahan, 'Reconciling Deep Learning with Symbolic Artificial Intelligence: Representing Objects and Relations' (2019) 29 Current Opinion in Behavioral Sciences 17.

[125] Stevan Harnad, 'The Symbol Grounding Problem' (1990) 42 Physica D: Nonlinear Phenomena 335.

[126] It is to note now that, then, the so-called 'intelligence of the system is associated with this ability to learn, and not just symbolise and, therefore, reproduce behaviours. This distinction is crucial to understanding the shift from automation and autonomy that is pursued by the AI Act. On this ability to infer and the elements characterising symbolic AI Leonelli (n 116); Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business' (2019) 2019 Columbia Business Law Review 494. For a purely technical perspective, see Marvin L Minsky, 'Logical Versus Analogical or Symbolic Versus Connectionist or Neat Versus Scruffy' (1991) 12 AI Magazine 34.

algorithms. Therefore, under this umbrella term, it is to put various techniques, that vary according to "the type and specifications of the data available to learn from".[127]

Table 1 – AI and its souls.



2.2.3.3 Machine learning and deep learning

As described *supra,* the new AI techniques, such as sub-symbolic AI approaches, encompass a variety of techniques,[128] including machine learning (ML) and its subset, deep learning. In a nutshell, they can handle unstructured and complex data, making them ideal for real-world applications like autonomous vehicles, image recognition, and predictive analytics. [129]

[127] Ali Akbari, 'Facial Recognition Technologies 101: Technical Insights' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

[128] It is here recalled the classification conducted by Floridi, 'Present' (n 84).

[129] Zeng, Zhao and Li (n 43); Pin Wang, En Fan and Peng Wang, 'Comparative Analysis of Image Classification Algorithms Based on Traditional Machine Learning and Deep Learning' (2021) 141 Pattern Recognition Letters 61; Xiangyu Zhang, 'Convolutional Neural Networks and Architectures' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024) <https://doi.org/10.1007/978-3-031-43567-6_2> accessed 3 December 2024; Jacqueline G Cavazos and others, 'Accuracy Comparison across Face Recognition Algorithms: Where Are We on Measuring Race Bias?' [2020] arXiv:1912.07398 [cs] <http://arxiv.org/abs/1912.07398> accessed 3 December 2024.

Machine learning allows systems to automatically improve their performance on tasks by analysing data.[130] It employs a range of learning methods, each suited to specific types of problems.[131]

First of all, machine learning can be 'supervised', or 'unsupervised'. The supervised approach systems are trained on labelled datasets where inputs are paired with known outputs. For example, in facial recognition, the system might be trained using pairs of images labelled as "same person" or "different person" to learn how to compare facial features accurately.[132]

In an 'unsupervised' context, instead, it is the system that should identify patterns or clusters[133] within the data on its own. Saying it differently, such connections are made without receiving instructions or learning from external sources, as in the supervised learning environment. In the biometric identification context, the use of unsupervised learning might involve group analysis distinguishing people for biometric features – long neck, big mouth, small eyes – or emotions, like happiness or anger, without knowing these features before or the exact names for these emotions. Therefore, the human 'gives' to the system the data, without labelling "what we are looking for". As we will see in Chapter 3, this type of analysis is frequent in emotion recognition, biometric categorisation and real-time biometric identification systems.

Finally, the third category is 'reinforcement learning'. This approach trains systems by rewarding desired behaviours and penalising undesired ones: "[it] is used when neither the samples nor the answers are available as a batch in the beginning".[134] These systems are, for instance, used for playing video games by maximising their score through trial and error. Another example might be that of self-driving cars. It starts with no knowledge of how to drive but learns by trial and error. The system is rewarded for actions like

[130] Zhou (n 106); Julia Black and Andrew Douglas Murray, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10 European journal of law and technology; Alex M Andrew, 'REINFORCEMENT LEARNING: AN INTRODUCTION by Richard S. Sutton and Andrew G. Barto, Adaptive Computation and Machine Learning Series, MIT Press (Bradford Book), Cambridge, Mass., 1998, Xviii + 322 Pp, ISBN 0-262-19398-1, (Hardback, £31.95).' (1999) 17 Robotica 229.

[131] Ali Akbari, 'Facial Recognition Technologies 101: Technical Insights' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

[132] Id.

[133] "Bringing together sets of objects with similarities or relevant connections (documents dealing with the same objects or problems, people with similar characteristics, words with similar meanings or functions)", Sartor (n 5), p. 47. Text translated by the author of this thesis.

[134] Akbari (n 130).

staying in the correct lane, stopping at traffic lights, and avoiding collisions, while penalties are applied for running red lights or hitting obstacles.

A particular branch of machine learning is that of 'deep learning'.[135] This latter one is a specialised subset that uses neural networks to model complex, high-dimensional data. Inspired by the human brain, neural networks consist of layers of artificial neurons, each processing information and passing it to the next layer. The aim of deep learning systems is specifically to create systems that can understand and analyse human language.[136] Those systems present numerous and different applications – for instance, in the content moderation sector –[137] as well as potential challenges due to their complexity and, *ça va sans dire,* opacity.

Key architectures in deep learning include: i) Convolutional Neural Networks (CNNs), ideal for image processing tasks, CNNs are widely used in facial recognition and medical imaging; Recurrent Neural Networks (RNNs), designed for sequential data, RNNs excel in tasks like speech recognition and time-series analysis; iii) Transformer Models, these are at the heart of large language models (LLMs) like OpenAI's GPT-4, enabling advanced natural language processing and generation.[138]

Deep learning has transformed AI by enabling systems to tackle tasks that were previously thought to be impossible, such as real-time language translation and autonomous driving. However, it also introduces challenges. Neural networks often function as "black boxes," making it difficult to interpret how they arrive at their decisions. This lack of transparency raises concerns about accountability and bias, especially in high-stakes applications like hiring or criminal justice.

---

[135] "Deep-learning methods are representation-learning methods with multiple levels of representation at one level (starting with the raw input) into a representation at a higher, slightly more abstract level. With the composition of enough such transformations, very complex functions can be learned. For classification tasks, higher layers of representation amplify aspects of the input that are important for discrimination and suppress irrelevant variations […] The key aspect of deep learning is that these layers of features are not designed by human engineers; they are learned from data using a general-purpose learning procedure", Yann LeCun, Yoshua Bengio and Geoffrey Hinton, 'Deep Learning' (2015) 521 Nature 436.

[136] Andrew Jason Shepley, 'Deep Learning For Face Recognition: A Critical Analysis' [2019] arXiv:1907.12739 [cs]; Marta Garnelo, Kai Arulkumaran and Murray Shanahan, 'Towards Deep Symbolic Reinforcement Learning' (arXiv, 1 October 2016).

[137] Pollicino and Dunn, 'IA e Valori Democratici' (n 123).

[138] LeCun, Bengio and Hinton (n 63); Ziwei Liu and others, 'Generative Networks' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024) <https://doi.org/10.1007/978-3-031-43567-6_3> accessed 3 December 2024; Zhang (n 57).

2.2.3.4 What about FRT?

Facial Recognition Technology (FRT) serves as a practical and impactful application of AI since it integrates techniques from ML and deep learning to achieve its objectives. This chapter aimed, therefore, to set the base for understanding the connection between AI, ML, and deep learning, particularly in the context of FRT, to reveal how these technologies evolve to address complex challenges and risks. As a matter of fact, the evolution of FRT reflects the transition from symbolic to subsymbolic AI.[139]

As Chapter 3 will further analyse, initially, FRT systems relied on symbolic AI, whilst more recent systems are based on sub-symbolic ones. Deep learning further revolutionised FRT by introducing CNNs: in this way, it is possible to extract and analyse features from facial images. These networks process images through successive layers, each focusing on increasingly detailed features.[140]

Thus, FRT illustrates the practical application of the synergy between AI, ML, and deep learning, revealing their transformative potential alongside inherent risks. While these technologies offer remarkable adaptability, they also introduce ethical and technical challenges, particularly in areas where fundamental rights and societal norms are at stake. These challenges highlight the critical need for governance frameworks that address not only the technological aspects but also the broader implications for society.

The shift from automation to autonomy, as exemplified by AI systems, lies at the heart of these governance concerns. This transition signifies a paradigm where systems are no longer confined to executing pre-programmed instructions but instead operate with varying degrees of independence, learning, adapting, and evolving in response to their environments. The AI Act aims to address precisely this shift, acknowledging the unique risks and opportunities posed by autonomous AI systems. This framework represents a pioneering effort to regulate the complexities introduced by AI technologies, that are constantly eroding the human control over such results, either because of the opacity of the system, its complexity, or its increasing use in highly sensitive areas, such as law enforcement.

---

[139] Akbari (n 130).

[140] Anirudha Ghosh and others, 'Fundamental Concepts of Convolutional Neural Network' in Valentina E Balas, Raghvendra Kumar and Rajshree Srivastava (eds), *Recent Trends and Advances in Artificial Intelligence and Internet of Things* (Springer International Publishing 2020).

However, as this chapter transitions into the legal analysis, it becomes clear that the challenges extend beyond the technical domain. The opacity of subsymbolic methodologies, the systemic risks associated with deep learning, and the ethical dilemmas posed by FRT demand a multidisciplinary approach.

Thus, the legal analysis that follows will delve into how the AI Act responds to this evolution, providing a regulatory framework to reconcile the technological shift from automation to autonomy with the preservation of democratic principles and the protection of fundamental rights. This interplay between technological innovation and legal governance underscores the importance of addressing AI's societal impact with a comprehensive and principled approach.

2.3 From automation to autonomy

The evolution from automated processes to autonomous systems has profound implications, raising urgent questions about accountability, ethics, and the balance of power between humans and machines.[141] The key issue is no longer just about when and how AI should be deployed, but how its autonomous nature impacts core democratic principles, including transparency, accountability, and human dignity.[142]

This transition is usually exemplified by the addition of the word "smart" alongside everything that becomes digitised. This is how smart cities are emerging alongside smart borders, smart policing, and even smart governance frameworks, reshaping traditional decision-making processes.[143] One striking example of this shift is the increasing use of AI in biometric surveillance, particularly in law enforcement. While early algorithmic systems primarily served to assist human decision-making by analysing vast amounts of

[141] Eleni Kosta, "Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights," *Regulation & Governance* 16, no. 1 (2022): 212–24.

[142] Andrea Simoncini and Erik Longo, "Fundamental Rights and the Rule of Law in the Algorithmic Society," in *Constitutional Challenges in the Algorithmic Society*, ed. Hans-W. Micklitz et al. (Cambridge University Press, 2021), 27–41, https://doi.org/10.1017/9781108914857.003.

[143] One crushing example of the step toward further automation of the decision making in the migration sector, especially in border management. The topic is analysed by Melanie Fink, 'Robo Swarms and Polygraphs: The Future of European Border Management and Its Costs' (2 July 2024) <https://papers.ssrn.com/abstract=4883130> accessed 3 December 2024.

data,[144] AI-driven systems now possess the capability to make decisions autonomously, for their technical advances described *supra.*[145]

This change is more than a technical enhancement; it alters the dynamics of governance, as AI assumes responsibilities traditionally held by humans, including tasks that directly affect constitutional rights such as freedom of expression, privacy and data protection.

Moreover, this change is reflected by the definition that the AI Act adopted for AI systems[146] AI as "a machine-based system designed to operate with varying levels of autonomy."[147] In this context, autonomy refers to the ability of AI systems to act independently of human intervention, making decisions or taking actions without requiring constant oversight.[148] Adaptiveness, on the other hand, highlights the self-learning capabilities of these systems, allowing them to evolve, improve, or modify their behaviour over time as they interact with data and environments.

However, what truly distinguishes AI from conventional software is its ability to "infer." While traditional software operates through predefined, step-by-step instructions set by developers, AI systems possess the capacity to analyse data, draw conclusions, and make decisions without explicit human direction. This ability to infer empowers AI systems to engage in higher-order tasks like learning, reasoning, and modelling, moving far beyond basic data processing.[149]

---

[144] Karen Yeung, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation & Governance 505.

[145] There are many areas in which AI is used and which affect the fundamental rights of individuals. Among others, it is to mention the law enforcement sector Sascha van Schendel, *Regulating Risk Profiling by Law Enforcement: A Task for Data Protection Law, Non-Discrimination Law and Criminal Procedural Law*, Tilburg University, 2024. Also allow the reference to Federica Paolucci, 'From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights' (1 August 2024) <https://papers.ssrn.com/abstract=4929132> accessed 3 December 2024.

[146] It is to note that the AI Act does not define AI, but just AI systems.

[147] AI Act, Art. 3, para. 1, no. 1). As mentioned *supra,* this definition is borrowed by the OECD.

[148] AI Act, Rec. 12. See also Martin Ebers and others, 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 J 589; Nathalie A Smuha and Karen Yeung, 'The European Union's AI Act: Beyond Motherhood and Apple Pie?' (24 June 2024) <https://papers.ssrn.com/abstract=4874852> accessed 3 December 2024.

[149] AI Act, Rec. 12, "include machine learning approaches that learn from data how to achieve certain objectives; and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved", with either implementation going "beyond basic data processing" and enabling "learning, reasoning or modelling". Hence, the AI Act further elaborates on the techniques that enable this inference capability. Two main approaches are identified: machine learning methods, which allow systems to learn from data and adapt to achieve certain objectives, and logic- or knowledge-based approaches, which use encoded rules or symbolic reasoning to solve tasks. Both approaches enable AI systems to function in a way that is not only independent but also dynamic, adapting to new data and situations.

This perspective underscores the complexity of AI systems compared to traditional software. AI's ability to continuously learn, reason, and improve makes it a transformative technology that requires specific regulatory oversight.[150]

Such an evolution – that in technical terms marked the passage from symbolic to sub-symbolic AI – is specifically characterised by the shift from algorithmic governance to AI-driven one: this passage represents a profound transformation of the regulatory landscape.[151]

As a matter of fact, the term 'algorithmic governance' traditionally refers to the use of automated decision-making (ADM) systems that process large volumes of data based on pre-defined criteria.[152] ADM, in this context, involves using algorithms, a sequence of steps expressed in mathematical or logical terms, embedded within decision-making processes.[153] These systems range from fully automated decisions to hybrid approaches – i.e., purely automated decisions, automated triage, automated suspects and automated trials[154] – where algorithmic outputs assist human decision-making.[155] However, a recurring challenge lies in ensuring that these outputs do not merely shift responsibility away from human actors or obscure accountability through their complexity and opacity.[156]

---

[150] As autonomy increases, assigning responsibility becomes gradually difficult, given the diminished importance or relevance or "control over the system due to its high degree of autonomy and capacity for self-learning", cit. Anetta Jedličková, 'Ethical Approaches in Designing Autonomous and Intelligent Systems: A Comprehensive Survey towards Responsible Development' [2024] AI & SOCIETY <https://doi.org/10.1007/s00146-024-02040-9> accessed 3 December 2024.

[151] "Algorithmic technologies are not only instruments to exercise powers, which can interfere with fundamental rights, but can also be considered as rule-makers", in Giovanni De Gregorio, 'The Normative Power of Artificial Intelligence' (2023) 30 Indiana Law Journal .

[152] Simona Demková, *Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023); Stine Lomborg, Anne Kaun and Sne Scott Hansen, 'Automated Decision-Making: Toward a People-Centred Approach' (2023) 17 Sociology Compass e13097.

[153] Madalina Busuioc, 'Accountable Artificial Intelligence: Holding Algorithms to Account' (2020) 81 Public Administration Review.

[154] According to scholarly analysis, ADM can be classified as: solely automated decisions, automated triage, automated suspicion, and automated evidence. For a taxonomy of ADM see Francesca Palmiotto, 'When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis' (2024) 25 German Law Journal 210.

[155] Explanation and reasoning are the key aspects that, as a matter of fact, trigger the put into place of these technologies in the public actors' duties. On the duty of reasons of administrative law, see M Fink and M Finck, 'Reasoned A(I)Dministration: Explanation Requirements in EU Law and the Automation of Public Administration' (2022) 47 European Law Review 376.

[156] Rodríguez distinguishes between *output* types. The classification is based on the position of the 'data subject' and its relationship to the output of ADM. The first category of possible outputs of ADM includes evaluations, rankings, predictions, recommendations or classification of content. The ADM lists, classifies, ranks, filters, ranks or recommends. The second category of output concerns decisions made by the WMD

While ADM systems have traditionally involved structured, rule-based automation, the emergence of AI introduces a layer of autonomy and adaptability, enabling systems to learn and evolve beyond static criteria.[157] Unlike traditional algorithms, AI systems leverage advanced methodologies, such as machine learning, to generate outputs that are not always easily explainable, raising significant concerns about transparency, fairness, and accountability. [158] This shift from structured automation to autonomy represents a profound challenge for constitutional law, which has not yet fully adapted to address the opacity, adaptability and unpredictability of these systems.[159] Moreover, as Demkova highlights, the right to human oversight and the ability to contest algorithmic decisions are safeguards that must be robustly implemented to mitigate the risks associated with ADM systems and uphold fundamental rights.[160] Especially, as also underscored by Pasquale, the risk of the rising AI autonomy is that of eroding individuals, trivializing concepts, like the rule of law, "a system of social relationships and legitimate governance, not simply the transfer and evaluation of information about behaviour".[161]

From a technical point of view, the opacity of ADM systems, often described as a 'black-box', *supra*, complicates efforts to ensure transparency and accountability, both of which are foundational to constitutional governance.[162] In turn, in the legal environment, it has been advocated for a 'right to explanation' of the automated decision, based on an interpretation of Article 22 of the GDPR.[163] While this provision seeks to provide transparency by requiring meaningful information about the logic, significance, and consequences of ADM it has been criticised for its vagueness and limited practical

concerning the person concerned. In these cases, the person interacting with the ADM is directly affected. Teresa Rodríguez de las Heras Ballell, 'Guiding Principles for Automated Decision-Making in the EU' (2022) ELI Innovation Paper 28.

[157] Id.

[158] Edwards and Veale (n 122).

[159] Fink (n 59). For a technical point of view, Mohsen Soori, Behrooz Arezoo and Roza Dastres, 'Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics, a Review' (2023) 3 Cognitive Robotics 54.

[160] Simona Demková, *Automated Decision-Making and Effective Remedies : The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice*, Elgar Studies in European Law and Policy (Cheltenham, UK: Edward Elgar Publishing, 2023); Stine Lomborg, Anne Kaun, and Sne Scott Hansen, "Automated Decision-Making: Toward a People-Centred Approach," *Sociology Compass* 17, no. 8 (2023):13097.

[161] Pasquale, 'A Rule of Persons, Not Machines' (n 115).

[162] Olsen and others (n 81).

[163] Ljubisa Metikos, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188; Finale Doshi-Velez and others, 'Accountability of AI Under the Law: The Role of Explanation' [2017] arXiv.org; Chiara Gallese, 'The AI Act Proposal: A New Right to Technical Interpretability?' (arXiv, 14 March 2023) <http://arxiv.org/abs/2303.17558> accessed 3 December 2024.

applicability.[164] This complexity, paired with the risk of superficial compliance by organisations, underscores the inadequacy of current mechanisms to ensure accountability.

Recently, the legal debate has been coupled also with the technical one, resulting in a shift from concepts like "explainable AI" or xAI:[165] since the explanations, while necessary, do not always lead to genuine understanding, it is urged, instead, to strive for "understandable AI" (uAI), meaning going beyond mere explanation to focus on fostering understanding.[166] Particularly, from a technical perspective, this shift can be achieved by building a framework that includes incoming propositions, knowledge bases, knowledge fusion, and confidence-change mechanisms to foster genuine understanding. This system will ensure that explanations are aligned with the users' existing knowledge base and cognitive processes.[167] Saying it in simple words, on the one hand, the purpose of xAI is to explain the internal workings of the model — for instance, by breaking down decisions into understandable components,[168] creating *post-hoc* explanations, or simplifying the model to make it interpretable;[169] on the other hand, understandable AI goes beyond merely explaining how decisions are made. It emphasizes creating AI systems that foster

[164] Critics argue that Article 22 does not explicitly mandate full explanations but only "meaningful information," leaving ambiguity about what level of transparency is sufficient. Furthermore, ADM systems, particularly those based on machine learning, make it difficult to offer clear, actionable insights into their decision-making processes. Edwards and Veale (n 122); Fink and Finck (n 158); Wachter, Mittelstadt and Floridi (n 122).

[165] Explainable AI refers to methods and techniques in artificial intelligence (AI) that make the functioning of AI models understandable to humans. The primary objective of xAI is to ensure that the decisions and actions made by AI systems can be interpreted and explained, thereby fostering trust, transparency, and accountability. In particular, xAI aims to provide insights into the internal mechanisms of complex AI models, such as neural networks, which are often considered "black boxes" due to their opacity. 'Explainable AI (XAI)', in Keri Grieman, *Law, Death, and Robots: The Regulation of Artificial Intelligence in High-Risk Civil Applications* (1st ed., Hart Publishing 2024).

[166] Hussein Abbass and others, 'Editorial: From Explainable Artificial Intelligence (xAI) to Understandable Artificial Intelligence (uAI)' (2024) 5 IEEE Transactions on Artificial Intelligence 4310.

[167] Víctor Rodríguez-Doncel and others, 'Introduction: A Hybrid Regulatory Framework and Technical Architecture for a Human-Centered and Explainable AI' in Víctor Rodríguez-Doncel and others (eds), *AI Approaches to the Complexity of Legal Systems XI-XII* (Springer International Publishing 2021).

[168] "Requiring every AI system to explain every decision could result in less efficient systems, forced design choices, and a bias towards explainable but suboptimal outcomes. For example, the overhead of forcing a toaster to explain why it thinks the bread is ready might prevent a company from implementing a smart toasting feature—either due to the engineering challenges or concerns about legal ramifications. On the other hand, we may be willing to accept the monetary cost of an explainable but slightly less accurate loan approval system for the societal benefit of being able to verify that it is nondiscriminatory." Doshi-Velez and others (n 166).

[169] Abbass and others (n 169).

a deep understanding for users, especially non-experts.[170] uAI focuses on aligning the system's explanations with the user's cognitive processes and prior knowledge to ensure that users not only receive an explanation but also comprehend it fully. In a nutshell, uAI seeks to make AI models and their outputs more intuitive and meaningful to a wider range of users.

The implications from a legal standpoint are such that appeared in a recent ruling by the Constitutional Court of Colombia underscores the importance of human oversight in AI-driven decision-making. In this case, a judge used ChatGPT 3.5 to assist in drafting a legal decision.[171] The court affirmed that while AI can complement human judgment, it must not replace it. The judge did not rely on AI to resolve the case but rather employed it as a tool to assist in writing the decision, based on reasoning provided by the judge. This case illustrates how AI can be integrated into decision-making in a way that respects human authority and maintains a clear boundary between assistance and autonomy.[172]

Coming back to the European Union context, in the *Schufa* ruling by the Court of Justice of the European Union (CJEU), it emerged that what constitutes "automated decision-making" is not only the actual output of algorithmic analysis.[173] The CJEU established that even if a human is involved in the final decision-making process – e.g., a bank deciding whether to grant a loan – if an automated system, as a credit scoring algorithm, plays a key role in influencing that decision, it may still qualify as automated decision-making under data protection laws. This ruling posed attention to a crucial matter: it is to be considered from a legal stand, not only the "algorithmic output", but the result as a whole, even though a human is involved in the final stage.[174] Essentially, the court found that while the final decision to grant or deny credit may involve human intervention, the credit score itself plays a crucial role in that decision-making process.

[170] Brent Daniel Mittelstadt and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society 2053951716679679.
[171] República de Colombia Corte Constitucional, Ruling T-323/2024, in particular paras. 422-424.
[172] Id., para. 424, lett. i).
[173] Court of Justice of the European Union, Judgment of 7 December 2023, *OQ v Land Hessen*, C-634/21, ECLI:EU:C:2023:957.
[174] Asymina Aza, 'Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context' [2024] Industrial Law Journal dwae035; Gianluca Fasano, 'L'interpretazione estensiva della nozione di "decisione automatizzata" ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali' (2024) 6 Rivista italiana di informatica e diritto 15.

As such, the automated calculation of the credit score is an integral part of the overall automated decision-making process.

Henceforth, the turn from algorithmic governance to AI governance represents a profound transformation in the regulatory landscape, where this shift is essentially driven by the increasing reliance on technological autonomy.[175] This transition, fueled by the increasing reliance on autonomous and adaptive AI systems, fundamentally alters the dynamics of accountability and oversight, necessitating a rethinking of regulatory structures. While algorithmic governance focuses primarily on automating pre-existing rules and processes, AI governance introduces complexities tied to self-learning systems, opaque decision-making, and far-reaching societal impacts. Building on this evolution, the next section delves into the regulatory challenges posed by these advanced systems, exploring how AI technologies, particularly through high-profile cases like COMPAS, Clearview AI, and OpenAI, have forced lawmakers to grapple with fundamental rights implications. These incidents highlight the urgent need for proactive and comprehensive frameworks, as reactive measures have struggled to address the rapidly evolving risks of AI deployment.

2.3.1 The power of autonomy: new unprecedented challenges

The emergence of AI autonomy marks a pivotal shift in the landscape of digital governance, with far-reaching implications for constitutional principles and regulatory frameworks. As remarks Pollicino, studying the features of this new era,

> "The autonomy of AI systems challenges traditional notions of accountability and oversight, prompting scholars and policymakers to seek new frameworks that can properly regulate these technologies while upholding constitutional values such as democracy, the rule of law, and fundamental rights. For example, the lack of transparency of some AI decisions may pose a direct challenge to the

[175] As observed by De Gregorio, "Algorithmic technologies are not only instruments to exercise powers, which can interfere with fundamental rights, but can also be considered as rule-makers", in De Gregorio, 'The Normative Power of Artificial Intelligence' (n 5)., id.

constitutional principle of due process, which requires that decisions, particularly those affecting the rights of individuals, be understandable and appealable".[176]

In particular, Pollicino understands this crucial evolution through the different phases of digital constitutionalism.[177] Specifically, the first era revolved around addressing the power of platforms like Google, Facebook, and Amazon, ensuring they remained accountable within a framework of fundamental rights and democratic oversight. This era, often described as the first phase of was largely reactive, as courts like the Court of Justice of the European Union (CJEU) played a pivotal role in translating traditional constitutional principles to the digital sphere.[178]

However, as the algorithmic society gave way to the rise of AI-driven autonomy, the regulatory focus expanded.[179] No longer confined to holding platforms accountable, governance now faces the challenge of managing systems capable of self-learning, adaptation, and decision-making beyond explicit human instructions.[180]

Consequently, a second phase, oriented towards the development of regulatory frameworks, started, e.g., with the General Data Protection Regulation (GDPR)[181]: it was specifically designed to impose checks on the power of these platforms, ensuring that they did not violate individual rights.

Moreover, since the second half of the 2010s, the EU has adopted a series of sector-specific legislative measures aimed at introducing new obligations for providers – and especially for hosting service providers – in order to make them more responsible for combating illegal conduct and material online. Thus, with the Directive (EU)

[176] Pollicino, 'Regolare l'Intelligenza Artificiale: La Lunga via Dei Diritti Fondamentali' (n 90). Text translated by the author.
[177] Pollicino, 'Potere Digitale' (n 3).
[178] The aspects hereby mentioned have been further analyzed in Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Bloomsbury Publishing 2021).
[179] Pollicino, 'Potere Digitale' (n 3).
[180] As emphasised by Pollicino, "The increasing autonomy of such technologies raises crucial questions about how democratic decision-making processes can be influenced or distorted by the massive use of artificial intelligence in sensitive areas such as political communication, information and even predictive analysis for electoral purposes", Pollicino, 'Regolare l'Intelligenza Artificiale: La Lunga via Dei Diritti Fondamentali' (n 90). Text translated by the author.
[181] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2018/1808,[182] the legislator amended the audiovisual market regulation, introducing a series of obligations for providers of video-sharing platforms; the Directive (EU) 2019/790 innovated in the field of copyright to adapt the sector legislation to the new challenges of the Internet;[183] the Regulation (EU) 2021/784 introduced a specific discipline aimed at combating online terrorist content.[184] Moreover, in 2022, with the approval of the Digital Services Act (DSA) a general and, so to speak, 'horizontal' reform of the European regulatory framework on the moderation of online content was finally carried out.[185] Hence, the second phase represents a procedural turn, where the focus shifted towards creating robust mechanisms for ensuring transparency, accountability, and the enforcement of digital rights, by giving more and more supervisory powers to the European Commission.[186]

This evolution represents a profound transformation in the regulatory landscape—one that demands a shift from principles of algorithmic governance to those capable of addressing the complexities of AI autonomy. Autonomous systems, unlike traditional automated processes, introduce novel challenges due to their ability to function without human oversight, relying on self-learning mechanisms and adaptive algorithms. While these capabilities enable unprecedented efficiency and innovation, they also pose risks to transparency, accountability, and the protection of fundamental rights. These challenges are particularly acute in areas like law enforcement, where AI's capacity for autonomous decision-making directly impacts privacy, non-discrimination, and other core rights.[187] The pervasive influence of the algorithmic society extends beyond information management into various other contexts, such as healthcare, labour, justice, and public

[182] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, 2018 O.J. (L 303) 69.

[183] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the digital single market and amending Directives 96/9/EC and 2001/29/EC.

[184] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, 2021 O.J. (L 172) 79.

[185] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

[186] Pieter Van Cleynenbreugel, 'The Commission's Digital Services and Markets Act Proposals: First Step towards Tougher and More Directly Enforced EU Rules?' (2021) 28 Maastricht Journal of European and Comparative Law 667.

[187] Luciano Violante, "Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi," *BioLaw Journal - Rivista di BioDiritto*, no. 1 (April 12, 2022): 145–53.

security. In these sectors, too, we witness the widespread adoption of automated decision-making systems, which not only reinforce the role of algorithms but also highlight the increasingly intertwined relationship between public and private entities. This growing presence of private actors in traditionally public domains underscores a significant shift in governance structures.[188]

However, as we transition from an algorithmic society to one increasingly driven by AI, this shift takes on even greater complexity. Moreover, the development of the AI regulatory framework discussed in this chapter was a direct response to the profound effects these systems were having on fundamental rights and societal norms. These regulations often emerged as reactive measures, spurred by public outrage over specific incidents where AI technology demonstrated its capacity to infringe on human rights.

A particularly prominent example is the use of COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), an algorithm used in the U.S. criminal justice system to evaluate the likelihood of recidivism. This tool faced significant criticism for perpetuating racial bias, disproportionately labelling Black defendants as high-risk compared to their white counterparts.[189] Such bias undermined the fundamental rights to equality and a fair trial, as COMPAS-influenced decisions directly impacted sentencing and parole outcomes.[190] The opaque nature of the algorithm exacerbated the problem, as individuals had little insight into or recourse against the automated decisions.[191] This lack of transparency in decision-making processes posed serious concerns about due process and the right to a fair and impartial trial, two cornerstones of justice in democratic societies.[192]

---

[188] The shift powerfully described by Balkin as the "Algorithmic Society", Balkin (n 111).

[189] *State v. Loomis*, 881 N.W.2d 759 (Wis. 2016).

[190] Julia Angwin Mattu Jeff Larson,Lauren Kirchner,Surya, 'Machine Bias' (*ProPublica*) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 3 December 2024. See also, Erik Longo, 'Predizione, Profilazione e Giustizia: Le Prospettive Costituzionali', *Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche* (Edizioni Scientifiche Italiane 2022).

[191] Francesca Lagioia, Riccardo Rovatti and Giovanni Sartor, 'Algorithmic Fairness through Group Parities? The Case of COMPAS-SAPMOC' (2023) 38 AI & SOCIETY 459.

[192] As observed by Simoncini, the outcome of the US Supreme Court did not spark a violation on the right to "due process". Even though the use of these tools may, in fact, give rise to constitutionally relevant issues, but, in the present case, it reiterates the diriment argument of non-exclusivity: the algorithm was not the sole reason for the decision and, hence, was found to not being violating the principle of "due process". Andrea Simoncini, 'L'algoritmo Incostituzionale: Intelligenza Artificiale e Il Futuro Delle Libertà' (2019) 15 BioLaw Journal-Rivista di BioDiritto 63.

Another high-profile incident was the Clearview AI scandal, which revealed that the company had scraped billions of images from social media without user consent to build a facial recognition database for law enforcement use.[193] The widespread deployment of this technology, often without adequate public oversight, raised serious concerns about the right to privacy and data protection. Clearview AI's practices were particularly alarming as they infringed on individuals' control over their personal data, enabling unwarranted surveillance and tracking without their knowledge or consent.[194] This form of pervasive surveillance also had broader implications for freedom of expression and assembly, as individuals might hesitate to exercise these rights under the belief they were being constantly monitored. The case sparked international debates on the ethical use of facial recognition technology and highlighted its potential for misuse by both public and private entities.[195]

In addition to these cases, the rise of generative AI has introduced new regulatory challenges, as demonstrated by the OpenAI case in Italy in 2023.[196] Specifically, the Italian Data Protection Authority (DPA, or Garante) temporarily banned OpenAI's ChatGPT due to concerns over the unlawful collection and processing of personal data, and the lack of adequate mechanisms to prevent minors from accessing the platform. The case raised questions about how generative AI systems collect, store, and use personal information, especially when operating at such large scales.[197]

The Garante ordered OpenAI to implement stronger privacy safeguards and transparency measures, including age verification tools and greater user control over their data. The incident attracted widespread attention, marking the first regulatory action taken

[193] The case was addressed by numerous authorities: especially the Italian Data Protection Authority (DPA, Garante) fined the US-based company Clearview AI EUR 20 million after finding it applied what amounted to biometric monitoring techniques also to individuals in the Italian territory, and it impeded the processing of biometric data of Italian citizens. Italian DPA, Injunction Order against Clearview AI - 10 February 2022, Register of Measures, No. 50 of 10 February 2022. A similar direction was followed by the French Supervisory Authority (CNIL), Deliberation of the restricted committee N° SAN-2022-019 of 17 October 2022 concerning Clearview AI.

[194] The case and its far-reaching data protection and fundamental rights implications have also been analysed in this contribution:

[195] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' *The New York Times* (18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> accessed 3 December 2024.

[196] Italian DPA, Measure of 30 March 2023, Register of Measures, No. 112 of 30 March 2023.

[197] Gianluigi M Riva, 'Diritto e Intelligenza Artificiale Generativa: L'istruttoria Del Garante per La Protezione Dei Dati Italiano Su OpenAI e ChatGPT' [2024] Ciberspazio e diritto : rivista internazionale di informatica giuridica : 25, 1, 2024 153.

against a major generative AI system in Europe. As a consequence of this huge societal echo, the regulation of such systems entered the radar of the European legislator, which eventually included specific provisions first European law on AI.[198]

Henceforth, the episodes involving COMPAS, Clearview AI, and OpenAI highlight the urgent need for comprehensive AI regulations, particularly in light of the growing autonomy of these systems. AI's ability to function independently – learning, adapting, and making decisions with minimal human intervention – raises profound concerns about safeguarding fundamental rights. Issues such as discrimination, bias, privacy violations, and data security are exacerbated by the opacity and unpredictability inherent in autonomous AI systems. These cases reveal a pattern of reactive regulation, where lawmakers address specific incidents only after harm has occurred, rather than proactively anticipating the broader challenges posed by AI's autonomous capabilities. This reactive approach has created a precarious "cat-and-mouse" dynamic, with legislators scrambling to address the consequences of increasingly autonomous systems while struggling to develop long-term, comprehensive frameworks. As AI continues to evolve, this cycle of reactionary governance risks leaving significant gaps in oversight, exposing society to ongoing and unforeseen vulnerabilities. By failing to account for the unique challenges of AI autonomy, current regulatory efforts may fall short of effectively addressing the transformative and disruptive potential of these technologies.

Furthermore, the growing autonomy of AI systems marks a pivotal transformation in both technological innovation and regulatory requirements, presenting unprecedented challenges to traditional governance structures. This evolution highlights the pressing need for a forward-thinking regulatory approach: one that not only addresses immediate risks but also anticipates the broader societal and legal consequences of increasingly independent AI technologies.

In this context, the AI Act, introducing a risk-based framework specifically designed to tackle the challenges of AI autonomy, by focusing on high-risk systems and emphasising safeguards for transparency, accountability, and fundamental rights, aims to establish a model that aligns technological innovation with democratic values. As the discussion shifts from understanding the concept of autonomy to addressing its regulatory

[198] European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for an Artificial Intelligence Act, COM(2021)0206 – C9-0146/2021 – 2021/0106(COD), Amendment 168.

implications, the AI Act is going to be in-depth analysed to explore its mechanisms, objectives, and implications, particularly how it addresses the challenges posed by AI systems while balancing innovation, autonomy, and the protection of fundamental rights.

2.4 The Artificial Intelligence Act

> "Europe's fundamental values are prosperity, equity, freedom, peace and democracy in a sustainable environment. The EU exists to ensure that Europeans can always benefit from these fundamental rights."[199]

Europe's core values are indeed deeply embedded in the European Union's legal framework and guide its response to emerging challenges, including AI,[200] whilst ensuring that this technology does not undermine the rights it is committed to protecting.[201] The AI Act marks a significant step in balancing technological advancement with the preservation of fundamental rights such as privacy, data protection, freedom of expression, and non-discrimination.[202] Furthermore, the regulation of AI in Europe is not just about mitigating risks but also fostering innovation that aligns with core European values, the alignment of which is the object to be evaluated by this work.

The regulation's ambition lies in establishing a "new" legal framework tailored to the complexities of AI technologies. As outlined in its objectives, the Act promises to ensure that AI available within the Union market – or impacting individuals within its jurisdiction – remains human-centric, trustworthy, safe, and respectful of fundamental rights.[203] Building on the EU's regulatory tradition seen in instruments like the GDPR and the DSA,[204] the AI Act adopts a risk-based approach, classifying AI systems into tiers

[199] Draghi (n 76).

[200] See European Commission, Explanatory Memorandum, Proposal For a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,{Sec(2021) 167 Final} - {Swd(2021) 84 Final} - {Swd(2021) 85 Final}.

[201] Anu Bradford, 'Europe's Digital Constitution' [2023] Verfassungsblog <https://verfassungsblog.de/europes-digital-constitution/> accessed 3 December 2024. As also noted by Finocchiaro, "Europe relies on regulation, while the US creates a shared path with large American companies", Finocchiaro (n 88).

[202] AI Act, Rec. 1-3.

[203] Explanatory Memorandum published within the proposal for a Regulation of the European Parliament and of the Council, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21.4.2021, COM(2021) 206 final.

[204] Pietro Dunn and Giovanni De Gregorio, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review.

according to the level of risk they pose.[205] This stratified framework seeks to safeguard rights, promote transparency, and foster trust while maintaining a competitive single market within the EU.

Through this lens, this work critically examines the AI Act, focusing on its general framework, regulatory mechanisms, and their implications for fundamental rights and autonomy.[206] At the heart of this paragraph lies a critical question: does the AI Act, as a pioneering regulatory framework, effectively address the unique challenges posed by autonomous AI systems, particularly in contexts where FRT is deployed, or does it fall short, leaving critical gaps that could compromise the fundamental rights it seeks to protect? The forthcoming analysis focuses on the key features of the AI Act, which serve as a foundational framework for understanding its regulatory approach FRT, analysed in Chapter 3.

2.4.1 Objectives of the Regulation: between product safety and fundamental rights

The AI Act marks a significant step in balancing technological advancement with the preservation of fundamental rights such as privacy, data protection, freedom of expression, and non-discrimination.[207] At the same time, the regulation of AI in Europe is not just about mitigating risks but also fostering innovation that aligns with core European values. This purpose is specifically symbolised by Article 1 of the AI Act, which sets the subject matter of the Regulation and specifies that

> "the purpose […] is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, and fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation."

[205] In particular, Annex III further specifies Art. 6 of the AI Act and lists the AI systems which are considered "by default" by the EU legislator "high risk".
[206] AI Act, rt. 3, para. 1, no. 2), "risk means the combination of the probability of an occurrence of harm and the severity of that harm".
[207] Ibid, Rec. 1-3.

Indeed, the AI Act emerges as a bold attempt to chart the uncertain waters of AI regulation, striving to strike a balance between innovation and the protection of fundamental rights. At its core, the AI Act is primarily a product safety regulation, designed to ensure that AI systems are safe for public use and comply with specific technical standards.[208] This classification places the AI Act within the broader framework of EU legislation aimed at regulating products,[209] like the General Product Safety Regulation.[210] The AI Act adopts indeed a product-oriented approach to regulate AI technologies based on safety thresholds before being placed on the market.[211]

However, this focus on product safety creates tension with the need to protect fundamental rights. While the AI Act imposes stringent requirements for high-risk AI systems, particularly in sensitive areas like biometric surveillance, it may not fully address the broader societal and ethical challenges posed by AI autonomy. The risk-based classification, rooted in product safety logic, may overlook the subtleties of how AI systems impact human rights in non-technical contexts, such as the potential for AI to erode democratic values through surveillance or biased decision-making.[212]

More importantly, the AI Act clearly has two souls. Being a product safety regulation, as mentioned, the AI Act is strongly focused on the rule about the development, training, while it also aims to protect fundamental rights and, broadly, European values as enshrined in Article 2 TEU. This means that rather than focusing solely on the creation or development of these AI systems, the regulation imposes specialised rules that govern their specific uses, outlining the modalities, limitations, and conditions under which such technologies can be deployed. This clash between product safety regulation and fundamental rights protection becomes especially evident when the AI Act tries to contemplate its two souls as in the case of the Fundamental Rights Impact Assessments

[208] Nikos Th Nikolinakos, *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act / by Nikos Th. Nikolinakos.* (1st ed. 2023., Springer International Publishing 2023).

[209] Marco Almada and Nicolas Petit, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (18 October 2023) <https://papers.ssrn.com/abstract=4308072> accessed 3 December 2024.

[210] Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC.

[211] AI Act, Section 5 (Artt. 40-49) on Standards and Conformity Assessments.

[212] Nathalie A Smuha and Karen Yeung, 'The European Union's AI Act: Beyond Motherhood and Apple Pie?' (24 June 2024) <https://papers.ssrn.com/abstract=4874852> accessed 3 December 2024.

for high-risk AI systems.[213] Still, the reliance on a technical, compliance-based framework under the AI Act could leave gaps in addressing the deeper societal risks posed by these technologies.

The AI Act's general framework primarily focuses on ensuring AI systems meet specific technical and safety standards before they are placed on the market. This includes requirements related to data quality during the training phase, transparency requirements, and post-market monitoring.[214] However, when it comes to uses which can impact fundamental rights and democratic values, as in the case of biometric systems, particularly those used for real-time remote identification in public spaces, the regulation takes a more detailed and restrictive approach. These systems are classified as prohibited or high-risk not only because of their technical complexity but also due to the significant constitutional concerns they raise.

Furthermore, the AI Act introduces a *lex specialis* specifically for biometric technologies. As a matter of fact, Recital 38 states:

> "The use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner".

This means that rather than focusing solely on the creation or development of these AI systems, the regulation imposes specialised rules that govern their specific uses, outlining the modalities, limitations, and conditions under which such technologies can be deployed. The emphasis is thus on how biometric technologies are applied in real-world contexts, ensuring their use adheres to fundamental rights and democratic values. Hence, unlike other AI systems that are governed through general principles aimed at ensuring product safety and transparency, biometric technologies receive special attention because of their profound impact on fundamental rights, as the thesis aims to unpack.

[213] AI Act, Art. 27.
[214] Ibid., Arts. 8-15.

The AI Act's general framework primarily focuses on ensuring AI systems meet specific technical and safety standards before they are placed on the market. This includes obligations related to data quality during the training phase, transparency requirements, and post-market monitoring.[215] However, when it comes to biometric systems, particularly those used for real-time remote identification in public spaces, the regulation takes a more detailed and restrictive approach. These systems are classified as prohibited or high-risk not only because of their technical complexity – rather they are quite simpler than Generative AI – but also due to the significant ethical and societal concerns they raise.

Differently, the *lex specialis* provisions for biometric systems go beyond the general safety and transparency obligations. They regulate specific uses of biometric technologies in sensitive contexts, focusing on their implementation rather than just their design or market entry. For example, real-time biometric surveillance, commonly used in law enforcement, is permitted only under strict circumstances where the need for such technologies should be clearly justified. This direct focus on implementation reflects the heightened concern over how these systems are deployed in practice, rather than simply ensuring their compliance as products.

2.4.2 Material and territorial scope

The scope of the AI Act is defined by its Art. 2,[216] establishing that the Regulation applies to providers, meaning entities – "natural or legal person, public authority, agency or other body"[217] – that develop and place an AI system or service on the market, and deployers, meaning entities[218] – same as above – "that use an AI system under their authority, except where the AI system is used in the course of a personal, non-professional activity."[219] Such entities, both public and private actors – might be placed in the EU or outside. For the Regulation to be applied is necessary that the AI system is placed in the EU market or that the used system is impacting parties in the EU.[220] Therefore, the

[215] AI Act, Art. 8-15.
[216] AI Act, Art. 2.
[217] AI Act, Art. 3, no. 3.
[218] Id.
[219] AI Act, Art. 3, no. 4.
[220] AI Act, Art. 2, para. 1.

provision ensures broad applicability by covering providers, deployers, and intermediaries across the AI value chain, including those outside the EU whose systems impact individuals within the Union. As clarified by Recital 22,

> "to prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union."

In terms of exemptions, it has been highly discussed the risks of excluding the applicability of the Regulation to military purposes.[221] Hence, systems used exclusively for military, defence, or national security purposes are excluded from the AI Act. Although this choice may surprise to a certain extent given the limited competence – or lack of – the European Union on this subject, nonetheless, operationalising these exemptions could prove challenging, particularly when distinguishing between national security and law enforcement activities, resulting in potential loopholes of absence of protection.

Specifically, Recital 24 recognises that, if an AI system developed, placed on the market, put into service, or used for military, defence, or national security purposes is subsequently used, even temporarily or permanently, for civilian or humanitarian purposes, law enforcement, or public security purposes, it falls within the scope of the Regulation. In such cases, the entity using the AI system is required to ensure its compliance with the AI Act unless it is already compliant. This approach aims to mitigate the risk of regulatory loopholes, as mentioned above as potential negative outcomes, and try to maintain the EU oversight in mixed-use scenarios. The integration of existing legal frameworks further reflects the Act's pragmatism, ensuring that its obligations do not overlap or conflict with established laws such as the GDPR or the Law Enforcement Directive (LED).[222] At the same time, the provision leaves room for Member States to

[221] Ibid, Art. 2(3).

[222] 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

introduce stricter worker protections under Article 2(11), addressing concerns about AI-driven surveillance and decision-making in employment contexts.

Additionally, the exemption of the AI Act also applies to research and development in order to support innovation while maintaining regulatory oversight during real-world testing, albeit with potential compliance costs that could deter experimentation.[223] Another relevant case is related to public authorities in a third country and international organisations where those authorities or organisations use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such a third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Likewise, the AI Act does not apply to deployers who are natural persons using AI systems in the course of a purely personal non-professional activity, thus limiting the scope of the AI Act to deployers using AI systems for non-commercial purposes.

2.4.3 Method: the risk-based approach

The AI Act is the quintessence of risk regulation.[224] It categorizes AI systems into different tiers based on the level of risk they pose, ranging from minimal to prohibited,[225] as well as other digital policies before it.[226] This approach is intended to safeguard

penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[223] AI Act, Art. 2(6) and Recital 25.

[224] Tobias Mahler, 'Between risk management and proportionality: The risk-based approach in the EU's Artificial Intelligence Act Proposal' (2022) *The Swedish Law and Informatics Research Institute* 247; Giacomo Zanotti, Daniele Chiffi and Viola Schiaffonati, 'AI-Related Risk: An Epistemological Approach' (2024) 37 *Philosophy & Technology* 1. For an overview of what means risk regulation today, see Alberto Alemanno, 'The Past, Present and Future of Risk Regulation' (2017) 8 *European Journal of Risk Regulation* 1

[225] In particular, Annexes I and III further specifies Art. 6 of the AI Act and lists the AI systems which are considered "by default" by the EU legislator "high-risk". Claudio Novelli and others, 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act' (2024) 3 *Digital Society* 1; Margot E Kaminski, 'Regulating the Risks of AI' (2023) 103 *BU L Rev* 1347.

[226] See Pietro Dunn and Giovanni De Gregorio, 'The European risk-based approaches: Connecting constitutional dots in the digital age' (2022) 59 *Common Market Law Review* 473; Tytti Rintamäki and others, 'High-Risk Categorisations in GDPR vs AI Act: Overlaps and Implications' (2023) 11 *IEEE Access* 1; Marco Almada and Nicolas Petit, 'The EU AI Act: a medley of product safety and fundamental rights?', EUI, RSC, Working PaperAvailable at: https://cadmus.eui.eu/handle/1814/75982.

fundamental rights, promote transparency, and build trust in AI systems while maintaining a competitive and harmonized single market within the EU.[227]

In this sense, the AI systems are categorized into four tiers. At the top of the hierarchy are AI systems deemed to impact severely on individual rights and are outright banned. These include, for instance, biometric recognition systems used in real-time in public spaces for identification by law enforcement authorities,[228] social scoring systems, or those that use subliminal techniques to manipulate individuals or groups in ways that may cause them harm.[229]

High-risk systems occupy the second level.[230] This category covers systems that, while not prohibited, pose a significant risk to safety, fundamental rights, and societal interests. The AI Act specifically outlines high-risk sectors in Annexes I and III, including biometric identification, critical infrastructure, education and vocational training, employment and worker management, access to essential private and public services, law enforcement, migration, asylum, border control, and judicial administration. This is the most comprehensive category in the AI Act, with the majority of the regulation dedicated to ensuring that these systems are transparent, fair and accurate.[231]

Limited-risk AI systems, which are considered in this comment, occupy the third level.[232] These systems are designed for human interaction, the creation or manipulation of content, including deepfakes,[233] image or audio generation systems. They are subject to specific transparency obligations, ensuring that users are aware when interacting with AI systems.[234] While obliged to comply only with the requirements as set out by Art. 50 AI Act, such systems still pose specific challenges, particularly regarding transparency.

At the base of the hierarchy are AI systems with minimal risk, largely exempt from stringent requirements. Providers of these systems are encouraged to adhere to voluntary codes of conduct and governance mechanisms, promoting self-regulation.[235]

---

[227] AI Act, Art. 3, para. 1, no. 2), "risk means the combination of the probability of an occurrence of harm and the severity of that harm".
[228] AI Act, Annex II details the crime for which such AI systems can be put into place.
[229] AI Act, Art. 5.
[230] AI Act, Art. 6 and Annex III.
[231] AI Act, Artt. 8-27.
[232] AI Act, Art. 50.
[233] AI Act, Art. 50, para. 4.
[234] AI Act, Rec. 132.
[235] AI Act, Rec. 165.

General Purpose AI (GenAI)[236] is positioned outside this hierarchy but is considered risky, requiring specific and consistent regulation (Chapter V) mainly to prevent catastrophic uses of this technology.

The AI Act risk-based approach has been defined to be "ambiguous",[237] due to its very centralized and rigid risk assessment model, which contrasts with more flexible frameworks like the one in the Reg. (UE) 2016/679. This approach may fail to adapt to the fast-paced development of AI technologies and the varied contexts in which they are used, creating uncertainty in ensuring that risks to fundamental rights are properly mitigated. Moreover, typically, the risk-based approach is illustrated as a pyramid, with minimal risk at the base and progressively greater risks as you move upward. However, the AI Act can be more aptly compared to an elevator than a pyramid for three key reasons.

First, in a pyramid, risks are typically seen as a continuum, with smooth gradations between minimal, limited, and high-risk levels. However, the AI Act introduces rigid categories, as mentioned. These categories are fixed, and AI systems are "placed" into one of them by the legislator. The approach lacks flexibility for AI systems to "move" dynamically between categories based on their real-world usage and emerging risks.[238] Hence, rather than being a gradual, continuous assessment like a pyramid, the AI Act's model operates like an elevator: AI systems are placed into specific "floors" or levels, with no easy movement between them based on evolving risks. In addition, this rigid classification is particularly problematic in instances where an AI system is deployed in a specific domain (e.g., healthcare) but does not meet the criteria for high-risk designation, despite presenting various risks (e.g., to patients and care recipients, given its direct and indirect effects on physical and mental health).[239]

---

[236] Natali Helberger and Nicholas Diakopoulos, 'ChatGPT and the AI Act' (2023) 12 Internet Policy Review <https://policyreview.info/essay/chatgpt-and-ai-act> accessed 3 December 2024; Levantino (n 12); Ballell (n 32).

[237] Pietro Dunn and Giovanni De Gregorio, 'The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies' (CEUR Workshop Proceedings 2022) <https://cris.unibo.it/handle/11585/894759> accessed 3 December 2024.

[238] AI Act, Artt. 7 and 97. As a matter of facts, while the EU Commission is empowered under Article 7 of the AI Act to amend the classification of high-risk AI systems, this power alone may not be sufficient to address the rapidly evolving nature of AI technologies. Technologies like deepfakes, which have the potential to cause profound psychological, financial, and societal harm, often do not fit neatly into predefined classifications when they are first introduced in the information loop.

[239] Martin Ebers, 'Truly Risk-Based Regulation of Artificial Intelligence-How to Implement the EU's AI Act', SSRN 4870387, SSRN. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387.

Second, it is up to the providers themselves to document and determine whether a system does not qualify as high-risk under a self-pre-assessment of the system.[240] By the way, this specific aspect contains potential loopholes regarding the consistency and robustness of compliance, as it places a considerable burden on providers to police themselves, potentially conflicts of interest. In particular, even though the provider might have created a system for some scopes, it would be the deployer to actually utilise it: therefore, would be their role a bit of fortune tellers?[241]

The clearest example of this 'elevator mechanism' can be observed in the provision considering GenAI systems, which are defined in Article 3, no. 66, as AI systems based on general-purpose models that can serve various functions, either directly or integrated into other systems, and present unique regulatory challenges due to their broad applicability. These models are categorized based on a tiered risk approach, with systems classified as posing systemic risks being subject to more stringent obligations under the AI Act. However, the threshold is not in the context where the model is depoloyed, but on a mathematical assumption of "high impact capabilities pursuant to paragraph 1, point (a), when the cumulative amount of computation used for its training measured in floating point operations is greater than 10(^25)".[242]

Systems with such systemic risks are always subject to the AI Act's obligations due to the potentially severe adverse effects they can cause.[243] Hence, saying it differently in this "elevator" structure, systemic risks automatically trigger regulatory obligations, that sum up with the 'high risk' obligations if the model with systemic risk is indeed put into function for a purpose identified as 'high risk' by the Regulation.

Finally, different from the GDPR and the Digital Services Act (DSA),[244] which strongly focus on protecting a couple of fundamental rights mainly[245] – privacy and data protection, the former, freedom of expression, the latter –, the AI Act has a completely

[240] AI Act, Art. 6 para. 3.
[241] Sandra Wachter, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) 26 Yale Journal of Law and Technology.
[242] AI Act, Art. 51, para. 2.
[243] AI Act, Rec. 112.
[244] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.
[245] Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 48).

different scope of application. As evident even from the choice of the legal basis,[246] the Regulation on AI is a product safety norm that intersects with a wider range of issues, as the case of deepfakes will illustrate.

These concerns converge on a fundamental issue: the Act's binary categorisation of "risky" versus "non-risky" AI uses oversimplify the complexities of AI technologies. This reductive approach overlooks AI systems nuanced and evolving nature, particularly regarding their autonomy and potential for long-term impacts on fundamental rights, human dignity, and the rule of law.

2.4.4 Prohibited risk AI Systems

One of the defining features of the AI Act is its list of prohibited AI practices, which outlines AI systems that pose an unacceptable risk to safety and fundamental rights. These systems are entirely banned from use, production, and commercialization within the European Union due to their potential to undermine human dignity, democratic values, and societal well-being.[247] Article 5 of the AI Act specifically addresses these unacceptable risks, defining several AI applications as incompatible with EU values.[248]

Prohibited systems include those that deploy subliminal techniques to manipulate individuals beyond their conscious awareness,[249] and those that exploit vulnerabilities based on personal characteristics like age or disability.[250] These provisions reflect the EU's commitment to preventing the misuse of AI for manipulative or deceptive purposes, ensuring that individuals are not unknowingly influenced by AI systems.

Particularly significant is the prohibition of biometric categorization systems that use biometric data to infer sensitive attributes such as race, religion, or political beliefs.[251] These systems are seen as infringing on fundamental rights to privacy and non-

[246] The AI Act is primarily grounded in Article 114 of the Treaty on the Functioning of the European Union (TFEU), which focuses on establishing and ensuring the functioning of the internal market. Since some of the AI considered in the regulation affects personal data (e.g., biometric identification), the legal basis has also been extended to Article 16 of the TFEU.

[247] AI Act, Rec. 3 and 33.

[248] AI Act, Rec. 28.

[249] AI Act, Art. 5, para. 1, lett. a). On the interpretation of Art. 5, see the European Commission, 'ANNEX to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)', published 4 February 2025, C(2025) 884 final.

[250] AI Act, Art. 5, para. 1, lett. b).

[251] AI Act, Art. 5, para. 1, lett. g).

discrimination, posing severe ethical concerns. However, exceptions exist for law enforcement, since biometric categorization and real-time remote biometric identification, with some differences from one another, can be deployed for specific uses, as the next chapter will further explain.

Another critical ban applies to social scoring systems that evaluate individuals or groups based on their social behaviour over time,[252] reminiscent of the controversial systems seen in other jurisdictions like China.[253] Such practices are seen as fundamentally incompatible with European values of individual liberty and autonomy.[254]

Despite these prohibitions, there remain concerns that certain prohibited practices, like predictive policing tools, were not included on the prohibited list. These technologies, which have demonstrated significant potential for bias and harm, continue to be permissible under the AI Act's framework, albeit with stricter regulations. This creates an ongoing tension between the desire to promote innovation and the imperative to safeguard fundamental rights, raising questions about whether the AI Act sufficiently addresses the most egregious risks. The prohibitions serve as a safeguard against the most dangerous applications of AI, but the framework leaves room for further debate about what and how to correctly find a balance.

2.4.5 High risk AI systems

The AI Act devotes special attention to high-risk AI systems, recognizing that certain technologies, while not prohibited, pose significant risks to fundamental rights, safety, and societal well-being. As specified by Rec. 46,

> "High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law".

[252] AI Act, Art. 5, para. 1, lett. c).
[253] Lagioia, Rovatti and Sartor (n 194).
[254] Wachter (n 244).

Hence, these systems are subject to stringent regulations to mitigate potential harm while allowing for their controlled deployment. Annex III of the AI Act provides a detailed list of high-risk applications, and these systems are regulated with specific pre-market and post-market obligations, reflecting the EU's risk-based approach to AI governance.

High-risk AI systems are those that operate in sectors where their misuse or malfunction could have serious consequences for individuals or society. Article 6 introduces two broad categories: AI Systems as safety components or products under union harmonisation legislation, as per Article 6(1), and 'standalone' high-risk systems that are specifically listed in Annex III of the AI Act. In the first category falls high-risk systems that are safety components of products. These systems are already subject to third-party conformity assessments**,** reflecting their inherent risks to health and safety in regulated sectors such as medical devices, machinery, or vehicles. Whereas, in the second category, as per Article 6(2), it is recalled Annex III that provides a detailed list of high-risk applications, and these systems are regulated with specific pre-market and post-market obligations, reflecting the EU's risk-based approach to AI governance. These use cases span critical domains such as biometric systems, education, employment, law enforcement, and migration control. The list aims to ensure clarity but has been criticised for its susceptibility to over- and under-inclusiveness.[255]

The list set forth in Annex III includes systems used in areas such as biometric identification, critical infrastructure, employment, law enforcement, education, and migration. To ensure that high-risk AI systems do not violate fundamental rights, the AI Act imposes a series of pre-market obligations on providers of these systems. These include conducting risk assessments, ensuring the quality and governance of the data used to train AI models, and implementing robust transparency measures. Additionally, providers must maintain detailed technical documentation and ensure that their systems are capable of human oversight, with real-time intervention mechanisms in place if the AI system behaves unexpectedly.[256] The following grid contains an explanation of the sectors included in Annex III and, therefore, considered high-risk systems by the AI Act.

[255] ibid; Smuha and Yeung (n 151).
[256] AI Act, Chapter III.

Table 2 – high risk systems as regulated in the provisions of Annex III, AI Act.

Category	Use cases
Biometric systems	- Remote biometric identification systems (excluding biometric verification for authentication); - Biometric categorization based on sensitive characteristics; - Emotion recognition systems (except for workplace and education).
Critical infrastructure	- AI systems used as safety components in managing critical infrastructure, such as transport, energy, water, or gas networks.
Education and vocational training	- AI systems for determining admission, assigning, or evaluating students; - Systems monitoring behaviour during tests.
Workers and employment	- AI systems using in the human resources sector (e.g., filters for CVs); - Systems evaluating performance, allocating tasks, and monitoring workers.
Access to essential service	- AI system for evaluating creditworthiness; - Risk assessment for life and health insurance; - Ai systems used in emergency and healthcare triage.
Law enforcement	- Predictive policing systems; - Tools for evaluating the criminal risk assessment; - Polygraphs for personality assessment.
Migration and border control	- Systems for assessing risks (e.g., security, irregular migration) at borders; - AI used for processing asylum and visa applications.
Administration of justice	- AI system used for assisting judicial authorities;

	- Tools for evaluating or influencing a person's behaviour in the exercise of his or her vote in elections or referenda.

Art. 6(3) provides an important exemption for the systems listed above. Namely, if the provider deems them to pose no significant risk "of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making", they should document the assessment before the system is put into place or into the market.[257] More plainly, if the provider, hence the producer of AI systems, evaluates that the latter does not pose any significant risk due to the following criteria, the system is not considered high risk: i) the AI performs a narrow procedural task; ii) the system is used to improve results of a previously completed human activity; iii) the system detects patterns and deviations without replacing or influencing prior human assessments; iv) the AI conducts preparatory tasks for assessments relevant to Annex III use cases. Providers who claim this exemption must document the assessment before putting into market the system and register the system as such under Article 49(2) that disciplines the registration process of any high-risk AI before it enters the market.[258] Additionally, they should provide relevant documentation to the Market Surveillance Authority (national one) upon request.

This whole exemption has already been strongly criticised for the heavy power that leaves on the providers which are left upon their self-assessment, with an oversight that is exercised '*una tantum*' by the national authorities.[259] While this offers flexibility, critics argue that it delegates too much discretion to providers, raising concerns about enforcement and oversight.[260] Furthermore, while the AI Act emphasises the importance

[257] AI Act, Art. 6(4).

[258] Ibid, Rec. 131 states "providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, as well as providers who consider that an AI system listed in the high-risk use cases in an annex to this Regulation is not high-risk on the basis of a derogation, should be required to register themselves and information about their AI system in an EU database, to be established and managed by the Commission".

[259] The AI Act is quite opaque in this respect, as well as on which authority, if any, is going to exercise oversight on the compiling of the register mentioned in Art. 49. As it will be mentioned during the course of this Chapter, many provisions of the AI Act, even though sensible, lack concrete enforcement as they are laid down, with the prospective of future – maybe – clarifications by the European Commission on their interpretation.

[260] Wachter (n 244).

of transparency and accountability,[261] there are concerns that its reliance on self-assessment by AI providers may not be sufficient to prevent abuses or ensure consistent compliance across the EU.[262]

Furthermore, according to Article 7, the European Commission has the power to amend Annex III via delegated acts. Namely, upon this procedure, the Commission can add new high-risk cases if they pose risks to health, safety, or fundamental rights comparable to existing high-risk systems, or it can remove use cases where there is reliable evidence that the system no longer poses significant risks. To determine these changes, the Commission relies on a detailed set of criteria outlined in Article 7(2), including the nature of the data processed, the level of human oversight, power imbalances, and the potential harm's intensity, scale, and reversibility. However, despite these comprehensive safeguards, there are ongoing concerns that the scope of high-risk applications remains too narrow. Critics argue that important areas, such as recommender systems, predictive policing, and certain financial technologies, have not been adequately classified as high-risk, even though they present significant ethical and societal challenges.[263]

In conclusion, Articles 6 and 7 form the backbone of the AI Act's approach to high-risk systems, combining predefined risk categories with mechanisms for dynamic updates. While this risk-based strategy provides clarity and adaptability, its reliance on self-assessment and limited public oversight underscores the need for robust enforcement mechanisms to safeguard health, safety, and fundamental rights effectively.

Post-market obligations are also critical for high-risk AI systems. Providers and deployers are required to monitor the operation of AI systems continuously and report any incidents or malfunctions to regulatory authorities.[264] This ongoing monitoring is essential for identifying unforeseen risks and ensuring that AI systems remain compliant with the regulatory framework.

---

[261] Philipp Hacker, 'A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act' (2021) 13 Law, Innovation and Technology 257.

[262] Kim Lane Scheppele, Dimitry Vladimirovich Kochenov and Barbara Grabowska-Moroz, 'EU Values Are Law, after All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union' (2020) 39 Yearbook of European Law 3; Hannah Van Kolfschooten, 'EU Regulation of Artificial Intelligence: Challenges for Patients' Rights' (2022) 59 Common market law review 81.

[263] Wachter (n 244).

[264] AI Act, Art. 72.

Moreover, the Fundamental Rights Impact Assessment (FRIA) is a key requirement for high-risk AI systems.[265] This assessment is designed to evaluate how these systems could potentially affect fundamental rights, such as privacy, non-discrimination, and freedom of expression. By mandating FRIA, the AI Act aims to ensure that AI systems used in sensitive areas do not erode democratic values or compromise individual freedoms.[266] Furthermore, while the AI Act emphasises the importance of transparency and accountability,[267] there are concerns that its reliance on self-assessment by AI providers may not be sufficient to prevent abuses or ensure consistent compliance across the EU.[268]

2.4.6 Limited risks

Beyond the categories of prohibited and high-risk AI systems, the AI Act also delineates a category for limited-risk AI systems.[269] These applications, while not posing significant threats to fundamental rights or public safety, still necessitate regulatory oversight to ensure transparency and protect users from potential misunderstandings or misuse. Limited-risk AI systems typically include technologies such as chatbots, basic recommendation engines, and content-generation tools.

For these limited-risk AI systems, the AI Act imposes transparency obligations aimed at ensuring users are aware they are interacting with an AI-driven application. Specifically, providers must inform users that they are engaging with an AI system, thereby preventing deception and fostering trust in digital interactions. This requirement is crucial in maintaining user autonomy and ensuring that individuals can make informed decisions when interacting with AI technologies.

Unlike high-risk systems, limited-risk AI applications are not subject to extensive pre-market assessments or rigorous post-market monitoring. Moreover, such requirements also lack a dedicated enforcement authority, leaving compliance to the self-assessment of interested deployers and providers.[270] The primary regulatory focus is on user awareness

[265] AI Act, Art. 27.
[266] Wachter (n 244).
[267] Hacker (n 263).
[268] Scheppele, Kochenov and Grabowska-Moroz (n 264); Kolfschooten (n 264).
[269] AI Act, Art. 50.
[270] Wachter (n 244); Claudio Novelli and others, 'A Robust Governance for the Ai Act: Ai Office, Ai Board, Scientific Panel, and National Authorities' (2024) 4 European Journal of Risk Regulation 1.

rather than comprehensive risk mitigation. However, providers are encouraged to adopt best practices that enhance transparency and user understanding, such as clear labelling and user prompts that disclose the AI nature of the system.

The AI Act's approach to limited-risk systems underscores the importance of proportional regulation, where the level of oversight corresponds to the potential impact of the AI application. Furthermore, the transparency requirements for limited-risk AI systems contribute to the broader objective of fostering a human-centric AI ecosystem. By ensuring that users are informed about the AI-driven nature of their interactions, the AI Act promotes accountability and informed consent, aligning with the EU's commitment to protecting fundamental rights and democratic values in the digital age.

However, the broad flexibility given to providers, coupled with the lack of strong enforcement mechanisms, could result in inconsistent compliance and insufficient safeguards for users. As AI technologies continue to evolve and become more sophisticated, these critical aspects must be addressed to ensure that limited-risk systems do not become a blind spot in the EU's regulatory framework for AI.

2.4.7 Requirements for high-risk Systems

The AI Act establishes a comprehensive set of obligations for high-risk AI systems to ensure their safety, transparency, and alignment with fundamental rights. These requirements, found in Articles 8 to 15, address the entire lifecycle of high-risk AI systems, from design and development to deployment and post-market monitoring. Each obligation reflects the EU's commitment to mitigating risks associated with AI technologies while maintaining their effectiveness and trustworthiness.

A continuous risk management system is central to high-risk AI systems, functioning as an ongoing process across the system's lifecycle. For this reason, Article 8 sets the scene for the following provisions, specifically establishing that providers, when an AI is part of a product, should be responsible for "ensuring that their product is fully compliant with all applicable requirements under applicable Union harmonisation legislation".[271]

[271] AI Act, Art. 8(2). See also Rec. 46 that recalls generally the legal framework applicable to such products.

Particularly, providers are required to identify and analyse risks and make evaluations in order to adopt any measure that can reduce or eliminate hazards.[272]

Article 9 establishes a risk management system as a core requirement for all high-risk AI systems,[273] emphasising the identification and mitigation of risks to health, safety, and fundamental rights.[274] Article 9 applies universally to all high-risk AI systems, covering risks across health, safety, and fundamental rights during the design and development phases.[275] Different from other requirements for deployers, risk management under Article 9 is the requirement of providers that incorporate risk identification and mitigation measures into the system's design, adhering to essential requirements.[276] Particularly, providers are required to:

- Identify and analyse risks that the AI system may pose to health, safety, or fundamental rights, whether through intended use or reasonably foreseeable misuse;
- Estimate and evaluate risks, including emerging risks detected via post-market monitoring feedback;

[272] Ibid, Rec. 64 states "the hazards of AI systems covered by the requirements of this Regulation concern different aspects than the existing Union harmonisation legislation and therefore the requirements of this Regulation would complement the existing body of the Union harmonisation legislation. For example, machinery or medical devices products incorporating an AI system might present risks not addressed by the essential health and safety requirements set out in the relevant Union harmonised legislation, as that sectoral law does not deal with risks specific to AI systems".

[273] The definition of a risk management system is a process that "specifies how providers of high-risk AI systems must identify, assess and respond to risks", Jonas Schuett, 'Risk Management in the Artificial Intelligence Act' (2024) 15 European Journal of Risk Regulation 367.

[274] AI Act, Art. 9(2): "The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps: (a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose; (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse; (c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72; (d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a)".

[275] Ibid, Rec. 65.

[276] Ibid, Art. 9(5) specifies that identifying the essential requirements for performing the risk management system are "(a) elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system; (b) where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated; (c) provision of information required pursuant to Article 13 and, where appropriate, training to deployers. With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used".

- Adopt risk mitigation measures, ensuring technical design reduces or eliminates hazards wherever feasible;
- Ensure residual risks – those that cannot be eliminated – are reduced to an acceptable level;
- Account for the system's potential adverse impact on vulnerable groups, such as minors, and consider deployers' technical knowledge and training.

Testing plays a crucial role in the risk management process, requiring providers to assess system performance against predefined metrics and thresholds. Testing may include real-world conditions and must occur throughout development and before market placement to ensure consistency and compliance. Providers under Article 9 may also adhere to harmonised standards to fulfil their risk management requirements. These standards, while voluntary, offer structured methodologies for compliance.[277]

High-risk AI systems that rely on training, validation, and testing datasets must meet quality and governance requirements.[278] The provider must have knowledge of how the system has been trained before putting it on the market and should certify that the dataset used in the whole AI-life cycle is representative, relevant, complete, and as free of errors and biases as possible, aligned with the system's intended purpose.[279]

More importantly, the provider should test and conduct evaluations of whether the system is able to detect bias and mitigate any discriminatory outcomes, particularly where outputs influence decision-making processes.[280] Such data governance practices should be complemented with documenting data collection, preparation, and processing, including annotation, cleaning, updating, and assumptions regarding data

[277] Ibid, Rec. 61. For the role of standards in the AI Act, see Mélanie Gornet and Winston Maxwell, 'The European Approach to Regulating AI through Technical Standards' (2024) 13 Internet Policy Review.

[278] Ibid, Rec. 67, "high-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become a source of discrimination prohibited by Union law. High-quality data sets for training, validation and testing require the implementation of appropriate data governance and management practices. Data sets for training, validation and testing, including the labels, should be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose of the system. In order to facilitate compliance with Union data protection law, such as Regulation (EU) 2016/679, data governance and management practices should include, in the case of personal data, transparency about the original purpose of the data collection".

[279] Ibid, Art. 10(3-5).

[280] Ibid, Art. 19(2)(f).

representativeness. Moreover, in evaluating the quality of the data, the provider should take into account the geographical, behavioural, or functional context, ensuring datasets reflect the specific environments in which the system will operate.[281] If special categories of personal data are processed to detect and correct bias, providers must implement exceptional safeguards, such as pseudonymisation, strict retention policies, and access controls, ensuring compliance with data protection laws like the GDPR.

This is a paramount provision since, as also recalled by Recital 69, the right to privacy and data protection "must be guaranteed throughout the entire lifecycle of the AI system". Therefore, the measures taken by the provider and evaluated through this check data management system must also take into consideration the compliance with principles such as "data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed".[282]

The applicability of such a principle is crucial for ensuring compliance with the GDPR.[283] However, some commentators highlighted potential conflicts with the very concepts of minimisation and privacy by design due to the inherent features of AI. As clarified by the Spanish Data Protection Authority (AEPD), "the effective application of the principles of accountability, minimisation and accuracy, data protection by design, and efficiency assessment are linked to the use of mature development methodologies." This means that the selection of a technology or another, the choice of the training methodologies, cannot be done without taking into account these principles. Therefore, while extensive data use may be justified to improve model quality, developers must ensure that only data with added value is processed, avoiding unnecessary categories, e.g. certain social media datasets, that may conflict with the proportionality test.

In accordance with the principle of accountability, providers must produce detailed technical documentation before placing a high-risk AI system on the market and should continue for the whole AI life cycle. This documentation serves as evidence of compliance and facilitates assessments by competent authorities and notified bodies.[284] It

[281] Ibid, Art. 10(4).

[282] See also Art. 5 GDPR. For a comment, Cécile de Terwangne, 'Article 5 Principles Relating to Processing of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[283] CNIL (French Data Protection Authority), AI system development: CNIL's recommendations to comply with the GDPR, 07 June 2024; Marvin Bartels, 'A Balancing Act: Data Protection Compliance of Artificial Intelligence' (2024) 73 GRUR International 526.

[284] See, also, AI Act, Rec. 71.

must include, at a minimum, the elements outlined in Annex IV, covering system design, development, intended purpose, performance metrics, and risk mitigation strategies. SMEs and start-ups benefit from a simplified format, reducing administrative burdens.[285]

Connected to the previous requirements, providers are asked to document also high-risk AI systems' automatic logging capabilities throughout their lifecycle.[286] The recording of logs is meant to ensure traceability to:

- Identifying potential risks, hazards, or substantial system modifications;
- Supporting post-market monitoring and enabling deployers to analyse system behaviour;
- Monitoring biometric systems, where logs must include input data, results, and details of operator verification.

All the previous requirements are connected with the more general burden of transparency. As a matter of fact, providers must ensure that high-risk AI systems are transparent and interpretable for deployers. Systems must be accompanied by clear and accessible instructions, including:

- System characteristics, limitations, and expected performance, e.g. accuracy, robustness, and cybersecurity metrics;
- Human oversight requirements and guidance for interpreting outputs appropriately;
- Technical capabilities for input and output management, including information on training data and operational boundaries.

These measures ensure deployers understand the system's functionality, risks, and proper use, fostering accountability and responsible deployment. For this reason, Recital 72 specifies that the information should not only be transparent but delivered to the deployer in a clear and accessible manner. Furthermore, to enhance legibility, the provider should include "instructions of use, where appropriate, illustrative examples, for instance on the limitations and on the intended and precluded uses of the AI system".

[285] This Article provides specifically that the EU Commission should provide a simplified format for SMEs.
[286] AI Act, Rec. 71 specifies that "high risk AI systems should technically allow for the automatic recording of events, by means of logs, over the duration of the lifetime of the system".

The system cannot be left to produce results autonomously; instead, it must be subject to real human oversight. This is only achievable if the documentation-keeping requirement is fulfilled, the system is trained using data that are managed and governed in compliance with the principle of accountability, and transparency regarding the system's features, metrics, and technical capabilities is ensured by the provider. These elements underpin the obligations set out in Article 14, which establishes that high-risk AI systems must be designed to allow effective human oversight during operation, minimising risks to safety and rights. Providers must implement measures that enable humans to perform essentially three activities: monitoring the system behaviour, in order to detect anomalies, avoiding bias by not over-relying on the AI outputs, and overriding the operation when necessary.[287] For this purpose, the AI Act sets an obligation to develop appropriate interfaces that do not impair the oversight and training of the deployer should be met.[288] This latter aspect may fall in the broader issue of the 'AI literacy' obligation examined above. For certain remote biometric identification systems, results must undergo manual verification by at least two competent individuals unless exemptions apply.[289] However, such a rule is not applied in the case of law enforcement and migration, as specified by Article 14.

Furthermore, providers must ensure high-risk AI systems achieve consistent levels of accuracy, robustness, and cybersecurity throughout their lifecycle. Specific requirements include:

- Declaring system accuracy metrics and ensuring resilience to errors, faults, or unpredictable conditions;[290]

[287] Ibid, Art. 14(4): "the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate: (a) to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance; (b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available; (d) to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system; (e) to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state".

[288] Ibid, Art. 14(1).

[289] Ibid, Rec. 73 clarifies that "this requirement should not pose unnecessary burden or delays and it could be sufficient that the separate verifications by the different persons are automatically recorded in the logs generated by the system".

[290] Ibid, Art. 15(2).

- Implementing measures to prevent feedback loops that may reinforce biased outputs over time;[291]
- Protecting systems against cybersecurity threats, such as data poisoning, adversarial attacks, or exploitation of vulnerabilities. Technical solutions must detect, mitigate, and respond to these risks effectively.[292]

Before moving on to the analysis of the obligation set for by complied by the providers and the deployers of high-risk systems, these roundup requirements Act reflects a comprehensive and risk-focused regulatory approach. By mandating robust risk management systems, high-quality data governance, technical transparency, and human oversight, the Act aims to ensure that high-risk AI systems are trustworthy and safe and that providers are accountable for their use.

2.4.8 Obligations for high-risk Systems

The AI Act outlines precise obligations for providers (entities developing or placing AI systems on the market) and deployers (entities using AI systems) of high-risk AI systems, importers and distributors. These obligations cover every stage of the system's lifecycle. As mentioned in many of these obligations and requirements, the responsibility does not end at the moment when the system is placed into the market. To this end, importers, distributors, or deployers who substantially modify an AI system assume the obligations of a provider under Article 16. These obligations also apply when they:

- Place their name or trademark on a system already on the market;
- Modify the intended purpose of a system such that it becomes classified as high-risk;
- Make technical changes that affect the system's risk classification.

In these cases, the original provider is no longer responsible for the modified system but must cooperate with the new provider to ensure compliance.[293]

[291] Ibid, Art. 15(4).
[292] Ibid, Art. 15(5). Specifically, see also Recs. 75-78.
[293] Ibid, Rec. 86 specifies that "the former provider should nonetheless closely cooperate and make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems".

2.4.9 Obligations for Providers of High-Risk AI Systems

The quality management system (QMS) is a foundational requirement for providers of high-risk AI systems to ensure compliance with the AI Act and maintain system integrity throughout its lifecycle, also with respect to the sectorial rules on quality management.[294] Article 17(1) details which aspects should be included by the provider in the conformity assessment. Particularly, this should take into account a clear strategy for regulatory compliance, with processes to manage conformity assessments and system modifications. Secondly, they must establish systematic design and verification procedures, ensuring rigorous oversight of the system's development, quality control, and validation. Moreover, testing procedures must be carried out both before and during development, incorporating robust methods for examining system performance.

Effective data management is a core component of the QMS, addressing governance measures such as data collection, labelling, bias detection, and retention to ensure compliance with transparency and accuracy standards. The QMS must also integrate a risk management system as outlined in Article 9, enabling providers to identify, mitigate, and monitor risks effectively. Beyond development, providers are required to implement post-market monitoring systems based on Article 72 to track performance and safety after deployment, as well as procedures for incident reporting according to Article 73 to ensure timely identification and resolution of serious incidents. Finally, the last paragraph recalls that while performing a QMS, providers must establish an accountability framework, clearly defining the roles and responsibilities of management and staff to maintain compliance. For financial institutions and sector-specific organisations, certain QMS obligations can be integrated with existing internal governance processes, streamlining requirements without compromising the rigour expected under the AI Act.

Moreover, providers are required to retain technical documentation based on Article 11 and quality management records for 10 years following the system's placement on the market. These records must demonstrate compliance with the AI Act and be readily available for review by competent authorities. Providers must also ensure the retention of automatically generated logs throughout the system's lifecycle to enable traceability and

[294] Ibid, Rec. 81.

monitoring. The logs must capture critical operational events, anomalies, and system inputs and outputs to facilitate risk identification and post-market oversight. For financial services, specific logging requirements apply, and they should "maintain the logs automatically generated by their high-risk AI systems as part of the documentation kept under the relevant financial services law".[295]

Providers must also take immediate corrective actions. If a high-risk AI system is found to present risks or fail to comply with the AI Act, they have to put in place actions to bring the system into conformity, withdrawing it from the market, recalling it, or disabling it entirely, depending on the severity of the issue. Providers are also required to cooperate fully with competent authorities, providing access to requested logs, technical documentation, and other evidence necessary to demonstrate compliance. This cooperation must be carried out transparently while respecting confidentiality obligations as outlined in Article 78, ensuring the protection of sensitive business information and trade secrets.

In case providers are located outside the EU, they must appoint an authorised representative within the Union before placing high-risk AI systems on the market. The representative acts as a liaison between the provider and competent authorities. In particular, authorised representatives can be addressed directly by competent authorities to ensure compliance. If a representative identifies that a provider is acting contrary to its obligations, they must terminate their mandate and notify the relevant authorities immediately.

2.4.10 Obligations for Deployers of High-Risk AI Systems

Deployers are responsible for ensuring that high-risk AI systems are used in accordance with the provider's instructions and for maintaining compliance with the AI Act.[296] The risks that an AI system may pose override the training phase, and involve the deployer, which is the main utiliser of the system. Hence, as clarified by Recital 93,

> "whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers

[295] Ibid, Art. 19(2).
[296] Ibid, Rec. 91.

of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system".

Thus, Article 26 guides the deployer in the compliance process. In particular, the deployers must take appropriate technical and organisational measures to guarantee proper system use, which includes assigning trained and competent personnel to oversee system operation. Human oversight remains a critical requirement to ensure accountability, as deployers must ensure that supervisors can effectively monitor the system and intervene when necessary.[297]

When deployers control the system's input data, they are obligated to ensure the data is relevant and representative of the AI system's intended purpose, as established for the providers. Additionally, they must monitor system performance to detect risks, incidents, or malfunctions, reporting these issues promptly to providers and competent authorities.[298] To enable traceability and accountability, deployers must retain automatically generated logs for at least six months unless a longer period is specified by national or Union law.

Special obligations apply to workplace deployments. Deployers are required to inform workers and their representatives when AI systems are in use. This obligation ensures transparency and safeguards workers' rights in accordance with labour laws.[299]Moreover, law enforcement deployers using post-remote biometric identification systems, which include obtaining judicial or administrative authorization before system use and maintaining detailed records of each deployment for audit and accountability purposes.[300]

2.4.10.1 Fundamental Rights Impact Assessment (FRIA)

[297] In particular, the deployer should monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Art. 72.
[298] AI Act, Art. 26(5-7).
[299] Ibid, Rec. 92.
[300] The regulation further allows Member States to adopt more restrictive laws governing the use of these systems, provided such measures comply with Union law. These provisions, aligned with Directive (EU) 2016/680 and Article 9 of the GDPR, emphasize the importance of safeguarding fundamental rights, including privacy and data protection, while balancing the needs of law enforcement. By establishing clear procedural safeguards, limits on usage, and accountability mechanisms, the AI Act aims to prevent misuse and ensure that biometric systems are deployed transparently and proportionately.

Among the obligations for high-risk systems, special attention should be devoted to the Fundamental Rights Impact Assessment, mandated by Article 27 of the AI Act, which serves as a crucial regulatory mechanism to safeguard fundamental rights in deploying high-risk AI systems.[301] The FRIA is a great idea built on other risk assessment mechanisms, such as the Human Rights Democracy and Rule of Law Impact Assessment (HUDERIA), elaborated in the context of the Council of Europe.[302]This assessment is a rights-based one, meaning that the deployer is asked to consider the risks that an AI system may pose by pondering every right in the Charter of Fundamental Rights of the European Union (CFREU), especially those "in the areas of education, healthcare, social services, housing, administration of justice".[303] Chapter 4 will delve deeper into the FRIA, offering a comprehensive analysis of its scope and application while proposing a structured model for understanding the rights at stake. This exploration will address not only the strengths of the FRIA as a regulatory tool but also its limitations, including challenges related to implementation and enforcement. Ultimately, the chapter will contribute to a more nuanced understanding of how fundamental rights can be effectively safeguarded in the era of AI-driven innovation.

It is worth to anticipate that only a few entities are, however, asked to comply with the FRIA. As specified by Art. 27 para. 1, fall into this category only public bodies utilizing high-risk systems,[304] and private entities providing public services, referred to in points 5 (b) and (c) of Annex III,[305] such as deployers used to evaluate people's creditworthiness and risk assessment in the case of life and health insurance. In a nutshell, banks and insurance.

---

[301] It was inserted with the European Parliament's position, and represents an advancement in making of the AI Act a Regulation less product oriented, and more prone to the protection of fundamental rights, as also noted by Francesca Palmiotto, 'The AI Act Roller Coaster: How Fundamental Rights Protection Evolved in the EU Legislative Process' (4 June 2024) <https://papers.ssrn.com/abstract=4904179> accessed 4 September 2024.

[302] This methodology was proposed in CAHAI 1425th meeting, 16.02.2022, CM(2021)173 and approved in the context of the Framework Convention by the Committee on Artificial Intelligence (CAI), 'Methodology for the Risk and Impact Assessment of Artificial Intelligence Systems from the Point of View of Human Rights, Democracy and the Rule of Law (HUDERIA Methodology)', Strasbourg, 28 November 2024, CAI(2024)16rev2.

[303] AI Act, Art. 27, to be read together with Art. 1, Rec. 93 and 96. The quote comes from Rec. 96.

[304] Excluded entities that fall into Annex III, para. 2, about deployers of critical infrastructures.

[305] AI Act, Annex III, points 5 (b) and (c): "(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud; (c) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance".

Even though the AI Act mandates the AI Office to come up with a template, it is already possible to extract some of the key features of the FRIA. Art. 27 demands that deployers provide a detailed description of the processes in which the AI system will be used, ensuring the technology's intended purpose aligns with legal and ethical standards.[306] This evaluation is not merely technical but also extends to how frequently and for how long the system will be operational. The inclusion of frequency and duration assessments is particularly important as it addresses concerns about the overuse or misuse of AI.[307] Furthermore, the FRIA mandates that deployers identify the categories of individuals or groups likely to be affected by the AI system.[308] This provision is essential in ensuring that vulnerable populations, such as minorities or marginalized groups, are not disproportionately impacted. The analysis of these affected groups must be complemented by an assessment of specific risks to their rights, which could include issues of bias, discrimination, or undue infringement on privacy.[309] Human oversight is another critical element of the FRIA, as the Act emphasizes that despite the increasing autonomy of AI systems, human involvement remains a cornerstone in ensuring accountability.[310] The assessment requires deployers to specify how human supervisors will monitor and intervene, if necessary, thus preventing the system from operating without meaningful checks. Finally, the FRIA requires deployers to outline mitigation strategies for any identified risks, as well as the internal governance structures and complaint mechanisms in place.[311]

Essentially, the FRIA will have three phases: identification of risks, analysis of and reactions to the risks, and mitigation. The complexity does not rely on the structure but especially on methodology[312] and its practical implementation: there is the risk that it will be mixed up with other assessments, such as the Data Protection Impact Assessment (DPIA) mandated under Art. 35 GDPR.[313]

---

[306] AI Act, Art. 27 para. 1, lett. a).
[307] AI Act, Art. 27 para. 1, lett. b).
[308] AI Act, Art. 27 para. 1, lett. c).
[309] AI Act, Art. 27 para. 1, lett. d).
[310] AI Act, Art. 27 para. 1, lett. e).
[311] AI Act, Art. 27 para. 1, lett. f.
[312] Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 48).
[313] Federica Paolucci, 'Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights' [2024] Verfassungsblog <https://verfassungsblog.de/shortcomings-of-the-ai-act/> accessed 3 December 2024.

Finally, an overarching doctrinal issue arises from the fact that human and fundamental rights have traditionally been designed to limit the powers of state actors, rather than to bind the private sector.[314] This distinction raises important questions about the utility and effectiveness of FRIA, particularly when applied to private actors deploying high-risk AI systems. While the AI Act mandates private entities to assess the impact of their AI systems on fundamental rights, this requirement may seem at odds with the traditional legal doctrine that human rights obligations do not apply directly to private companies.

This doctrinal gap challenges the extent to which FRIAs can meaningfully mitigate the risks associated with high-risk AI systems deployed in the private sector. Given that fundamental rights frameworks were originally created to curb state overreach, their direct application to private companies raises questions about legal enforceability and the scope of accountability for private actors. For instance, a private company developing or deploying AI systems in areas like healthcare or employment may influence fundamental rights (such as privacy or non-discrimination), yet the legal mechanisms to hold both companies and public actors accountable under human rights law remain limited.

2.4.11 Harmonised standards

Harmonised standards are a cornerstone of the AI Act, ensuring that high-risk AI systems and general-purpose AI models comply with regulatory requirements in Section 2 and other obligations, such as those in Chapter V. According to Article 40, when published in the Official Journal of the European Union, these standards create a presumption of conformity, streamlining compliance for providers and fostering legal certainty.[315] The European Commission plays a key role by issuing standardisation requests to the European Standardization Organizations ensuring comprehensive deliverables that address not only regulatory requirements but also AI sustainability goals, such as resource and energy efficiency.[316] These standards, crucial for harmonising

[314] Eleanor Spaventa, 'Fundamental Rights in the European Union', *European Union Law* (Oxford University Press 2023).
[315] Chiara Gallese Nobile, 'Regulating Smart Robots and Artificial Intelligence in the European Union' (2024) 1 Journal of Digital Technologies and Law 33.
[316] AI Act, Art. 47-48.

technical benchmarks across the Union, promote uniformity, enabling safe AI deployment in critical sectors like healthcare, law enforcement, and public services.[317]

The requests must also promote resource efficiency and sustainability, including reduced energy consumption across the lifecycle of AI systems and the energy-efficient development of general-purpose AI models. In this respect, Article 40(2) specifies that the standardisation process must involve consultations with the AI Office, stakeholders, and an advisory forum to maintain consistency and alignment with existing product legislation listed in Annex I. Additionally, participants in the standardisation process are tasked with promoting investment and innovation while safeguarding Union values and fundamental rights, as outlined in Article 40(3).[318]

Where harmonised standards are unavailable, incomplete, or delayed, Article 41 allows the Commission to adopt common specifications via implementing acts. This mechanism is a regulatory fallback, ensuring that AI systems remain subject to rigorous requirements. The adoption of common specifications occurs under four key circumstances: (1) when the European Standardization Organizations fail to accept or deliver a standardisation request within the set deadlines; (2) when harmonised standards are insufficient; (3) when harmonised standards fail to address fundamental rights concerns; or (4) when standards do not comply with the Commission's request.[319] Providers conforming to these common specifications are presumed to comply with the AI Act's requirements; however, Article 41(5), providers can adopt alternative technical solutions if they can demonstrate equivalence with the specified requirements. Importantly, if harmonised standards later become available, Article 41(4), mandates the Commission to repeal the relevant implementing acts to prevent duplication and ensure regulatory coherence.

Together, Articles 40 and 41 create a flexible yet robust framework for regulating high-risk AI systems. Harmonised standards provide a structured, industry-driven approach to compliance, ensuring alignment across sectors and fostering legal certainty. In contrast,

[317] Eduard Fosch-Villaronga, Hadassah Drukarch and Marco Giraudo, 'A Legal Sustainability Approach to Align the Order of Rules and Actions in the Context of Digital Innovation', *Technology and Sustainable Development* (Routledge 2023); Marta Cantero Gamito and Christopher T Marsden, 'Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act' (2024) 32 International Journal of Law and Information Technology.

[318] AI Act, Rec. 121.

[319] Ibid, Art. 41(4).

common specifications act as a safeguard, maintaining regulatory oversight in cases where harmonised standards fall short. However, the AI Act's reliance on these tools raises challenges: as AI technologies evolve rapidly, harmonised standards risk becoming outdated, necessitating frequent updates. Additionally, integrating fundamental rights assessments, central to the AI Act, requires expertise and stakeholder involvement beyond traditional technical standardisation processes. As such, Articles 40 and 41 reflect the AI Act's broader ambition to balance technological innovation with regulatory rigour, embedding ethical principles and sustainability at the heart of AI governance.

Providers are tasked with ensuring compliance with essential requirements and undergoing relevant conformity assessments.[320] A conformity assessment, in particular, is "a legal obligation, which must be fulfilled before a high-risk AI system is placed on the market. It aims at fostering accountability of AI providers".[321] According to Article 43, conformity assessment ensures compliance with the AI Act's requirements through external validation "to ensure a high level of trustworthiness of high-risk AI systems".[322] This requirement often involves third-party notified bodies, ensuring an independent review of compliance with the AI Act before the system can be marketed or used.

This assessment should be continuous. Providers must implement systems to monitor their AI applications throughout the lifecycle, report risks, malfunctions, or incidents,[323] and promptly undertake corrective measures. In cases of substantial modifications, a new conformity assessment is mandatory to maintain compliance.[324] Such mechanisms emphasise both ex-ante and ex-post accountability, aligning AI systems with ethical principles and legal safeguards.

Nonetheless, the assessment tools are many under the AI Act. Especially as mentioned above, providers under Article 9 may adhere to harmonised standards to fulfil their risk management obligations. These standards, while voluntary, offer structured

[320] Ibid, Art. 43.

[321] Eva Thelisson and Himanshu Verma, 'Conformity Assessment under the EU AI Act General Approach' (2024) 4 AI and Ethics 113. It is also proposed, in literature, a system of conformity assessment that establish "a procedure to implement ethics-based auditing", as in Luciano Floridi and others, 'capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act' SSRN, 2022.

[322] AI Act, Rec. 123.

[323] Ibid, Art. 73.

[324] Ibid, Art. 43(4). To clarify, in that case, the initial provider is no longer considered the provider. If the initial provider makes a substantial modification to the AI, then they are also no longer considered providers. This applies also to GenAI, as recalled by Rec. 139.

methodologies for compliance.[325] Conversely, the FRIA requires a context-specific assessment tailored to the intended use of the system. Deployers must evaluate how the system will function in its specific deployment environment,[326] including risks to privacy, non-discrimination, and human oversight. The conformity assessment, by contrast, focuses on verifying compliance with the Act's essential requirements through standardised testing and certification processes.

The interplay between providers and deployers highlights a significant information asymmetry. Providers possess technical knowledge about the system's design and limitations, which they disclose under Article 13. Deployers can and should rely on this information to perform their FRIA but also contribute unique insights from the deployment context, identifying risks specific to operational scenarios. This feedback loop requires deployers to inform providers of emerging risks or incidents, enabling providers to update their risk management systems and improve compliance mechanisms.

2.4.12 Governance and enforcement

The governance structure of the AI Act is designed to ensure effective enforcement through a combination of national and supranational bodies. At the EU level, two key institutions play a central role: the AI Office and the European AI Board. The AI Office, centralized within the Directorate-General for Communications Networks, Content and Technology (DG-CNECT), is tasked with overseeing the harmonized implementation and enforcement of the AI Act across all Member States.[327] The AI Office has already launched the organization team for the code of practice on general-purpose AI, and, more in general, provides support for implementing and delegated acts, facilitating, among other things, the establishment of regulatory sandboxes.[328]

In parallel, the European AI Board,[329] composed of representatives from each Member State along with observers such as the European Data Protection Supervisor, ensures

[325] Ibid, Rec. 61. For the role of standards in the AI Act, see Mélanie Gornet and Winston Maxwell, 'The European Approach to Regulating AI through Technical Standards' (2024) 13 Internet Policy Review.
[326] Ibid, Rec. 93, "Deployers […] can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use […]".
[327] AI Act, Art. 64 and Rec. 148.
[328] AI Act, Art. 57, para. 15.
[329] AI Act, Art. 65. Especially, para. 2: "the Board shall be composed of one representative per Member State. The European Data Protection Supervisor shall participate as observer. The AI Office shall also attend the

coordination among national competent authorities.[330] Its role includes facilitating the consistent application of the AI Act, issuing recommendations, and supporting the operation of regulatory sandboxes.[331] Saying it differently, it is a role of coordination: a vital aspect that ensures that the various national authorities responsible for overseeing AI systems can apply the regulation effectively and uniformly.[332] Thus, the Board will be the eyes of the Commission.

Nevertheless, at the national level, each Member State must establish or designate specific authorities, such as Market Surveillance Authorities (MSAs)[333] and Notifying Authorities. These authorities are responsible for monitoring AI systems' compliance, conducting real-world testing, and managing incident reports for high-risk AI systems.[334] For instance, in cases where AI systems present a threat to public safety or rights, MSAs have the power to take corrective actions, including bypassing standard assessment procedures.[335]

The integration of these bodies, both at the national and supranational levels, should ensure that AI regulation is not only implemented but also enforced in a way that protects public interests and fundamental rights.

However, concerns remain about the effectiveness of these entities, particularly regarding potential conflicts of interest for notified bodies and the capacity of national authorities to enforce AI regulations consistently. The issues related to these systems of governance, in substance, can be summarised as an over-complex system, a potential lack of autonomy and overlapping responsibilities of the bodies involved.[336]

On the first aspect, it is clear that the governance framework proposed by the AI Act involves multiple. In particular, unlike the European Data Protection Board under GDPR,[337] the AI Board lacks the authority to revise or resolve disputes between national

---

Board's meetings, without taking part in the votes. Other national and Union authorities, bodies or experts may be invited to the meetings by the Board on a case by case basis".

[330] AI Act, Art. 65, para. 3, "each representative shall be designated by their Member State for a period of three years, renewable once".

[331] AI Act, Art. 66.

[332] AI Act, Rec. 149.

[333] AI Act, Art. 70, para. 1, "Each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority for the purposes of this Regulation. Those national competent authorities shall exercise their powers independently, impartially and without bias".

[334] AI Act, Rec. 153-154.

[335] AI Act, Art. 79.

[336] Novelli and others (n 272).

[337] GDPR, Art. 65.

supervisory bodies with binding force. This could hinder the uniform application of the AI Act across Member States, particularly when national authorities interpret the legislation in divergent ways.[338] Generally speaking, the AI Act lacks detailed guidance on preventing conflicts of interest within these bodies and ensuring transparency, particularly when these bodies outsource their tasks: this might pave the floor for potential conflicts of interest involving notified bodies, which are responsible for assessing high-risk AI systems.[339]

Secondly, there is concern that the roles of the AI Board, the Advisory Forum, and the Scientific Panel are not clearly distinct, and, in general, overlap with existing authorities.[340] For example, both the Advisory Forum and the Scientific Panel provide expert advice to the Board and the Commission. This overlap could lead to inefficiencies, as these bodies might duplicate efforts instead of streamlining their functions.[341] AI governance is already fragmented, with multiple authorities overseeing different aspects of AI development and deployment. The AI Act might not help with making clarity.

Thus, since the governance structure of the AI Act is highly decentralized, the Commission has a critical role to play in coordinating these bodies to ensure that the nationalization of certain procedures does not weaken the overarching goals of the AI Act. This includes ensuring that AI regulations are enforced consistently across all Member States and that national authorities do not water down the protection of fundamental rights in the implementation phase. Indeed, the Commission, as the primary enforcer of the regulatory framework governing AI in the European Union, holds considerable powers that are fundamental to the proper functioning of this framework.[342]

One of its most important roles is monitoring compliance and ensuring enforcement across the EU.[343] In particular, the Commission reviews compliance reports from these authorities, and when non-compliance is identified, it is empowered to take corrective

[338] A provision that, instead, as proved to be crucial, as highlighted Lisette Mustert, 'The EDPB's Second Article 65 Decision - Is the Board Stepping up Its Game? Reports: European Union' (2021) 7 European Data Protection Law Review (EDPL) 416.

[339] AI Act, Art. 28-29.

[340] This aspect has been highlighted by the EDPB which issued the Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework, 16 July 2024.

[341] Scholars highlight the need for an "AI Coordination Hub" which will serve as a crucial element of collaboration between all the institutions involved in the enforcement of the AI Act. See Novelli and others (n 272).

[342] Especially, the EU Commission holds exclusive powers under some AI Act areas, as is the case in the enforcement of Chapter V on general-purpose AI models. AI Act, Art. 88.

[343] AI Act, Art. 74, para. 11.

action.[344] Another crucial power is the adoption of delegated and implementing decisions under Chapter XI of the AI Act.[345] These acts allow the Commission to update technical standards, specify the operational details for high-risk AI systems, and adapt the regulatory framework to evolving technological landscapes. These decisions are legally binding acts directly applicable across all Member States without the need for national transposition.[346] They are particularly important in ensuring the uniform implementation of EU legislation, especially in cases where national variations might lead to inconsistent applications[347] of prohibited and high-risk AI technologies, such as real-time remote biometric identification systems in law enforcement. Although the implementation of EU law primarily rests with the Member States,[348] also due to the principle of subsidiarity, the Commission's role in adopting implementing acts is seen as an exception to the rule, and it is subject to the oversight of the states.[349]

The role of the European Commission in adopting and implementing decisions is not just a technical necessity; it plays a pivotal part in bridging the gap between the diverging standards of oversight seen in judicial and administrative bodies. These implementing decisions allow the Commission to provide uniform guidance to Member States, ensuring that the AI systems, particularly those involving biometric identification, are regulated consistently across the Union.

2.4 Conclusion

This chapter has provided a comprehensive exploration of the conceptual, technical, and regulatory dimensions of artificial intelligence, laying a solid foundation for the

[344] AI Act, Art. 81.
[345] AI Act, Artt. 97-98, and Rec. 175.
[346] TFEU, Artt. 290-291.
[347] Under Article 291(2) TFEU, implementing powers may be conferred upon the Commission to adopt legally binding acts. These powers are exercised when the uniform application of EU legislation is required, and such decisions serve as a means to ensure consistency across Member States. Loewenthal, "Article 291 TFEU" in Kellerbauer, Klamert, and Tomkin (Eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press, 2019).
[348] Merijn Chamon, 'The Legal Framework for Delegated and Implementing Powers Ten Years after the Entry into Force of the Lisbon Treaty' (2021) 22 ERA Forum 21.
[349] As the EU powers are shaped, they are "naturally responsible for implementing the legally binding acts of the European Union [and they shoud be] responsible for controlling the Commission's exercise of these implementing powers". See Commission Proposal for a 'Regulation of the European Parliament and of the Council laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers' COM(2010) 83 final. For an understanding of the modification of the comitology system, see Robert Schütze, '"Delegated" Legislation in the (New) European Union: A Constitutional Analysis' (2011) 74 The Modern Law Review 661.

deeper discussions to follow. Beginning with an inquiry into the nature of AI, its conceptual and technical foundations were unpacked, offering clarity on what AI is, and what it is not. The distinctions between symbolic and sub-symbolic AI, as well as the transformative advancements in machine learning and deep learning, provided a critical backdrop for understanding the trajectory of AI's development. These insights culminated in the discussion of FRT as a case study, illustrating the intersection of AI's technical capabilities with its ethical and societal implications.

The shift from automation to autonomy, explored in Section 2.3, highlighted the unprecedented challenges posed by AI systems capable of making decisions independently. This evolution introduces complex questions around accountability, transparency, and fundamental rights, all of which demand robust governance mechanisms. These challenges were directly linked to the objectives and structure of the AI Act, a pioneering regulatory framework by the European Union.

The chapter delved into the core elements of the AI Act, including its objectives, material scope, and risk-based approach. The detailed analysis of prohibited and high-risk AI systems, alongside the requirements and obligations imposed on providers and deployers, underscored the regulation's dual focus on product safety and fundamental rights protection. Of particular relevance was the discussion on the Fundamental Rights Impact Assessment (FRIA), which bridges the technical and ethical dimensions of AI governance. This assessment tool serves as a critical mechanism for ensuring that high-risk systems, including FRT, align with European values and do not infringe upon fundamental rights.

This chapter's exploration of the AI Act sets the stage for Chapter 3, where the focus shifts to facial recognition technology. By zeroing in on FRT, the next chapter examines how this specific application of AI challenges existing legal frameworks and calls for tailored governance strategies. The discussions in Chapter 2, from the technical intricacies of AI to the legislative innovations of the AI Act, are instrumental in understanding the complexities of regulating FRT and ensuring the protection of fundamental rights. Chapter 3 will build upon this foundation, offering a critical evaluation of how FRT exemplifies the broader challenges and opportunities within AI governance, ultimately paving the way for a robust analysis of the rights at stake and the potential for an effective regulatory framework through FRIA.

In conclusion, the AI Act's approach to regulation, particularly in high-risk areas like biometrics, underscores the critical need for human oversight and robust enforcement mechanisms: both to rebalance the AI power of autonomy. As AI continues to evolve, the challenge for both the EU and its Member States will be to maintain this delicate balance, ensuring that technological progress does not come at the expense of fundamental rights. It is the duty of constitutional law to guide and test the consistency of these rules with fundamental principles, ensuring that they uphold the values of "prosperity, equity, freedom, peace and democracy".[350]

[350] Draghi (n 76).

3. THE REGULATION OF FACIAL RECOGNITION TECHNOLOGY

SUMMARY: 3.1 Introduction. – 3.2 The context; 3.2.1 Law enforcement use of FRT: a taxonomy; 3.2.2 From traditional forms of surveillance to FRT: looking for a new paradigm. – 3.3 The technical framework. – 3.4 The fuel of FRT: biometric data; 3.4.1 Special categories of personal data: the GDPR paradigm on biometric data; 3.4.2 Special categories of personal data: the LED paradigm on biometric data; 3.4.3 Non-law enforcement use of biometric data: the case of the Digital Identity Wallet. – 3.5 The regulation of FRT in the AI Act; 3.5.1 The AI Act *lex specialis*; 3.5.2 Issues and *de iure condito* perspectives. – 3.6 Toward a comprehensive legal framework for FRT; 3.6.1 The GDPR framework; 3.6.2 The LED framework; 3.6.3 The AI Act framework; 3.6.4 Integrated obligations across the GDPR, LED, and AI Act. – 3.7 Conclusion.

3.1 Introduction

Having explored in Chapter 2 foundational principles, challenges, and regulatory frameworks shaping the governance of AI, particularly in high-risk applications, the present chapter focuses on the European regulatory landscape for FRT. By examining the interplay between key instruments such as the GDPR and the LED, and the AI Act, this chapter delves into the evolving standards and requirements for the processing of biometric data. As highlighted in Chapter 2, the rapid deployment of AI-driven technologies has introduced unprecedented risks to privacy, autonomy, and fundamental rights, necessitating a coherent and harmonized legal framework. This chapter builds on these insights to assess the regulatory challenges and opportunities in the governance of biometric systems within the European Union.

Facial recognition technology is a specimen of how technology relates in our time. Its adaptiveness and ubiquity make of FRT a definitory tool of these times: especially since the outbreak of COVID-19, it has been exploited by both public authorities and

private actors. From public spaces[351] to the use in the workspace[352], in schools,[353] in airports,[354] or through personal devices,[355] FRT is increasingly embedded in our daily lives.[356]

While the ability to identify individuals solely from a facial image is undeniably valuable, especially in the context of crime prevention, it also raises concerns regarding privacy protection, which entails the right to safeguard against unwanted intrusions into one's personal sphere: i.e., for purposes of contact tracing, authentication, forensics, and surveillance.[357]

This chapter, after having situated, in Ch. 2 FRT within the larger context of AI technologies,[358] explores its technical foundations, societal implications, and legal frameworks. Beginning with an overview of the broader societal and technological landscape, the chapter transitions to the technical functioning of FRT, offering a detailed analysis of its mechanisms and applications. Subsequently, it addresses the legal and regulatory environment governing biometric systems, including the GDPR, the LED and the AI Act, as anticipated. Particular attention is devoted to how these frameworks intersect and their adequacy in addressing the unique challenges posed by FRT. Finally, the discussion narrows its focus to FRT-specific governance, particularly its use in law enforcement, considering its interplay with other biometric systems and the implications for fundamental rights. While FRT has been lauded for enhancing efficiency and security, it simultaneously triggers substantial concerns related to privacy, data protection,

[351] Italian DPA, Measure of 11 January 2024, Register of Measures, No. 5 of 11 January 2024. Theodore Christakis and others, 'Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term' SSRN (15 May 2022).

[352] Italian DPA, decisions no. 105, 106, 107, 108 and 109, 22 February 2024. On the same matter, also the Information Commission Officer (ICO), Order against Serco Limited UK, 23 February 2024.

[353] Trib. Adm. de Marseille, n. 1901249, 3 February 2020. On this case, allow the reference to Federica Paolucci, 'Riconoscimento Facciale e Diritti Fondamentali: È La Sorveglianza Un Giusto Prezzo Da Pagare?' [2021] MediaLaws - Rivista di Diritto dei Media.

[354] 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), 24 May 2024.

[355] Giuseppe Mobilio, 'Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies' (2023) 12 Internet Policy Review; Tanja Kammersgaard Christensen, 'Pre-Installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective' (2024) 53 Computer Law & Security Review 105980.

[356] Natalia Menéndez González, *The Impact of Facial Recognition Technology Empowered by Artificial Intelligence on the Right to Privacy* (Routledge 2022).

[357] Arianna Vedaschi and Chiara Graziani, 'New Dynamics of the "Post-COVID-19 Era": A Legal Conundrum' (2023) 24 German Law Journal 1612; Marta Gomez-Barrero and others, 'Biometrics in the Era of COVID-19: Challenges and Opportunities' [2021] arXiv:2102.09258 [cs].

[358] See §2.2.3.4.

procedural fairness, and civil liberties. Striking a balance between technological progress and the protection of individual rights represents a key regulatory challenge. This chapter, that concludes the first part of the work, critically examines this balancing act, shedding light on the transformative impact of FRT and its regulation within the European Union, with a specific focus on its deployment in law enforcement, while exposing the limitations in granting full fundamental while exposing the limitations in granting full fundamental rights protection under the current framework.

3.2 The context

FRT are one of the most significant and rapidly developing artificial intelligence technologies currently available. In countries such as the United Kingdom (UK), the United States (US), and Canada, the use of this technology and its application has been widely discussed.[359]

Defined by the European Agency of Fundamental Rights "as a unique biometric identifier",[360] many governments welcome such tools and are investing in applications of this technology. In France, for instance, several initiatives have been taken to use biometric recognition, such as the introduction of a program applied to public offices that has as its object the automated recognition of faces on identity documents.[361] Another example comes from nine schools in the United Kingdom, where the North Ayrshire Council decided to install cameras in order to fasten the pupils' identification for the payments of meals in the school canteen.[362] Welcomed by the parents as a measure capable of "safeguard pupils by eliminating touchpoints from their lunchtime service",[363] it was soon challenged by privacy watchdogs and the dismissal was ordered by the Information Commission Officer (ICO) of the UK as potentially infringing minors' rights.[364]

---

[359] Elizabeth McClellan, 'Facial Recognition Technology: Balancing the Benefits and Concerns' (2020) 15 Journal of Business & Technology Law 363.

[360] European Union Agency for Fundamental Rights FRA.: Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. (2019).

[361] Fink (n 146).

[362] O'Murchu C.: Facial Recognition Cameras Arrive in UK School Canteens. Financial Times (17 October 2021) <https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9> accessed 3 December 2024.

[363] 'Parental flyer', <https://www.north-ayrshire.gov.uk/Documents/EducationalServices/facial-recognition-parental-flyer.pdf> accessed 3 December 2024.

[364] This issue indeed emerged in a case that regarded some high schools in the French Provinces of Marseille and Nice that, due to a partnership with Cisco International Limited, installed cameras that would perform

However, the application of FRT in the context of law enforcement represents a more complex and controversial dimension. Law enforcement agencies have increasingly adopted FRT and AI systems due to their unparalleled ability to enhance the efficiency, accuracy, and effectiveness of policing efforts,[365] and this is the specific sector this thesis is looking at. With the term 'law enforcement authorities' we refer to Member State agencies and encompasses "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[366]

As anticipated,[367] the deployment of FRT in law enforcement is governed by multiple legal frameworks, including the EU Charter of Fundamental Rights, the GDPR, and the LED. These frameworks emphasise principles such as necessity and proportionality, ensuring that FRT use is strictly necessary for its stated purpose and proportionate to its impact on individuals' rights. Despite these safeguards, gaps remain in public awareness and oversight mechanisms: for instance, the EDPB has called for explicit legal bases for FRT deployment and robust measures to prevent misuse in the law enforcement context.[368]

Given the specific focus of this thesis, the following sections aim to unpack these challenges and to provide a structured analysis of these practices to better understand the deployment of FRT in law enforcement contexts.

facial recognition on students. Following the appeal filed by the parents' association, the Tribunal of Marseille was called upon to pronounce judgment and two aspects emerged. First, the violation of the GDPR by the school office through the installation of devices, inasmuch as they violate Article 9 of the Regulation. Secondly, in the absence of necessity and proportionality, among other things, such a system of surveillance would represent an opt-out mechanism.

[365] Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' (2018) 8 International Data Privacy Law 52; Eleni Kosta, 'Chapter 3: A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon' (2022).

[366] LED, Art. 1 (1).

[367] §1.2.2.

[368] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26 April 2023.

3.2.1 Law enforcement use of FRT: a taxonomy

Between May 2017 and April 2019, the police in South Wales (UK) scanned approximately 500,000 faces while using automated facial recognition[369] systems during public events. The applicant, Mr. Bridges, a civil rights activist, brought a judicial claim[370] against the law enforcement body to assess the legal basis of the technology and its compatibility with the right to respect for private life. That technology was meant to capture live biometric images automatically saved in a dataset and compared with face images already collected and itemized in a watchlist. The Divisional Court rejected Mr. Bridge's claim. On a second stance, the Court of Appeal considered the issue and found that the use by the police of the facial recognition technology was unlawful on the ground that it was breaching the individuals' privacy and data protection rights, under Art. 8 of the ECHR. Remarkably, the Court found that the operation lacked a proper data protection impact assessment (DPIA),[371] meaning the obligation to conduct an assessment on the processing of personal data, when the processing operations are "likely to result in high risk to the rights and freedoms of individuals".[372] Recital 38 of the GDPR further specifies,[373] in fact, that:

> "where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-

[369] Technically speaking, FRT is identifiable as a *deep learning* system and a *multilayered deep neural network,* which can be applied to many different uses: to unlock a device; CCTV cameras used to match a face with a watchlist of possible thieves; e-boarding in the airports; e-identification systems in the public administration. Xiao Han and Qingdong Du, 'Research on Face Recognition Based on Deep Learning', *2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC)* (2018).

[370] Court of Appeal, The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058, 11 August 2020.

[371] GDPR, Art. 35. This obligation will be further unpacked in Chapter 4.

[372] Eleni Kosta, 'Article 35 Data Protection Impact Assessment' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[373] At the time of the case, Brexit agreement was not in force yet. However, the Information Commissioner Office, the UK Data Protection Authority, is still relying on the GDPR model for many aspects, as witnessed by the publications of the 'Data Protection Impact Assessment Canva', 28.11.2023. The analysis of the data protection framework in the UK goes beyond the scope of this thesis that, as stated in Chapter 1 is mostly focused on the EU regulatory framework. The author relies on the analysis of Nora Ni Loideain, 'Lawfulness and Police Use of Facial Recognition in the United Kingdom: Article 8 ECHR and Bridges v. South Wales Police' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024); Giulia Gentile, 'Does Big Brother Exist?: Facial Recognition Technology in the United Kingdom' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024); Monique Mann and Marcus Smith, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 University of New South Wales Law Journal 121.

out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk".

Therefore, the legal framework on which the South Wales used FRT during the public event was insufficient to address the risks to some rights that the technology would infringe; not only on privacy but also it can produce a chilling effect on freedom of expression and freedom of association.[374]

This case highlights two critical dimensions. First, it underscores the need for robust legal frameworks that ensure the proportionality and necessity of FRT use. Second, it demonstrates the significant consequences of inadequate safeguards: harming the fundamental rights of the individuals.[375] By examining these implications, it becomes evident that the deployment of FRT requires comprehensive oversight and transparency to balance security needs with the protection of individual freedoms.[376]

FRT serves law enforcement in several primary capacities.[377] The most common application is real-time identification, where live images are compared against watchlists or databases to locate suspects, missing persons, or individuals of interest.[378] A second cluster, is composed of post-incident investigations use FRT to analyse recorded footage, identifying perpetrators or witnesses at crime scenes.[379] Thirdly, an authentication processes frequently rely on FRT to verify identities at checkpoints such as border crossings or secure facilities.[380] Lastly, categorisation involves grouping individuals

[374] Court of Appeal, The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020], id., §153.

[375] European Union Agency for Fundamental Rights (FRA): Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, id.

[376] Natalia Menéndez González, 'The Rights to Privacy and Data Protection and Facial Recognition Technology in the Global North' in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023) <https://doi.org/10.1093/law/9780192882486.003.0009> accessed 16 October 2024.

[377] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, id.; Desara Dushi, 'The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications' (Global Campus 2020).

[378] Giulia Formici, 'Sistemi Di Riconoscimento e Dati Biometrici: Una Nuova Sfida per i Legislatori e Le Corti.' (2019) 39 DPCE Online.

[379] "This forms a major shift from traditional policing, in which a specific individual is usually the starting point for a query into sources, or in which a specific crime is the starting point and where human non-automated profiling can take a long time to detect a suspect. Alternatively, risk profiling can be used to assess the risk of individuals or groups that are being surveilled to determine whether to deploy further investigative powers against them". van Schendel (n 148).

[380] In this respect, scholars distinguish between direct and indirect methods of identification, as in Miranda Mourby and Elaine Mackey, '14. Identity, Profiles and Pseudonyms in the Digital Environment' in Bart Sloot and Sascha Schendel (eds), *The Boundaries of Data* (Amsterdam University Press 2024).

based on inferred attributes, like age, gender, or ethnicity, to support crowd management or predictive policing strategies.[381] These applications significantly enhance operational capabilities but also raise critical legal and ethical concerns, requiring robust safeguards and transparent governance.[382]

As a matter of fact, identification through FRT involves comparing facial images against extensive databases: for example, during the *Bridges v. South Wales Police* case, real-time FRT was deployed to analyse live footage and identify individuals on predefined watchlists.[383] However, such practices raise concerns about privacy invasion, algorithmic bias, and the lack of transparency in defining watchlist criteria that are unprecedented.

Differently from other forms of surveillance, such as wiretapping, FRT enables real-time and large-scale monitoring of individuals in public spaces, allowing for the identification, tracking, and analysis of movements and interactions without the need for direct targeting or consent. As scholars pointed out, it is not possible to draw metaphors and parallels with previous forms of control used by public and private actors since

> "Facial recognition surveillance involves the generalised monitoring of public places or third-party image sets using facial surveillance technologies to match faces with a prepopulated list of face images held by the government. [...] This system can identify individuals at any point they are recognized by a camera, creating a virtual retrospective map of movements and activities over time".[384]

[381] This issue concerns also the use of AI in border control. This topic, while also relevant in the use of biometrics, is out of the scope of this thesis. Please refer to Simona Demková, 'The EU's Artificial Intelligence Laboratory and Fundamental Rights' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024); Francesca Palmiotto, 'Op-Ed: "Is Predictive Policing Prohibited in the EU? Yes, It Should Be"' (*EU Law Live*, 19 December 2024) <https://eulawlive.com/op-ed-is-predictive-policing-prohibited-in-the-eu-yes-it-should-be/> accessed 8 January 2025.

[382] Erik Longo, 'Predizione, Profilazione e Giustizia: Le Prospettive Costituzionali', *Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche* (Edizioni Scientifiche Italiane 2022).

[383] Genia Kostka, Léa Steinacker and Miriam Meckel, 'Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States' (2021) 30 Public Understanding of Science 671; Loideain (n 375); Allison Amatuzzo, 'Wherever We Go, We Leave a Trail: Surveillance and Sousveillance in the United States and United Kingdom' (2019) 7 Penn St. JL & Int'l Aff. 489; Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum För Rättvisa' (*EJIL: Talk!*, 26 May 2021) <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/> accessed 3 December 2024.

[384] Andrew Guthrie Ferguson, 'Facial Recognition and the Fourth Amendment' (2021) 105 Minnesota law review 1105.

Furthermore, FRT enables a sort of "travel back in times", allowing for its deployer the possibility to access stored data, rebuilding and following peoples' movements, actions, behaviours in a big span of time, and in a live or *post factum* environment, hindering the true colours of the right to privacy: *"the right to be let alone".*[385] Hence, the combination of what we have called "power of autonomy", and the scale of digital networks are melting in creating strong impact on fundamental rights, especially in the law enforcement context. In contrast, traditional forms of surveillance, as will be further explained *infra,* typically involves specific individuals and is governed by stringent procedural safeguards. Specifically, wiretapping targets one communication channel, whereas "FRT aggregates personal data, locational tracking, and behavioral patterns into a comprehensive, intrusive system of surveillance".[386]

3.2.2 From traditional forms of surveillance to FRT: looking for a new paradigm

As mentioned above, the use of control and surveillance systems has interested legislators in both European and national contexts for more than a century. Telephone tapping, finding its ancestors in mail control, eventually evolved into telephone and telematic interception.[387] Traditional forms of surveillance like these have been governed by well-established safeguards to ensure a balance between individual rights and public safety.

A landmark case is that of *Katz v US*[388] where the US Supreme Court established the right to privacy, namely of the individuals and not of the places. As a matter of fact, data protection, historically rooted in the broader concept of privacy, a principle introduced by Warren and Brandeis in 1890. More precisely, in Katz, the Court considered a situation involving the transmission of gambling information over the telephone to clients in other states. Federal agents used an eavesdropping device situated close to a public phone booth specifically in order to gather such information. Based on the recordings, Katz was

[385] Samuel D Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4, no.5 Harvard Law Review 193. See Olmstead v United States 277 US 438 (1928), Brandeis' dissenting opinion.
[386] Id.
[387] Davide Zecca 'La Tutela Costituzionale Della Segretezza Delle Comunicazioni Fra Avvento Dell'era Digitale e Crisi Del Paradigma Tradizionale Nella Ricerca Della Prova', in Davide Zecca, *La tutela costituzionale della segretezza delle comunicazioni e della corrispondenza alla prova delle tecnologie emergenti: profili comparati* (Editoriale Scientifica 2023).
[388] Katz v United States 389 US 347 (1967).

convicted of the illegal transmission of wagering information through different states.[389] Hence, the US Supreme Court established that:

> "The protection of a person's general right to privacy – his right to be let alone by other people – is, like the protection of his property and of his very life, left largely to the law of the individual States […] For the Fourth Amendment protects people, not places".[390]

A similar line was also pursued by the ECtHR, by acknowledging that the application of Article 8 of the Convention (ECHR) also to telephonic wiretapped conversations,[391] being an ancillary asset that contributes to the protection of private and family life.

In the European Union, the protection of personal data serves as a cornerstone of this effort, reflecting the shift from viewing privacy as a passive-negative right (Art. 7 CFREU) to an active, enforceable right within the digital landscape (Art. 8 CFREU).[392] As digital technologies advanced, particularly in the European Union, privacy and data protection began to evolve as distinct but complementary rights, with the EU Charter enshrining them as fundamental protections in Articles 7 and 8. This shift reflects a deeper understanding of privacy in the digital age, where individuals require active control over their personal data in response to pervasive data collection practices.[393] By mean of example, in *Digital Rights Ireland,*[394] the CJEU emphasised the necessity of proportionality and strict safeguards when processing personal data, underscoring that blanket data retention measures violate the essence of Articles 7 and 8 of the Charter. This landmark decision set a precedent for limiting state surveillance powers and highlighted the critical balance between security and privacy in the digital era.

The pressure of Courts and legislators have not been just focusing on limiting the use of surveillance systems without limits, but and moreover, it was oriented by the principle

---

[389] Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (n 5).
[390] Katz v United States, id., §350.
[391] ECtHR, *Klass and Others v Germany*, App no 5029/71, judgment of 6 September 1978.
[392] Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25 European Law Journal 140.
[393] Orla Lynskey, *The Foundations of EU Data Protection Law / Orla Lynskey* (University Press 2015); Gloria Gonzalez Fuster, *The Essence of the Fundamental Right to Data Protection: Background Paper Commissioned by the European Data Protection Supervisor (EDPS)* (European Data Protection Supervisor (EDPS) 2023).
[394] CJEU (Grand Chamber), Joined C-293/12 and C- 594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.

of proportionality, therefore, by identifying those safeguards to allow, where necessary, the use of such control instruments.

The essential cornerstone for traditional measures of surveillance has been the establishment of judicial oversight at multiple stages, including during the authorization procedure and through subsequent reviews to ensure compliance. This principle has been consistently highlighted by international and national courts.

Specifically, the ECtHR stated that "it is in principle desirable to entrust supervisory control to a judge" [395], by adopting a flexible approach according distinguishing between bulk and targeted surveillance, particularly in cases involving secret intelligence services.[396]

However, these bodies must demonstrate independence, effectiveness, and comprehensive access to the necessary information to ensure robust safeguards. This approach aligns with cases like *Klass v. Germany*[397] and *Kennedy v. UK*,[398] where quasi-judicial systems or hybrid mechanisms were deemed acceptable when judicial oversight was unavailable, provided they maintained a high standard of procedural safeguards.

In contrast, targeted surveillance, like the use that the AI Act allows of biometric identification systems by law enforcement authorities, given its higher potential for rights infringement, often requires stricter judicial oversight to ensure compliance with the principles of proportionality and necessity. In cases like *Zakharov v. Russia*[399] and *Szabò and Vissy v. Hungary*[400], the ECtHR affirmed that judicial review remains the preferable safeguard due to its inherent impartiality and its capacity to apply stringent scrutiny to intrusive surveillance measures. Nevertheless, the ECtHR has shown flexibility, recognising non-judicial oversight systems as effective when judicial components, independence, and broad oversight powers are integrated.[401]

---

[395] ECtHR, *Klass & Others v. Germany*, no. 5029/ 71 (1978).

[396] As observed by De Hert and Malgieri, the Court has often accepted alternative remedies, especially for secret services surveillance, where, traditionally, the Member States have provided "non-judiciary" oversight of secret service surveillance. Gianclaudio Malgieri and Paul De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017).

[397] Supra.

[398] ECtHR [IV Sec.,], *Kennedy v. UK*, no. 26839/05, 18 May 2010.

[399] ECtHR [GC], *Zakharov v. Russia*, no. 47143/ 06, 4 December 2015.

[400] ECtHR [IV Sec.,], *Szabò and Vissy v. Hungary*, no. 37138/ 14, 12 January 2016.

[401] Kosta, 'Algorithmic State Surveillance' (n 144).

Moreover, the Court has emphasised that any oversight system, judicial or non-judicial, must effectively address the risks of abuse inherent in surveillance practices. This was particularly evident in *Szabò and Vissy*, where the ECtHR rejected oversight mechanisms that lacked sufficient independence or the ability to assess strict necessity.[402] Similarly, in *Digital Rights Ireland*, mentioned above, the CJEU underscored the necessity of precise and rigorous safeguards for any form of surveillance.

Also on a national level, it is possible to observe how the Constitutional Courts were during the years invested with questions regarding the balance between privacy and safety. For instance, the Italian Constitutional Court has clarified the scope of application for instruments such as telephone and environmental wiretapping, stressing the need to balance two key parameters of the Italian Constitution – namely, Article 15, which protects the secrecy of correspondence, and Article 24, which guarantees the right to defence. In its rulings, the Court has stressed the importance of ensuring that procedural safeguards are in place when using these intrusive instruments.[403] Nonetheless, it is not sufficient for the legal framework to merely be proportionate to the goal of safeguarding public security. The Court also addressed the question of the procedural guarantees, or saying it differently, the check and balance between the deployment of surveillance systems within a fair procedural environment: in this sense, the Italian Constitutional Court specified that any order for surveillance or wiretapping must be issued by a judge in the form of a decree, and this decree must clearly outline the reasoning and justification for the authorisation. This includes providing a clear legal basis for the decision and ensuring that the use of such surveillance tools is both justified and limited to what is necessary to achieve its purpose.[404]

---

[402] Catherine Jasserand, 'The Future AI Act and Facial Recognition Technologies in Public Spaces: Nice to Have or Strictly Necessary?' (Social Science Research Network, 15 December 2023) <https://papers.ssrn.com/abstract=4947432> accessed 28 October 2024.

[403] Constitutional Court, dec. n. 34/1973. See, for an extensive analysis of this decision, Davide Zecca, *La Tutela Costituzionale Della Segretezza Delle Comunicazioni e Della Corrispondenza Alla Prova Delle Tecnologie Emergenti: Profili Comparati* (Editoriale Scientifica 2023). The Constitutional Court, in judgment no. 34/1973, emphasized that Article 15 of the Italian Constitution guarantees the inviolability of communications while permitting limitations by judicial authority under strict legal safeguards. These safeguards ensure that the right to privacy is not disproportionately sacrificed for crime prevention and investigation.

[404] In particular, the Constitutional Court has ruled that the requirement for serious indications of an offense is met when the order presents, even in summary form, the key elements that allow for a probabilistic assessment of the criminal conduct being investigated. This approach highlights the importance of both proportionality and judicial oversight to prevent potential abuses, ensuring that the use of such surveillance tools aligns with constitutional principles and protects individual rights.

In contrast, the deployment of facial recognition technology lacks comparable regulatory rigor. Although FRT represents a significant evolution in surveillance capabilities, it introduces risks that far exceed those posed by traditional forms of surveillance.[405] While wiretapping is typically targeted and subject to stringent procedural safeguards, FRT enables large-scale, real-time monitoring in public spaces without individuals' consent or awareness. This raises profound ethical concerns, including privacy erosion, mission creep, and discriminatory impacts.

FRT systems are particularly problematic because they operate on highly sensitive biometric data.[406] Unlike traditional surveillance, FRT involves the collection, analysis, and storage of vast amounts of biometric information, enabling not only identification but also categorisation and profiling.[407]

Despite these heightened risks, the safeguards established for traditional surveillance have not been robustly extended to FRT. Applying an argumentum *a fortiori*, if traditional forms of surveillance are subject to such rigorous protections, FRT, with its far greater potential for intrusion, should require even stricter oversight. Yet, the legal frameworks governing FRT often lag behind its rapid deployment, leaving critical gaps in accountability and transparency.

The combination of modern facial recognition software with digital networks creates a new surveillance paradigm fundamentally different from earlier technologies.[408] This

[405] "Escaping the equivalence trap allows us to distinguish face surveillance from the analog tradition of officers taking photos on the street or watching fixed camera feeds. The difference is the scope, scale, detail, personal data, locational data, and retrieval capabilities at play", Ferguson (n 386).

[406] Kindt, 'The Risks Involved upon the Use of Biometric Data and Biometric Systems' (n 59).

[407] This capability amplifies risks of misidentification and systemic bias, as demonstrated by studies from the National Institute of Standards and Technology (NIST), which highlight higher error rates for women, young people, and individuals from minority groups. See NIST, 'Face Recognition Technology Evaluation (FRTE)', (2024), in part., p. 491.

[408] These biases are rooted in the training datasets used to build AI models, which are often skewed toward predominantly white and male subjects. These disparities in accuracy raise serious ethical concerns, particularly when FRT is used in high-stakes environments such as law enforcement.[408] Misidentifications can lead to wrongful arrests, discrimination, and the reinforcement of existing societal biases. For instance, in the United States, several cases have emerged where African Americans were falsely identified by FRT, leading to wrongful detentions,[408] highlighting the potential for technologies like FRT to exacerbate racial profiling and other forms of systemic discrimination. See the analysis in Gizem Gültekin-Várkonyi, 'Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation' (2024) 13 Internet Policy Review. Cases have been collected on the age and racial biases replicated by FRT, such as in 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 3 December 2024; Kashmir Hill, 'Wrongfully Accused by an Algorithm' *The New York Times* (3 August 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> accessed 3 December 2024.

paradigm raises questions about the balance between security and fundamental rights. Systems like FRT enhance the ability of both public and private entities to monitor individuals in real-time, eroding privacy and fostering a chilling effect on freedoms such as movement and assembly. [409] As Richards aptly observed, surveillance can chill civil liberties, discouraging people from engaging in lawful but unconventional or controversial activities due to fear of being monitored. [410]

Given these premises, the need for robust legal frameworks to regulate the deployment of FRT is urgent. The next sections will analyse the technical and legal dimensions of biometric surveillance systems, outlining the critical risks to fundamental rights and proposing pathways to ensure compliance with constitutional principles and international human rights standards.

3.3 The technical framework

Biometric systems like FRT are specialised applications of AI, as they enable technologies to interpret and recognise human faces in a way that mimics human cognition. The growing reliance on FRT exemplifies how AI technologies are moving beyond theoretical research and into practical, impactful applications with broad societal implications.

Before moving to the depth of the technical analysis, it is to be explained the distinction between biometrics and biometric data. The former refers to the technology and methods used to measure and analyse unique physical or behavioural characteristics, like facial recognition, fingerprint scanning, or voice recognition. This term encompasses the processes, devices, and systems involved in capturing and using these traits.[411] Instead, the term biometric data refers to the actual data used to train or to make analyses or measurements gathered from individuals through biometric methods: "it covers the technical transformation of biometric characteristics into formats that can be used for biometric recognition".[412] Hence, speaking of biometric data, from a data protection

[409] Malcolm Katrak and Ishita Chakrabarty, 'Privacy, Political Participation, and Dissent: Facial Recognition Technologies and the Risk of Digital Authoritarianism in the Global South' in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023).
[410] Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934.
[411] Catherine Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data'' (Social Science Research Network, 1 June 2016) <https://papers.ssrn.com/abstract=3230342> accessed 3 December 2024.
[412] Id.

perspective,[413] is the digital representation of a physical or behavioural trait used for identification or verification purposes.

Facial recognition systems, indeed, fall into the broader category of biometrics, and this why the AI Act positions the regulation of FRT in the broader umbrella of "biometric identification systems", dividing it in real-time biometric systems and post-remote biometric systems, as explained *infra*. The distinction between biometric data and biometric systems is crucial to not misunderstand the different regulatory layers that touch upon the processing of biometric data, on the one hand, and on the use of systems trained with them, on the other, being FRT a picture of this latter one.

Hence, looking at the technical aspects, at the very beginning, biometric systems were similar to symbolic AI, where they attempted to analyse faces in a way that mimicked human thinking.[414] These approaches relied on measuring facial features based on rules, similar to anthropometry, whilst struggling with accuracy because small variations in images, like lighting or angle changes, made it hard to get consistent measurements.[415]

The approach evolved with the introduction of "Eigenfaces"[416] in the 1990s, which took a more mathematical and data-driven route. Instead of identifying specific facial features, this new computer science method treated each face image as a set of pixel values.[417] This "holistic" approach viewed faces as vectors in a high-dimensional space, simplifying the process by skipping detailed feature extraction.

Whereas, at the heart of modern FRT systems are machine learning and AI algorithms. These algorithms train on massive datasets of facial images to learn the unique patterns of human faces, improving the accuracy and efficiency of the recognition process. However, the reliance on AI also introduces concerns about bias, accountability, and transparency in how FRT operates. When FRT systems fail to perform correctly,

---

[413] Hence, linking the collection of biometric data to an identified or identifiable natural person. See the Italian Data Protection Authority (DPA), 'Guidelines on Biometric Recognition and Graphometric Signature Annex A to the Garante's Order of 12 November 2014' (2014).

[414] See §2.2.3.2.

[415] Ali Akbari, 'Facial Recognition Technologies 101: Technical Insights' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

[416] Nikola Vukobrat and others, 'Chapter 4 - Implementation of Two Factor Authentication Using Face and Iris Biometrics' in Bharat Bhushan and others (eds), *Blockchain Technology Solutions for the Security of IoT-Based Healthcare Systems* (Academic Press 2023) <https://www.sciencedirect.com/science/article/pii/B9780323991995000045> accessed 8 January 2025.

[417] Danny Styvens Cardona-Pineda and others, 'Face Recognition—Eigenfaces' in Julian Andres Zapata-Cortes and others (eds), *Handbook on Decision Making: Volume 3: Trends and Challenges in Intelligent Decision Support Systems* (Springer International Publishing 2023).

especially in critical areas like law enforcement, the consequences can be severe, leading to false identifications and potential rights violations. As a matter of fact, the real breakthrough came with deep learning,[418], especially with the use of Convolutional Neural Networks (CNNs).[419] These networks can automatically learn important features from images without relying on manually set rules. CNNs break down the image into patterns, identifying increasingly complex features layer by layer. This automated learning process has made deep learning-based facial recognition systems far more adaptable and accurate, even in challenging conditions, leading to modern successes in both object and facial recognition.[420] In FRT systems, deep neural networks process images through successive layers, with each layer extracting increasingly detailed features of a face, such as the spatial relationships between eyes, nose, and mouth. This layered processing allows FRT to create a unique mathematical representation, or "template," of each face, enabling high accuracy even under varying conditions, such as changes in lighting, angle, or facial expression.[421]

The process of the face analysis involves several stages:[422]

- Image acquisition: the system captures an image or video frame of a face, typically through cameras.
- Preprocessing and feature extraction: the image is standardised, and essential features are extracted. this step reduces noise and enhances the system's ability to recognize faces accurately.
- Encoding: the extracted features are transformed into a mathematical representation, precisely a vector that uniquely characterizes each face.
- Matching and verification: The system compares this encoded template against a database of stored templates for identification or verification.

---

[418] Specifically, deep Learning is a subset of machine learning techniques, as examined in Chapter 1, that employs multi-layered neural networks – hence the term "deep" – to model complex, abstract patterns in large datasets. Han and Du (n 371).

[419] §2.2.3.3.

[420] Akbari (n 130); Xiangyu Zhang, 'Convolutional Neural Networks and Architectures' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024) <https://doi.org/10.1007/978-3-031-43567-6_2> accessed 25 October 2024; Shepley (n 139).

[421] Anirudha Ghosh and others, 'Fundamental Concepts of Convolutional Neural Network' in Valentina E Balas, Raghvendra Kumar and Rajshree Srivastava (eds), *Recent Trends and Advances in Artificial Intelligence and Internet of Things* (Springer International Publishing 2020); Jacqueline G Cavazos and others, 'Accuracy Comparison across Face Recognition Algorithms: Where Are We on Measuring Race Bias?' [2020] arXiv:1912.07398 [cs]; Li, Jain and Deng (n 2).

[422] FRA, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 21 November 2019;

FRT systems generally operate by capturing and analysing facial features to identify or verify a person's identity. The process typically involves several key stages.[423] First, there is "face detection": the system first detects a face from an image or video feed, isolating the face from the background and other objects. This step is crucial for ensuring that the system can accurately focus on the individual to be identified.[424] After detecting the face, the system aligns the facial features, such as the eyes, nose, and mouth, into a standard format. This normalisation process ensures that FRT can work accurately even if the face is viewed from different angles or under varying lighting conditions. The system then extracts a set of key features from the aligned face using machine learning algorithms. These features – such as the distance between the eyes or the shape of the nose – are converted into a biometric template, a numerical representation that uniquely identifies the individual. Finally, the system compares the biometric template against a database of stored images (e.g., watchlists, ID databases) to find a match. In some cases, this step involves comparing the input face with thousands or millions of other faces to identify the individual (identification mode). In others, the system simply verifies that the input face matches a specific person in the database (verification mode).[425] The whole features are summarized in the table below.

Table 3 – Face recognition key features.

Stage	Description	Technical focus
Detection	The system detects a face from an image or video feed, isolating it from the background.	Image processing and facial detection algorithms.
Alignment	Once detected, the system aligns the facial features into a standard format, ensuring	Normalization of facial data to adjust for angles, lighting, and pose variations.

[423] Akbari (n 130). See also Catherine Jasserand, 'Biometric Data, Within and Beyond Data Protection' in Bart Van der Sloot and Sascha van Schendel (eds), *The Boundaries of Data* (Amsterdam University Press 2024).

[424] Working Group 29, 'Opinion 3/2012 on developments of biometric technologies', 27 April 2012, 00720/12/IT WP193.

[425] Usually, FRT works in these two modalities: verification and identification. Verification (1-to-1 matching) stands for systems that check if a live image matches a single stored image, commonly used for access control. Then, identification (1-to-N matching) means systems that compare a live image against multiple stored templates, such as those in a database of suspects or persons of interest, a method often used in law enforcement.

	accurate recognition despite different angles or lighting.	
Extraction	Key facial features (e.g., eyes, nose, mouth) are extracted and converted into a numerical code or biometric template that represents the individual.	AI-driven feature recognition using deep learning models, extracting unique biometric data points
Matching	The biometric template is compared against stored databases or watchlists to either identify the person (identification) or verify a match (verification).	AI and machine learning algorithms match extracted features against stored facial data for identification or verification.

These systems are trained in biometric data, consisting of unique physical characteristics – such as facial geometry, which can uniquely identify individuals.[426] Biometric data is more than just image data; it is sensitive, personal information that requires robust protection due to its permanent and uniquely identifiable nature. Unlike passwords, biometric data cannot be changed if compromised, which raises significant privacy concerns, particularly in the context of mass surveillance or unauthorised use. For this reason, as will unpacked in the following legal framework, biometric data are classified by the GDPR as "special categories of personal data".[427] As the following sections will detail, the legal frameworks governing the use of biometric data, particularly within the European Union, underscore the need for coordination and robust safeguards to mitigate these risks and uphold fundamental rights. Hence, the following section will aim at describing the provisions applicable to biometric data and nuanced approaches between law enforcement and non-law enforcement uses of this type of data.

3.4 The fuel of FRT: biometric data

In the previous section of this chapter, the analysis of FRTs focused on their external context, exploring their unique features and the challenges they pose compared to traditional forms of surveillance. By examining how FRT functions and its underlying

[426] Els J Kindt, 'Biometric Data, Data Protection and the Right to Privacy' in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013).

[427] GDPR, Art. 9. See Rec. 51, "personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedom".

technological patterns, the discussion shifted from an external perspective to a deeper understanding of its intrinsic characteristics. Building on this foundation, the focus now turns to the "fuel" of FRT systems – biometric data – and the legal framework governing its use. This section delves into the regulation of biometric data, highlighting the interplay between key legal instruments such as the GDPR and the LED, and examining how these frameworks address the substantial risks and challenges associated with biometric data processing.

3.4.1. Special categories of personal data: the GDPR paradigm on biometric data

When analysing the legal context of FRT, one cannot depart from Article 9 of the GDPR. As briefly anticipated, it establishes a broad prohibition on processing "special categories of personal data," commonly referred to as "sensitive data."[428] Precisely, the Working Party 29 (WP29) clarified that

> "The rationale behind regulating particular categories of data in a different way stems from the presumption that misuse of these data could have more severe consequences on the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "normal" personal data. Misuse of sensitive data, such as health data or sexual orientation (e.g. if publicly revealed), may be irreversible and have long-term consequences for the individual as well as his social environment".[429]

This category includes information that can uniquely identify a person through biometric data, such as facial recognition data, and also encompasses genetic data,[430] data revealing racial or ethnic origin,[431] political opinions,[432] religious beliefs,[433] and health status.[434] Such data is regarded as especially vulnerable, meriting a higher standard of

[428] WP29, 'Advice paper on special categories of data ("sensitive data")' (2011).
[429] Id., p. 4.
[430] GDPR, Art. 4, para. 13.
[431] WP29 (2011), id., p. 11. The category is derived from Art. 21, para. 1, CFREU, itself drawn from Art. 19 TEU.
[432] CFREU, Art. 11.
[433] CFREU, Art. 10-11-21, para. 4.
[434] Also, Art. 6, Convention 108+ for the protection of individuals with regard to the processing of personal data, 2018.

protection due to its potential impact on fundamental rights and freedoms.[435] However, Article 9 forms a dual structure: a general prohibition paired with an exhaustive list of exceptions to ensure that sensitive data processing is both justified and necessary. Indeed, the GDPR does allow for certain exceptions to this prohibition under Art. 9, para 2. For example, processing may be permitted if the data subject gives explicit consent,[436] if processing is required for employment or social protection under specific legal provisions,[437] if it serves a substantial public interest under Union or Member State law.[438] Additionally, processing may be permitted in cases concerning health care, vital interests, or scientific research under strict safeguards.[439]

Focusing on biometric data, this concept was slowly introduced in the European regulatory framework, being absent in Directive 95/46/EC.[440] A definition only arrived in WP29's Opinion of 2007:[441] "biological properties, behavioural aspects, 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".

With the GDPR and Convention 108+, hence, it was established a precise definition of biometric data was "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".[442] Therefore, as also recalled by Rec. 15 of the GDPR, simple video footage or photographs, therefore, fall into this category insofar as these conditions relating to i) the nature of the data – i.e. the reproduction of the physical, physiological or

[435] Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[436] GDPR, Art. 9, para. 2, lett. a). Unlike general consent, explicit consent requires a clear, definitive agreement from the data subject, including a detailed explanation of processing purposes. Controllers must also inform data subjects that they can withdraw consent at any time. See Lee A Bygrave and Luca Tosoni, 'Article 4(11). Consent' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[437] GDPR, Art. 9, para. 2, lett. b). For instance, processing data on an employee's religion to calculate church tax, or using biometric data for workplace access, falls under this exception.

[438] Id., Art. 9, para. 2, lett. c).

[439] Id., Art. 9, para., 2, letts. d-j).

[440] 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.

[441] Working Party 29, 'Opinion 4/2007', WP136 (2007).

[442] GDPR, Art. 4, para. 1, no. 14).

behavioural characteristics of a natural person); ii) the means and modalities of the processing – i.e. their submission to specific technical processing); iii) the purpose of the processing, as in the possibility of uniquely identifying a natural person).[443] For instance, if the data controller is using the video collected by a CCTV camera and tracking some individuals for the purpose of monitoring them, it would amount to a biometric identification method because it is aimed at recognition through the use of specific technical processing.

Following the legal analysis, and given the variety of objectives FRT can serve, it becomes essential to distinguish between these different purposes. For instance, when FRT aims to identify a person via a one-to-many comparison, it is clear that biometric data regulations apply. Whereas, for one-to-one verification or authentication, the application is less straightforward. The EDPB clarified that even if the personal details of the subject are unknown, storing facial data for reference, such as for tracking someone, as in the example, still constitutes biometric data processing. Therefore, these regulations apply regardless of whether the system verifies a known individual – e.g. checking an ID photo – or merely uses a biometric template[444] without identifying details. This distinction highlights a nuanced approach: while strict 'identification' applies to one-to-many uses, 'detection' may better describe the use of stored biometric patterns for reference, where identification is not the primary purpose.[445]

Differently, in the case of 'face detection', meaning identifying that there is a face and not adding the level of recognising someone, does not constitute a processing of personal data if a biometric template is not created.[446] As also recalled by the Italian Data Protection Authority in the case of installation of 'totems' or digital signage in a railway station, e.g., display showing advertising news, the use of processing software capable of extracting statistical data from the images taken in an almost immediate manner, without

[443] EDPB, 'Guidelines 3/2019 on processing of personal data through video devices', 29 January 2020.

[444] "Templates are commonly used in biometric systems based on fingerprinting and are usually considered by system providers as a way to protect the individual. Nevertheless, depending on the system/algorithm used to generate the template, there are potential risks related to the possibility to link templates with other fingerprint databases in order to identify individuals", WP29, 'Opinion 3/2012 on developments in biometric technologies', 00720/12/EN WP193, 27 April 2012.

[445] Catherine Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data'' (Social Science Research Network, 1 June 2016) <https://papers.ssrn.com/abstract=3230342> accessed 3 December 2024; Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative* (n 61).

[446] Mobilio, Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative (n 2);

biometric processing or recording of images, or live access, "suggests that adequate safeguards are in place to ensure that the fundamental rights and freedoms, as well as the dignity and confidentiality of the persons concerned are not jeopardised".[447] Hence, since the software was not able to identify the data subject, but the system was just configured based on mere 'face detection' and not 'face recognition' algorithms, it cannot identify the individual's face, and it does not amount to the processing of biometric data.

Another layer is the use of such data for purposes of categorising a data subject, meaning establishing "whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action".[448] In this case, even if the identification of the data subject is not achieved, it will fall into the application of Art. 9 GDPR; hence, it will be considered a processing of special categories of personal data.[449]

As will be further explained *infra,* the jurisprudence of the CJEU has also reinforced the strict application of these rules, particularly focusing on the principle of proportionality and the necessity of adequate safeguards to protect fundamental rights.[450] The Court has consistently underlined that any derogation from Article 9's prohibition must meet stringent conditions to uphold the core principles of the GDPR, especially where sensitive data is involved. This layered structure within Article 9 reflects the European legislator's intent to tightly regulate biometric and other sensitive data processing, balancing the potential societal benefits of data use with individual rights protections.[451]

[447] Italian DPA (Garante), Order no. 551/2017, 21 December 2017, doc. no. 7496252. Trad. aut.
[448] EDPB, 2022, id.
[449] As specified by a briefing published by the European Parliament (EP), this use of biometric features that might extract information about the race and the sex of a natural person is particularly sensitive from an ethical perspective, "in relation to the definition of categories, the associated assumptions and the conclusions or reactions triggered by the system, leading to risks such as discrimination, stigmatisation, and the drawing of inappropriate inferences". EP (Juri and Peti committees), 'Biometric Recognition and Behavioural Detection', 2021.
[450] CJEU (Fourth Chamber), C-291/12, *Michael Schwarz v Stadt Bochum*, judgment of 17 October 2013.
[451] Els J Kindt, 'The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing' in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013).

3.4.2. Special categories of personal data: the LED paradigm on biometric data

In 2021, the Swedish Data Protection Authority (DPA) fined the Swedish Police Authority for using facial recognition technology in a pilot project without fully complying with the GDPR.[452] The Swedish Police Authority implemented FRT to support criminal investigations, but the DPA found several breaches of GDPR requirements, underscoring the need for robust data protection measures, especially with biometric data. In particular, the Police were using Clearview AI, the controversial American app, without conducting a sufficient DPIA before implementing FRT.

In this case, the DPA found that the Police Authority processed biometric data without a lawful basis under GDPR. Biometric data, considered a "special category" under GDPR, requires a specific legal basis for processing, usually involving explicit consent or necessity for substantial public interest. The Police Authority's lacked of sufficient legal justification for processing biometric data underscored a failure to comply with the GDPR standards.

This case is just an example of how the GDPR framework must necessarily complemented by the Law Enforcement Directive (LED), since the GDPR does not apply to specific law enforcement scopes, being the specific framework of the Directive, as specified also by Art. 1 LED.[453] Hence, the LED, under Art. 10, addresses the processing of sensitive data by law enforcement authorities, specifically in the context of criminal justice.[454]

The provision is very similar to Art. 9 of the GDPR, both in terms of the category of sensitive data and the structure. After a general prohibition in processing such data, Art. 10 specifies that the processing of these categories of data is permitted only under strict conditions, recognising the potential impact on individual rights and freedoms.[455] Thus,

[452] IMY (Swedish DPA), DI-2020-2719, 11 February 2021. For a comment, see Miriam Kohn, 'Clearview AI, TikTok, and the Collection of Facial Images in International Law Comments' (2022) 23 Chicago Journal of International Law 195.

[453] LED, Art. 1, para. 1 "competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

[454] Catherine Jasserand, 'Article 10: Processing of Special Categories of Personal Data' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED)* (Oxford University Press 2024).

[455] See LED, Rec. 37, "Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the

as outlined in Recital 104 of the Directive, any limitations on Articles 7 and 8 of the Charter must align with the requirements of Article 52(1) of the Charter, particularly observing the principle of proportionality. As repeatedly emphasized in CJEU jurisprudence, these rights are not absolute but must be balanced according to their societal role.[456] Therefore, when weighed against the general interest in prosecuting criminal offences, Articles 7 and 8 may be balanced to permit, under specific conditions outlined below, the processing of personal data for the purpose of conducting criminal investigations.[457]

Such conditions are: i) the processing should be strictly necessary; ii) respecting the applicable safeguards; iii) and, only when serious crimes are committed and, or, to be investigated.

First of all, the LED sets a threshold for processing sensitive data, mandating that such processing must be "strictly necessary"[458] and accompanied by "appropriate safeguards."[459] This means that law enforcement authorities can process sensitive data only when it is essential to the purpose at hand, such as investigating a serious crime, and

---

vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject.".

[456] CJEU (Grand Chamber), C-507/2017, *Google v. CNIL,* 24 September 2019, §60. See, also, more recently, CJEU (Grand Chamber), C-118/2022, *NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti*, 30 January 2024, where the Court reinstated the need to balance the protection of public security with fundamental privacy rights under Articles 7 and 8 of the EU Charter of Fundamental Rights. The Court stressed that even in the context of serious crime prevention, personal data processing by law enforcement must respect proportionality and necessity, ensuring that privacy rights are safeguarded.

[457] Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779; Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 European data protection law review (Internet) 367; Kindt, 'The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing' (n 453).

[458] As noted by the CJEU, strict necessary means that the processing of these data must be proportionately balanced with the public interest, e.g., the exact interest pursued by the authorities while investigating a crime. CJEU (GC), *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others***,** Joined C-203/15 and C-698/15, 21 December 2016, para. 117, and CJEU (GC), *La Quadrature du Net and Others v Premier ministre and Others*, Joined C-511/18, C-512/18, and C-520/18, 6 October 2020, paras. 141–142. The EDPB further specified in the aforementioned guidelines that "the interference to the protection of personal data and its restrictions is limited to what is absolutely necessary, i.e., indispensable, and excluding any processing of a general or systematic nature". See EDPB, 2022, id.

[459] The law must lay down the appropriate safeguards to prevent the adverse effects on individuals' fundamental rights. Specifically, Rec. 37 includes adequate security measures, stricter rules on staff access to sensitive data, a prohibition to transfer the data or limited data collection to cases when other data of the individual at stake are collected. As will be examined in the following chapters of this thesis, the jurisprudence of both the CJEU and the ECtHR followed up on this specific safeguard. Hence, the deletion of previous data and authorisation measures oversight by a judicial authority, complete the previous list.

only if no less intrusive means are available.[460] Additionally, the processing must be legally authorised, either by EU or Member State law, to protect vital interests or when the data has been manifestly made public by the data subject. Henceforth, the limits set out in the LED are more specific than the one of the GDPR, not only because of the different scope of the law but also due to the particularly delicate balance that must be achieved.

For this reason, the jurisprudence of the CJEU stated for a long time a principle that biometric and genetic data processing must adhere to stringent conditions and only be used to contrast serious crime.[461] For instance, in cases, such as *Ministerstvo na vatreshnite raboti* (C-205/21)[462], the Court underscored that sensitive data like biometrics or telecommunications records, constitutes a serious interference with rights under Articles 7 and 8 of the Charter. Hence, these restrictions hinge on principles of necessity and proportionality, mandating that data processing should only serve clearly defined, serious criminal purposes. The CJEU has emphasised that retaining data indiscriminately or using data collected for minor crimes without prior authorisation, violates EU law.

Thus, with respect to the third condition, the "serious crimes" requirement, in *Tele2 Sverige,*[463] the Court specifically held that access to data must focus solely on combating serious crime, with judicial or independent oversight required. In Ministerstvo na vatreshnite raboti, the Court further emphasised this aspect.[464] Especially, AG Pitruzzella, in his opinion, stressed that

> "the collection and processing of biometric and genetic data, such as photographs, fingerprints and samples in order to create a DNA profile, in so far as they constitute a serious interference with the right to the protection of personal

[460] LED, Rec. 26. In choosing the instrument, the general interest should be achieved via the less restrictive means to not infringe upon the individuals' fundamental rights.

[461] Usually correlated by longer prison sentence, as in Mark Leiser and Bart Custers, 'Time Limits for Storage and Review' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[462] CJEU (Fifth Chamber), C-205/2021, V.S. v. Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost, 26 January 2023.

[463] CJEU (Grand Chamber), Joined C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016.

[464] Taner Kuru, 'C-205/21 VS v Ministerstvo Na Vatreshnite Raboti, Glavna Direktsia Za Borba s Organiziranata Prestapnost: Indiscriminate and Generalised Collection of Biometric and Genetic Data by Law Enforcement Authorities in the EU Is Not Allowed' (2024) 10 European Data Protection Law Review 223.

data, are permitted only where strictly necessary for the pursuit of objectives linked to serious crime, which national law must clearly identify".[465]

The CJEU has highlighted the principles of data minimisation and purpose limitation as essential safeguards under the LED, reinforcing the need for a precise legal framework to limit the use of such sensitive data to what is absolutely required for law enforcement purposes.[466]

However, recently, the CJEU partially subverted these precedents, not with referral to biometric data *per se*, but with respect to the accessing a mobile phone of an individual suspected of a crime. In Case C-548/2021,[467] the CJEU, while reaffirming that accessing the personal data on mobile devices in criminal investigations constitutes a serious interference with the rights guaranteed by Articles 7 and 8 of the Charter, it acknowledged that limiting data access strictly to serious crimes could hinder broader law enforcement needs. As a result, the Court supported the theory for accessing to mobile data in investigations of non-serious crimes, provided that it meets proportionality and necessity standards, as set per Art. 52 para. 1 of the Charter. This means that the legal framework governing such data access must be precise and clear. The purpose of this requirement is to ensure that citizens understand the limitations on their privacy rights and to prevent arbitrary access to data by authorities.

Opening the spectre of serious crimes might be critical since it can enlarge the already existing differences among national standards. Therefore, it is on the national law to identify the situations and the crimes that might represent a serious threat to the public interest and that can justify the interference in the privacy and data protection of individuals, by collecting sensitive personal data, like DNA or biometric data. Hence, national laws governing biometric data collection should ensure proportionality, limiting data collection to cases strictly necessary for serious crime prevention.[468]

[465] Id., C-205/21 (Opinion AG), *Ministerstvo na vatreshnite raboti*, 30 June 2022, §58. More recently, CJEU (Grand Chamber), C- 548/2021*, C.G. v Bezirkshauptmannschaft Landeck,* 4 October 2024, (espec., §90-91).
[466] Id., decision, §126.
[467] CJEU (Grand Chamber), *C.G. v Bezirkshauptmannschaft Landeck,* 4 October 2024, §97-99.
[468] C-118/2022, NG v Direktor na Glavna direktsia 'Natsionalna politsia' pri Ministerstvo na vatreshnite raboti, id.

While the CJEU's decision implements the LED and supports the need for flexible investigative tools, the risk lies in how these expanded rights are implemented across Member States. Effective protections must be embedded within national frameworks to avoid a slippery slope toward arbitrary data collection, which would erode public trust in law enforcement and infringe upon fundamental privacy rights. It is clear that the LED exposes limitations in ensuring that rights are genuinely protected, often struggling to counterbalance the expanding reach of surveillance in law enforcement, also due to the role of the MS and their autonomy in sensitive areas, like national security.

In the next section, this chapter will delve deeper into other approaches to the use of biometric data in the context of different law enforcement, to highlight how the protective pattern followed in this context is also followed in the creation of the Digital Identity Wallet.

3.4.3 Non-law enforcement use of biometric data: the case of the Digital Identity Wallet

Facial recognition and the use of biometric technologies are most perceived as threats to privacy and data protection.[469] However, the deployment of these technologies might also create deleterious effects on democracy and civil liberties, as mentioned *supra*. In between "commercial pressures of the data-driven surveillance economy, the security imperatives of law enforcement, and civic values of freedom of expression, movement, and personal autonomy"[470], biometrics might also represent a tool for faster bureaucracy and digitalise processes.

The rapid digitalisation of services that occurred in the aftermath of the COVID-19 pandemic,[471] driven by the need to provide vital services such as healthcare online, has led to an increased demand for digital credentials for identification and authentication purposes. This demand arises from both governments and businesses striving to adapt to digital service delivery models to better serve customers and citizens. In sectors like healthcare and finance, secure identification and authentication systems are crucial not

[469] Woodrow Hartzog et al., 'Privacy Nicks: How the Law Normalizes Surveillance', (2023) SSRN.
[470] Neil Selwyn and others, 'Facial Recognition Technology: Key Issues and Emerging Concerns' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).
[471] Id.

only to comply with legal mandates but also to ensure high levels of security and trustworthiness, particularly concerning data protection. For these reasons, the EU aims to amplify the use of digital identification methods via the review of the European Electronic Identification and Trust Services (eIDAS) Regulation of 2014.[472] Alongside the demand described above, there is a growing threat of online fraud, including identity theft, which poses significant challenges to cybersecurity and law enforcement efforts. Every MS had to adopt on a voluntary basis a scheme which is defined in the Regulation as a system for electronic identification under which electronic identification means are issued.[473] Hence, the shortcomings of the eIDAS Regulation mainly stem from limitations predominantly within the public sector, complexities faced by private providers in system connectivity, and inadequate availability of notified eID solutions across Member States.[474] In response to these challenges, a proposal has been put forth for a European Digital Identity framework aimed at ensuring that at least 80% of citizens can access key public services digitally by 2030.[475] This framework seeks to instil confidence in citizens by offering security and control over their digital identity, including the ability to manage access to their data, while fostering the need for a harmonised European approach to digital identity.

On the operational and technical aspects of such a project, the text resulting from the negotiations between the European Parliament and the Council of the European Union[476] provides that users are going to be identified through a "reference to a minimum set of person identification data necessary to uniquely represent a natural or legal person […]" (Art. 12, para 4)[477]. Saying it differently, since the data collection should not go further than a minimum set of data – otherwise, the user consents. Hence, the minimum threshold of the data set is composed of the first and the last names of a person, their date of birth

[472] Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (Eu) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final.

[473] For a comment on the Directive on AI liability refer to Finocchiaro G (2016) The European e-IDAS Regulation. Diritto Mercato e Tecnologia:5-19.

[474] European Parliament (2024) Briefing Updating the European digital identity framework; Explanatory Memorandum of the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (Eu) No 910/2014, id. note no. 41. Finocchiaro G, id.; Finocchiaro G (2022) Il contratto nell'era dell'Intelligenza Artificiale. Rivista Trimestrale di Diritto e Procedura Civile 2:441-460; Baldini D (2024) The Impact of the Right to Personal Data Protection on the Design of the European Digital Identity Wallet. Italian Journal of Public Law 16:297-317.

[475] Explanatory memorandum, id.

[476] When this article is written, the institutions have reached an agreement in the first reading.

[477] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

and a unique identifier, namely a number via which any individual would be able to uniquely and persistently be identified.

The cautious approach taken by EU institutions mirrors the design of the new identity framework, where the collection of biometric data is approached with careful consideration. In alignment with the GDPR's principle of data minimisation (Art. 5, para. 1, letter c), the EU legislator has opted to limit the collection of biometric data within the context of the new identity framework. Despite the undeniable potential of biometric data for unambiguous identification, this decision aims to prevent excessive and disproportionate intrusions into individuals' privacy spheres. Moreover, the regulation underscores the importance of maintaining a clear separation between personal data associated with the European Digital Identity Wallets and any other data held by service providers. This emphasis on data segregation serves to mitigate the risks of unauthorised access or misuse of personal information, as outlined in Rec. 12.

By establishing this framework, the EU aims to uphold the principles of data protection and privacy while facilitating the adoption of digital identity solutions. The incorporation of the principle of proportionality into both the AI Act and the European Digital Identity Regulation reflects the legacy of the Court of Justice of the European Union (CJEU).[478] This principle serves as a cornerstone of the 'Brussels effect,' balancing the costs and benefits of technology deployment while safeguarding fundamental rights.[479] By striking a balance between data privacy and societal imperatives, such as national security and law enforcement, the EU continues to assert its leadership in shaping global standards for digital governance. By embedding principles of proportionality and data minimisation into its regulatory frameworks, the EU seeks to build trust among citizens and stakeholders while navigating the complexities of the digital age.

This general precautionary approach to the processing of biometric data was, among other things, also recently reaffirmed by the CJEU,[480] which ruled that the obligation to

[478] Defined by Art. 3 no. 42 as "an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals".

[479] Bradford A (2023), note no. 20:113. Art. 52, Charter of Fundamental Rights of the European Union. For a comment, Kindt EJ (2013) The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing. In: Kindt EJ (ed) Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Springer Netherlands, Dordrecht, pp 403–567.

[480] CJEU (GC), *RU v Landeshauptstadt Wiesbaden*, no. C-61/2022, 21 March 2024.

insert fingerprints in identity cards does not constitute a restriction to the exercise of fundamental rights to respect for private life and protection of personal data, which the Charter of Fundamental Rights guarantees. Nevertheless, the Court confirmed that such restriction is justified by the objectives of the general interest of combatting the production of false identity cards.[481] Therefore, in this case, the interference with fundamental rights resulting from the inclusion of two fingerprints in the storage medium of identity cards did not appear to be "of a seriousness which is disproportionate when compared with the significance of the various objectives pursued by that measure" (§123). The purpose of uniquely identifying a natural person, particularly in cross-border situations, has been deemed to be a "fair balance" (id.) with the fundamental rights involved. Hence, the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter (§81).

The discourse on biometric technologies and digital identification in the EU highlights the balance between privacy, data protection, societal needs, and technological advancement. Despite concerns, these technologies promise streamlined bureaucracy and better digital services. The proposed European Digital Identity framework aims to improve access to public services while ensuring data security and privacy, reflecting the EU's commitment to unified digital governance. Regulatory provisions, like cautious biometric data collection, demonstrate a balanced approach between innovation and rights protection. However, ensuring this balance throughout the technology's lifecycle remains challenging, with less attention given to operational and enforcement phases.

In the next section, this chapter will delve into how the described regulatory principles apply to facial recognition technology under the AI Act, particularly examining the challenges of aligning AI applications with GDPR principles in law enforcement and beyond.

[481] Nonetheless, the Court affirmed that Regulation (EU) 2019/1157 in question was adopted on an incorrect legal basis.

3.5 The regulation of FRT in the AI Act

The European Commission's proposal of the AI Act in April 2021[482] already contained dedicated provisions on biometric recognition systems, which have stood out for their representativeness.[483] Particularly, as stated by Rec. 3, "this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions on the use of AI systems for remote biometric identification for the purpose of law enforcement"; for this reason, together with art. 114 TFEU, the legal basis of the Regulation is precisely art. 16 of the TFEU, which pertains to the protection of personal data and privacy in the European Union.

Therefore, the chief, among other aspects, is the coordination of the new AI regulatory frame with the existing rules, especially the one on personal data: while providing that the rules in question must "continue to comply with all requirements resulting from art. 9(1) of GDPR, art. 10(1) of Regulation (EU) 2018/1725[484] and art. 10 of Directive (EU) 2016/680 (also, LED), as applicable",[485] the AI Act is strictly mandating the conditions upon which FRT can be placed in the market and put into service.

As anticipated in Chapter 2, the AI Act is primarily a product safety regulation, meaning that its main focus is on ensuring that AI systems deployed within the European Union meet specific safety and technical standards.[486] As a horizontal regulation, it establishes general principles that apply across various industries and sectors, with an emphasis on the design, development, and deployment of AI technologies.[487] However, there is a notable exception when it comes to certain AI applications, particularly the use of AI in specific sectors, where the focus shifts from regulating the AI system itself to

[482] 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts', Brussels, 21.4.2021 COM (2021)

[483] Bilgesu Sumer and others, 'AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data' in Kostina Prifti and others (eds), *Digital Governance: Confronting the Challenges Posed by Artificial Intelligence* (TMC Asser Press 2024).

[484] 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.

[485] AI Act, Rec. 39.

[486] Marco Almada, 'Regulation by Design and the Governance of Technological Futures' (2023) 14 European Journal of Risk Regulation 697; Gallese Nobile (n 317).

[487] Johann Laux, Sandra Wachter and Brent Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk' (2024) 18 Regulation & Governance 3.

regulating its actual use. One of the clearest examples of this is the regulation of biometric technologies,[488], particularly in the case of real-time remote biometric identification systems used in publicly accessible spaces for law enforcement purposes.[489]

A biometric system, which, according to a dated but accurate definition is "the science of automatic identification or identity verification of individuals using [unique] physiological or behavioral characteristics",[490] triggers many fundamental rights,[491] especially privacy, data protection, and civil liberties,[492] and for this reason, the AI Act does not merely regulate the technical characteristics of these AI systems but also imposes strict conditions on how and when they can be used.[493]

Moreover, the rules hereby established are true *lex specialis* concerning data protection and law enforcement frameworks. This means that they take precedence over general data protection laws in situations where specific risky AI applications, such as biometric identification, are concerned.[494] Specifically, Recital 38 of the AI Act makes it clear that the regulation's provisions, which prohibit certain uses of AI technologies like real-time biometric identification systems in publicly accessible spaces, should be understood as a more specialized set of rules derived from Article 16 TFEU.[495] These rules are meant to

[488] Menéndez González (n 61).
[489] van Schendel (n 148).
[490] John R Vacca, *Biometric Technologies and Verification Systems* (2007) <https://shop.elsevier.com/books/biometric-technologies-and-verification-systems/vacca/978-0-7506-7967-1> accessed 3 December 2024.
[491] Paul De Hert and Georgios Bouchagiar, 'European Biometric Surveillance, Concrete Rules, and Uniform Enforcement: Beyond Regulatory Abstraction and Local Enforcement' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024); Menéndez González (n 61); Giuseppe Mobilio, 'L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?' (ITA 2023).
[492] Margaret Hu, 'Biometric Surveillance and Big Data Governance', *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017); Kindt, 'The Risks Involved upon the Use of Biometric Data and Biometric Systems' (n 59).
[493] AI Act, Rec. 32, "the use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights".
[494] This classification ensures that the AI Act comprehensively governs both the use and processing of biometric data for law enforcement purposes, addressing the specific risks associated with these technologies in an exhaustive manner. By applying the principle of *lex specialis*, the Act ensures that the stricter rules it sets forth override more general provisions found in broader data protection laws. Consequently, when conflicts arise between the AI Act and other legal instruments on data protection, the AI Act's rules prevail, ensuring a more targeted regulatory approach to biometric surveillance and its potential impacts on privacy and civil liberties.
[495] AI Act, Rec. 3.

apply as *lex specialis* in relation to the data protection standards established in the GDPR and in Article 10 of Directive (EU) 2016/680.[496]

In the following sections, the regulatory framework for FRT under the AI Act will be analyzed in detail, focusing on its specific applications in law enforcement. This includes an in-depth exploration of real-time and post-remote biometric identification systems, as well as related AI-driven technologies such as predictive policing, emotion recognition, and biometric categorization. Each of these applications will be examined with respect to the safeguards, exceptions, and challenges outlined in the AI Act, highlighting their implications for fundamental rights, privacy, and democratic freedoms.

3.5.1 The AI Act lex specialis

As anticipated, the AI Act introduces strict rules for the use of real-time remote biometric identification (RBI) systems in publicly accessible spaces for law enforcement purposes, recognising the intrusive nature of such technologies and their potential to impact fundamental rights. These rules aim at balancing public safety with safeguarding individual freedoms.

Under Article 5 (1), lett. h) of the AI Act, the use of real-time RBI systems is generally prohibited, with exceptions only in narrowly defined circumstances.[497] These include the targeted search for victims of abduction, trafficking, or sexual exploitation, as well as the search for missing persons. Additionally, the use of such systems may be permitted to prevent specific, substantial, and imminent threats to life or physical safety, such as

[496] 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.

[497] AI Act, Art. 5, para. 1, lett. h), point i)-iii), "(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement".

terrorist attacks, or to locate or identify individuals suspected of committing serious criminal offenses, provided these crimes fall under Annex II of the AI Act and carry a custodial sentence or detention of at least four years in the MS. However, even when these exceptions apply, the deployment of real-time RBI systems is subject to stringent safeguards. These exceptions allow real-time biometric identification by law enforcement authorities only in cases that serve significant public interests, such as preventing imminent threats to life, investigating serious criminal offences, or responding to terrorist attacks.[498]

Law enforcement, when deploying RBI, must conduct a fundamental rights impact assessment (FRIA),[499] as mentioned in Rec. 34, to evaluate the potential effects on privacy, non-discrimination, and other rights: proohibited systems present unique challenges due to their intrinsic risks to fundamental rights and the AI Act is simply silent, besides Rec. 34 which establishes:

> "The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a fundamental rights impact assessment [..]."

Although Rec. 34 of the AI Act establishes that the use of real-time remote biometric identification systems in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a FRIA, the concrete implementation of this requirement remains ambiguous, especially with respect to the application of the other provisions for 'high risk system' to the prohibited ones.[500] Only in the 'Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)', published in February 2025, the Commission clarified that "most AI systems that fall under an exception from a prohibition listed in Article 5 AI Act will qualify as high-risk".[501] Therefore, the obligations for high risk systems shall apply also to the exceptions for RBI in law enforcement.

Finally, para. 3 of Art. 5 provides a crucial obligation which is going to be examined later on: judicial or independent administrative authorisation is mandatory for each use,

[498] AI Act, Art. 5 and Annex II.
[499] AI Act, Art. 27. See Chapter 4 *infra.*
[500] See Chapter 2, §2.4.9 and §2.4.10.
[501] Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), id, §37.

based on a reasoned request that demonstrates necessity and proportionality. Basically, the choice is left to the MS to determine whether a judicial or administrative authority should be recognized with the power to authorise the use of such systems.[502] These authorisations must also account for geographic, temporal, and personal limitations to ensure minimal interference with fundamental rights.

Beyond the rules for real-time RBI systems, the AI Act addresses the broader use of biometrics in law enforcement, particularly in the form of post-remote biometric identification systems. These systems differ from real-time systems in that they analyse biometric data after the fact, rather than in real time. In contrast, ex-post biometric identification systems – which are used *post factum* for identification purposes – are classified as high-risk AI systems under Article 6, paragraph 2 of the AI Act.[503] This classification also extends to other sensitive biometric technologies, such as biometric categorisation systems and emotional recognition systems, which are considered high-risk due to their potential to infringe on fundamental rights. Like real-time systems, deployers of high-risk post-remote biometric systems should require prior authorisation from judicial or independent administrative authorities, with the necessity and proportionality of their deployment rigorously scrutinised.[504] However, concerns remain about the potential for inconsistency across Member States due to divergent national practices and voids in regulation, as highlighted *infra.*

Furthermore, the AI Act contains also specific provisions on other two types of AI systems that might or are trained with biometric data: i) emotion recognition; ii) biometric categorisation.

---

[502] As clarified by the European Commission in the Annex to Art. 5 (*supra*), "National laws are required for operationalising the use of 'real-time' RBI systems in publicly accessible spaces for the purposes of law enforcement. At the same time, Article 5(5) AI Act provides that Member States remain free to decide whether to adopt such national laws. If a national law authorising the use of real-time RBI is adopted, the AI Act specifies the substantive elements which the national laws must contain to comply with the requirements laid down in the AI Act", §412.

[503] The distinction between the real-time and ex-post application of biometric recognition is futile from a fundamental rights perspective. The difference is purely technical and consists of two different moments of the identification process, but it entails the same consequences for the surveillance of citizens. Particularly, the biometric system is mostly the same, trained with a biometric data set, and it is used in two modalities: e.g., live while the crime is happening or after *ex-post.* See 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, 2021.

[504] AI Act, Art. 26. See §2.4.5.

Emotion recognition systems are deployed "for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data"[505] and they aim to infer emotional states from facial expressions, voice patterns, or physiological signals. However, these systems often rely on scientifically debatable assumptions and have been criticised for their inaccuracy and potential misuse.[506] For instance, the misinterpretation of emotional states could lead to wrongful accusations or discriminatory practices in law enforcement contexts. However, the AI Act classify as prohibited uses of emotion recognition only the specific sectors of "workplace and education institutions", as per Art. 5, para. 1, lett. f). All the other uses of emotion recognition are, therefore, permitted under the AI Act, included the law enforcement ones.[507]

Similarly, biometric categorisation systems, which classify individuals based on physical or behavioral traits, such as ethnicity, gender, or age, raising significant risks of stereotyping and reinforcing societal biases,[508] have a double classification under the AI Act. Article 5, para. 1, lett. g) includes in the high-risk list biometric categorisation systems[509] when they categorise individuals "based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation".[510] It is excluded from the prohibition of the use of such systems in the context of law enforcement. Instead, biometric categorisation systems that are based on inferred characteristics, such as age, gender, or ethnicity[511] are classified as high risk, according to Art. 6, para. 2, and Annex III, Art. 1, lett. b). No further specification on the differences between the two uses is provided, nor it is specified a particular procedure for the use under Art. 5 in the context of law enforcement. While the AI Act requires transparency requirements and communication to the users, under Article

[505] AI Act, Art. 3, para. 1, n. 39.

[506] Francesco Paolo Levantino, '"How Do You Feel Today?" Exploring IHRL and IHL Perspectives on Law Enforcement and Military Uses of Emotion Recognition Technology' (*Opinio Juris*, 15 November 2023) <https://opiniojuris.org/2023/11/15/how-do-you-feel-today-exploring-ihrl-and-ihl-perspectives-on-law-enforcement-and-military-uses-of-emotion-recognition-technology/> accessed 8 January 2025.

[507] AI Act, Rec. 54, "emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk."

[508] Studies have shown higher error rates for minority groups in facial recognition systems, further exacerbating concerns about equality and non-discrimination. Tambiama Madiega and Hendrik Mildebrath, 'Regulating Facial Recognition in the EU' (EPRS | European Parliamentary Research Service 2021).

[509] Defined by Art. 3, para. 1, no. 40, as "an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons".

[510] AI Act, Article 5, para. 1, lett. g.

[511] AI Act, Rec. 16.

50 (3), for both emotion recognition and biometric categorisation systems, their deployment in law enforcement contexts demands heightened scrutiny to ensure compliance with GDPR and Directive (EU) 2016/680.

Whereas a category is completely excluded from the Regulation: predictive policing systems. Such systems can be used to analyse historical crime data to predict future criminal activity or allocate law enforcement resources.[512] While predictive policing aims to enhance efficiency and crime prevention, it introduces significant risks, particularly in its potential to amplify discrimination and bias. Historical datasets often reflect systemic inequalities, disproportionately targeting marginalized communities, as seen in projects like the Netherlands' "Sensing Project," which raised concerns about over-policing and biased risk assessments, or the wide famous COMPAS case.[513] Failing to recognize the specific risks of these systems, the AI Act opens the floor for opaque application of Art. 5 and the Regulation in a very sensitive sector.

Finally, biometric verification systems are explicitly excluded from certain restrictive provisions under the AI Act, as noted in Recital 54. These systems, which confirm an individual's identity for specific authorised purposes, are typically used in contexts like secure access or identity verification and rely on active participation from the individual being verified. The Regulation recognises that verification systems present relatively low privacy risks compared to identification systems, which process biometric data on a larger, potentially unsolicited scale, and, therefore, are not interested by the regulation.

The following grid provides a comprehensive overview of the regulatory framework for biometric and AI systems under the AI Act, with a specific focus on their permissibility in law enforcement contexts. It categorises these systems based on their risk level, key legal provisions, and the conditions under which they may be deployed. This structured analysis highlights the varying degrees of regulation, from outright prohibitions to high-risk classifications, and emphasizes the safeguards necessary to ensure compliance with fundamental rights, such as privacy and non-discrimination. The grid also clarifies how

[512] Dirty Data, 'Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice'(Vol' 94 New York University Law Review 2019; Orla Lynskey, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 International Journal of Law in Context 162.

[513] Sascha van Schendel, 'The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI' in Leonie Reins (ed), *Regulating new technologies in uncertain times* (TMC Asser Press | Springer 2019).

the AI Act distinguishes between permitted, restricted, and unregulated uses of these technologies in law enforcement.

Table 4 – AI Act's *lex specialis* on biometric systems.

Biometric systems	AI Act article	Risk level	Key provision	Use in laaw enforcement
Real time biometric systems (RBI)	Article 5(1)(h)	Prohibited	Allowed only for victim searches, imminent threats, or serious crimes (Annex II). Requires FRIA, judicial/administrative authorisation, and EU database registration.	Yes, with strict conditions
Post-remote biometric systems	Art. 6; Annex III, (1)(a)	High-risk	No limitation to "serious crimes." Requires FRIA and prior authorization from judicial/administrative authorities.	Yes, with conditions
Emotion recognition systems	Article 5(1)(f); Annex III, (1)(c)	Prohibited; High risk.	Prohibited in workplace and education contexts. Permitted in law enforcement under general safeguards, including FRIA, transparency (Article 50), and GDPR compliance.	Yes, with conditions
Biometric categorisation systems	Article 5(1)(g); Annex III, (1)(b)	Prohibited; High risk.	Prohibited for deducing sensitive traits (e.g., race, religion) except in law enforcement. High-risk uses (e.g., age or ethnicity	Yes, with conditions

			categorisation) allowed under strict safeguards, including FRIA and GDPR compliance.	
Predictive policing systems	Excluded	Unregulated	Not addressed by the AI Act, leaving a significant regulatory gap despite systemic risks of discrimination and opacity.	Not covered.
Biometric verification systems	Excluded	Excluded	Excluded	Not covered.

All these systems amplify surveillance capabilities, raising concerns about privacy, data protection, and the chilling effect on democratic freedoms. The principles of data minimisation and purpose limitation under GDPR are challenged by the large-scale data collection required by these systems, while algorithmic biases risk perpetuating structural inequalities. Algorithmic biases further risk perpetuating structural inequalities, and the lack of transparency in deploying these systems can deter individuals from engaging in lawful but unconventional or controversial activities due to fear of being monitored. The cumulative effect of these technologies underscores the urgent need for robust regulatory safeguards and vigilant oversight.

3.5.2 Issues and de iure condito *perspectives*

Many complexities remain. Fundamental critiques of the AI Act's approach to biometrics are to be found in three crucial clusters: i) the proposed risk classification, ii) the risk categorisation; iii) proportionality and accountability.

An additional layer of complexity in the AI Act lies in its unclear delineation of obligations for high-risk versus prohibited practices. First, the Act's distinction between 'remote' and 'real-time' biometric identification systems (Articles 3, paras 36 and 37) has

been critiqued for creating confusion rather than clarity. [514] As well recalled by the EDPB, there is just one type of technology with different functions, not the opposite.[515] This aspect is crucial when attempting to draw a line between uses that fall into the recognition, identification, categorisation and verification since they are allowed for different purposes while being the same type of technology. Saying it differently, the technology's core capabilities remain consistent across these functions, but the regulatory framework treats each as if they are distinct, which can lead to ambiguity and potentially inconsistent enforcement. For instance, in one context, FRT may be used for *identification* in real-time public surveillance (generally prohibited under the AI Act except in narrowly defined cases), while in another, it may be used for *verification* in access control systems, such as airport boarding gates, where it is more permissible. Although both functions involve processing facial data, the purposes and permissible contexts differ. Whilst high-risk AI uses are receivers of detailed obligations, the Regulation does not explicitly state whether these stringent obligations apply to those practices the Act outright prohibits, adding ambiguity for deployers navigating compliance requirements.

The core of this critique lies in the fact that these distinctions – between functions like recognition, identification, categorisation, and verification – are treated as if they involve different technologies despite all being variations of the same biometric process. The regulatory framework of the Regulations treats each function distinctly, despite their reliance on the same underlying technology, potentially leading to inconsistencies in enforcement. For instance, FRT used for real-time public surveillance is generally prohibited under the AI Act, except in narrowly defined cases. Yet, the same technology might be permissible when used for verification purposes, such as at airport boarding gates, where it serves an access control function. The technology remains fundamentally the same in both scenarios, involving the processing of facial data, but the Act's regulatory distinctions hinge on context and intent, which can create interpretative challenges.

Furthermore, the AI Act delegates the responsibility of classification – determining whether a system is remote or real-time – to the deployer, relying heavily on self-assessment mechanisms. This approach, while intended to be flexible, has been critiqued by scholars and policymakers for its risks. As noted in Chapter 2, a heavy reliance on self-

[514] Michal Veale and Frederik Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act', Computer Law Review International 4:97–112.
[515] EDPB, (2022) id.

assessment may undermine compliance and enforcement, especially where oversight of AI applications, particularly FRT, is limited. The absence of external checks or standardised classification processes raises concerns about consistency, as deployers could misclassify technologies either unintentionally or to sidestep stricter regulatory obligations. [516]

A last point on this first cluster is that, as briefly anticipated above, post-remote biometric systems do not specify that deployment must relate to "serious crimes". As outlined in the very title of Annex II, the list of serious crimes suffices only for RBI uses, therefore, falling within Art. 5 "Article 5(1), First Subparagraph, Point (h)(iii)". This lack of specificity introduces a regulatory gap, leaving the application of these systems less clearly constrained, despite their significant potential for privacy infringements. This absence of detailed guidance highlights a broader critique of the AI Act's risk-based approach, which struggles to provide clarity on when biometric systems transition from high-risk to unacceptable-risk classifications.

Moving on the analysis of the second cluster, the AI Act lacks a precise definition of when AI poses unacceptable risks; instead, it categorises risk based on specific applications. Additionally, any expansion of the scope of prohibited uses under Article 5 would necessitate an amendment to the Act, as the current Regulation does not specify criteria for determining when AI systems present unacceptable risks to society and individuals; it merely establishes a presumption of risk. This means that extending the scope of Article 5 beyond the currently listed prohibited uses would require formal legislative changes to the Act.[517] Notably, the final articles dedicated to this aspect underscore the significant role of the European Commission in conducting bi-annual assessments in collaboration with the AI Board, as per Article 66(1)(e)(vii).[518] Although the mechanism was already provided for in the GDPR,[519] with the AI Act, it would broaden the scope of the Commission's action to also include the assessment of the material application of the standard with respect to high-risk profiles and annexes-aspects that are outside the certifying mechanisms in the GDPR.

[516] Smuha and Yeung (n 151); Wachter (n 244).
[517] Lillian Edward, 'Expert opinion: Regulating AI in Europe', (2022) Ada Lovelace Institute https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/. Accessed 3 December 2024.
[518] CJEU (GC), European Parliament and European Commission v Council of the European Union, Joined Cases C-124 and 125/13, 1 December 2015, §73.
[519] Rec. 166 of the AI Act.

A third fundamental critique of the AI Act's approach to regulating FRT lies in its limited requirement for empirical justification of necessity and proportionality in law enforcement contexts. For any use of FRT to be deemed necessary and proportionate under EU law, especially given its impact on privacy and autonomy, there should be robust evidence demonstrating that FRT is not only effective but is also the least intrusive means of achieving specific public security goals.[520] The principle of empirical justification demands that FRT, particularly in high-stakes applications like real-time surveillance, should be substantiated by clear, evidence-based outcomes showing that it performs better than alternative, less intrusive methods of crime prevention and law enforcement. However, the AI Act currently does not mandate that law enforcement agencies provide empirical data validating FRT's superior efficacy or unique capability. Critics argue that this lack of empirical requirements risks allowing FRT deployment in public spaces even when its effectiveness, necessity, and proportionality have not been adequately proven.[521]

Finally, in terms of accountability, it should also be noted that, as mentioned, Article 66 of the AI Act provides for bi-annual assessments, where the European Commission, in collaboration with the AI Board, is expected to review high-risk AI applications, including FRT, to ensure ongoing compliance and evaluate risks. However, this assessment process is not specifically required to include real-time empirical data on FRT's operational effectiveness. To strengthen accountability, the AI Act could specify that law enforcement agencies deploying FRT must submit regular performance reports, including data on accuracy, error rates, and effectiveness relative to public security outcomes. Another potential enhancement to accountability could involve mandating that independent bodies review FRT's deployment. For example, national data protection authorities or designated AI oversight committees could conduct audits on the real-world impacts of FRT, focusing on whether the technology effectively serves its purpose without unnecessary rights infringements. Such bodies would not only monitor compliance with

[520] "This means that the necessity to process data must be examined in the context of the relevant law enforcement task, with due attention to be paid to the objectives of such processing and the personal data to be processed", Maria Tzanou, 'Article 8 LED. Lawfulness of Processing' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enfocemente Directive (LED): a commentary* (Oxford University Press 2024).

[521] Catherine Jasserand, 'The Future AI Act and Facial Recognition Technologies in Public Spaces: Nice to Have or Strictly Necessary?' (Social Science Research Network, 15 December 2023) <https://papers.ssrn.com/abstract=4947432> accessed 3 December 2024.

the AI Act's high-risk criteria but also assess whether FRT continues to meet proportionality standards based on empirical data.[522] Another point to further potentiate the trust in this technology would be including mechanisms for citizen feedback that could enhance accountability by integrating public opinion into FRT's ongoing evaluation.[523] Public consultations or surveys on the perceived impact of FRT on community safety and privacy could inform assessments of its necessity and proportionality. This approach would give citizens a voice in shaping how invasive technologies like FRT are governed, adding an empirical, participatory dimension to accountability.

These three clusters of analysis represent only an initial framework; further challenges in protecting fundamental rights will be examined in the following chapters. Before moving on to assess the AI Act's compliance with fundamental rights in its framework for FRT, it is essential to clarify the complex regulatory landscape underlying these technologies. Following the discussion of the AI Act's specific provisions, this analysis will extend to the broader legal framework, with a comparative look at the GDPR and LED. Thus, from the preceding sections on the use of biometric data, a key necessity emerged: establishing a more systematic and structured regulatory framework for FRT.

3.6 Toward a comprehensive legal framework for FRT

The purpose of this chapter has been to underline the main conditions and regulatory requirements necessary for deploying technologies such as facial recognition in a way that aligns with fundamental rights and safeguards public trust. Nonetheless, as discussed, the deployment of FRT in law enforcement within the EU is governed by a multi-layered regulatory framework that balances the benefits of biometric surveillance with the protection of privacy and fundamental rights.[524]

[522] Wachter (n 244).

[523] This aspect is nuanced in Art. 27 of the AI Act, on the Fundamental Rights Impact Assessment (see next Chapter), where it is established that the deployer should take into consideration the categories of natural persons that might be affected by the AI system. This provision should be read together with Rec. 96 which establishes that the deployers in performing the assessment could also involve relevant stakeholders, including civil society organisations, in order to design the most correct measures to protect fundamental rights.

[524] For a comparison of the GDPR and the LED requirements only, see Joanna Mazur and Zuzanna Choińska, 'Chapter 7: European Union Data Protection Law and the Use of Facial Recognition Technology for the Purpose of Fighting Crime' (2024).

Each of these instruments imposes distinct but complementary obligations on controllers using FRT. The GDPR focuses on broad data protection principles, particularly relevant to the processing of special categories of personal data, *supra.* It sets foundational requirements for data minimisation, transparency, and the implementation of DPIAs in cases where biometric data is used. The LED, on the other hand, caters specifically to the law enforcement context, allowing for some flexibility while ensuring that biometric data processing aligns with the principles of necessity and proportionality, especially when it concerns public safety and crime prevention. Finally, the AI Act adds another regulatory layer by specifically categorising certain AI-driven systems as prohibited or high-risk and requiring compliance with strict standards in areas such as accountability, oversight, and bias mitigation.

Together, these frameworks create a comprehensive regulatory landscape for FRT. However, academic and policy discussions often analyze these frameworks in isolation, ignoring their interconnections and overlaps. This final section seeks to take a holistic perspective, highlighting the intersections and tensions within the regulatory framework.

By imposing these layered compliance requirements and legal safeguards, the EU aims to mitigate the risks of privacy infringements, algorithmic bias, and potential misuse associated with FRT, ensuring that the deployment of such technologies aligns with democratic values and fundamental rights protections. However, the fragmented nature of these regulatory frameworks leaves significant interpretive burdens on practitioners and authorities tasked with navigating their intersections. While this comprehensive approach underscores the EU's commitment to fostering responsible innovation in AI, it also reveals the urgent need to clarify the relationship between these overlapping systems of regulation. De *iure condito*, the following paragraphs will explore the obligations under the current legal framework to identify potential redundancies and gaps that may compromise the protection of individuals' rights. This effort aims to bring coherence to the complexity of FRT regulation while maintaining robust safeguards for fundamental rights.[525]

[525] See for a thorough analysis Mobilio, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative* (n 61).

3.6.1 The GDPR framework

As anticipated *supra*, given the sensitivity of biometric data used in FRT, controllers must establish a lawful basis for processing,[526] as biometric data is categorised as "special category" data under Article 9 of the GDPR, as mentioned above. Generally, the processing of such data requires explicit consent from the individual or must be deemed necessary for reasons of substantial public interest. The requirement for informed consent is integral to safeguarding individual autonomy and ensuring that FRT does not infringe on data protection without proper justification.[527] Regulators emphasise that consent must be explicit, informed, and revocable, empowering individuals to opt-out or withdraw from FRT use.[528] However, challenges remain, as achieving truly informed consent in mass surveillance settings, i.e., where facial recognition operates continuously and collecting data of broad groups of people, is complex. Transparency mechanisms, including clearly displayed information and accessible policies detailing FRT operations, are crucial in bridging this gap. As a matter of fact, in these situations, or when the consent cannot be given truly freely, the law is clear that another legal basis is to be found.[529]

---

[526] Consistent case law on the fundamental right to respect for private life, see CJEU Case C-73/07 para. 56 (Satakunnan Markkinapörssi and Satamedia); CJEU, Cases C-92/09 and C-93/09 para. 77 (Schecke and Eifert); CJEU - C-594/12, para. 52 (Digital Rights); CJEU Case C-362/14 para. 92 (Schrems).

[527] GDPR, Article 9 para. 2, states that processing is lawful a) for the purpose of fulfilling obligations or exercising rights in the field of employment and social security; b) where it is necessary to protect a vital interest where it is not possible to give consent; c) for the purpose of legitimate activities of foundations, associations or other non-profit bodies; d) where the particular personal data are manifestly made public by the data subject; e) for the performance of defence and investigation activities; f) for a substantial public interest in the field of public health; g) for archiving purposes in the public interest, scientific or historical research or statistical purposes; h) subject to possible derogations and adaptations introduced by Member States.

[528] Informed consent means that individuals must not only be aware that their biometric data is being collected and processed but also understand the purposes, potential consequences, and parties involved in data handling. This principle is particularly essential in contexts where FRT systems operate covertly, such as public spaces, and where individuals may not explicitly agree to or even realize the extent of surveillance to which they are subjected. Bygrave and Tosoni (n 69); Els J Kindt, 'A Legal Model for the Use of Biometric Data in the Private Sector' in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013); Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[529] This is the case of Tribunal administratif de Marseille, 2020, n. 1901249, *supra* (no. 5) but also of the Italian DPA, Decision no. 5/2024, 11 January 2024, doc. no. 9977020, against the municipality of Trento that started to deploy biometric recognition systems. In particular, the Marvel project ('Multimodal Extreme Scale Data Analytics for Smart Cities Environments') provided for the acquisition of footage from video surveillance cameras already installed in the municipality for urban security purposes, as well as audio obtained from microphones specifically placed on public streets. The data, which according to the municipality would be immediately anonymised after collection, would be analysed to automatically detect public safety risk events using artificial intelligence techniques. On the other hand, the Protector project

This is the case, for instance, of the use of biometric data in the context of law enforcement, but also in the workplace and schools, especially involving the collection of minors' data. The rationale is to protect the 'weak' side of the relationship that, in a subjection position, might not be fully free in giving consent.

On this line, another critical GDPR requirement for controllers using FRT is conducting a DPIA under Art. 35 GDPR, as mentioned previously. The DPIA is a structured risk assessment aimed at identifying and mitigating potential impacts on data subjects' rights and freedoms before processing begins.[530] For FRT, the DPIA must detail the purposes of data collection, assess whether less intrusive methods could achieve the same objective, and document safeguards implemented to protect data subjects' privacy. Key considerations for FRT-specific DPIAs include transparency, data minimization, security measures, and the strict limitation of data retention periods to what is necessary for law enforcement's goals.

Finally, individuals subjected to FRT have specific rights concerning their data. These rights include the ability to access their personal data collected by FRT systems, correct any inaccuracies, and object to the processing of their data if it infringes upon their privacy.[531] Data access rights empower individuals to remain informed about the extent of FRT's impact on their personal information, while correction rights ensure that inaccuracies do not lead to false identification or discrimination. The right to object is particularly significant, as it grants individuals control over their data in situations where FRT could affect their personal freedoms or subject them to unwarranted surveillance.

('PROTECTing places of wORship') provided, in addition to the acquisition of video surveillance footage (without an audio signal), for the collection and analysis of hate messages and comments posted on social networks, detecting any negative emotions and processing information of interest to the police, in order to identify risks and threats to the security of places of worship. After an in-depth investigation, the Garante found multiple violations of privacy legislation. The data controller, the municipality of Trento, did not prove the existence of any legal framework justifying the processing of personal data – also relating to crimes and special categories of data – and the consequent interference with people's fundamental rights and freedoms. Given that the data were also shared with third parties, including project partners, the processing carried out was therefore deemed unlawful. In addition, the anonymisation techniques used to reduce the possible risks of re-identification for data subjects proved to be insufficient. Criticisms also emerged in terms of transparency, since the municipality had not fully described the processing operations in the first and second-level disclosures, such as the possibility that conversations could also be recorded by microphones installed on the public street.

[530] Marit Hansen, 'Data Protection Impact Assessment' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024). See also EDPB, Guidelines 05/2022, id.

[531] GDPR, Art. 5, 11-22.

Through these rights, individuals can exercise a degree of autonomy over their interactions with FRT, reinforcing privacy protections.[532]

3.6.2 The LED framework

The LED builds on GDPR's foundational principles but is specifically tailored to law enforcement's unique requirements in the prevention, investigation, and prosecution of criminal activities. It applies where the GDPR does not fully address law enforcement contexts and focuses on ensuring that data processing is "strictly necessary" for fulfilling specific law enforcement purposes. Under the LED, controllers must demonstrate that any FRT deployment meets necessity and proportionality standards, limiting processing to cases involving serious crimes or significant public safety threats, as seen above. This limitation is crucial as it aims to prevent excessive surveillance that could infringe on individuals' privacy rights without adequate justification.

An effective legislative framework not only defines lawful applications but also imposes requirements for regular assessments of FRT's societal impact. Regulatory bodies should mandate audits and impact assessments that address potential biases, the efficacy of FRT, and its long-term implications on privacy and data security. Through these assessments, legislators can ensure that FRT operates within an adaptable legal structure, responsive to evolving privacy standards and technological advancements. The LED mandates that controllers conduct a DPIA, under Art. 27, similar to GDPR requirements, but with additional considerations unique to law enforcement.[533] The DPIA under the LED must justify the relevance of using FRT over less invasive tools and assess whether the technology's deployment could lead to discrimination or breaches of fundamental rights.[534] In practical terms, this means evaluating FRT's potential to misidentify or unfairly target certain demographic groups. This assessment must address biases in the FRT system itself, considering that many facial recognition algorithms

[532] See, Italian DPA, Decision no. 5/2024, 11 January 2024.
[533] See the IMY sanction to the Swedish Police, id. *supra.*
[534] LED, Rec. 58 "a data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases".

exhibit varying levels of accuracy across different population groups. The LED further requires that processing be limited strictly to the initial purpose for which the biometric data was collected;[535] data collected in one investigation, for instance, cannot be repurposed for another without establishing a separate legal basis, which reinforces the purpose limitation principle. Moreover, the DPIA should be conducted prior to the processing, since it "functions as a provident and precautionary instrument so that the controller becomes aware of the consequences of the processing beforehand and can decide on adequate risk-mitigating measures or, if this does not yield sufficient results for risk mitigation, to forge the planned processing".[536] Additionally, the results of the DPIA should be communicated to the 'supervisory authority', as per Art. 28. For example, if FRT is used in real-time to monitor a public space, the LED would require that controllers obtain prior authorization, particularly if such processing could have significant implications for individuals' rights, such as the freedom to assemble or move freely without surveillance.

Ultimately, the LED details the rights of the data subjects[537], that recall the GDPR framework. In particular, under Art. 13 of the LED, data subjects must be informed about the processing of their biometric data when FRT is used, especially in public spaces. This involves providing clear, accessible information about the purpose of data collection, the types of data collected, and the duration for which data will be stored. Information must also be provided on individuals' rights and the means to exercise them. In instances where notifying each individual is impractical, alternative public notices, such as signage, may be used to communicate the existence of FRT systems.[538] Secondly, data subjects have the right to access their personal data processed by FRT systems, as per Art. 14 LED. This right allows individuals to verify what biometric data has been collected and for what purpose, enabling them to evaluate how their personal data is managed. Access rights include the ability to obtain copies of data collected, along with information on the source,

[535] EDPB, Guidelines 5/2022, id.
[536] Hansen (n 530).
[537] LED, Art. 12-18. A complete analysis is to be found in the recalled EDPB, 05/2022 Guidelines.
[538][538] Ex multis, CJEU, C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală (ANAF), judgment of 1 October 2015. See also Gloria González Fuster, 'Communication and Modalities for Exercising the Rights of the Data Subject' in Eleni Kosta and Franziska Boehm (eds), The EU Law Enforcement Directive (LED): A Commentary (Oxford University Press 2024).

categories, and processing purposes of that data.[539] If biometric data processed by FRT is inaccurate, data subjects hold the right to request corrections. Given the potential consequences of erroneous data in FRT applications, such as misidentification, this right is vital for ensuring data accuracy and fairness. Data subjects may also request the deletion of their biometric data from FRT systems under specific conditions, as outlined in Art. 17 of the GDPR and, similarly, by Art. 16 LED. This right applies when the data is no longer necessary for the purpose for which it was collected, when the data subject withdraws consent, or when the data processing does not comply with legal requirements. In law enforcement contexts, data erasure may be limited by public interest concerns, but individuals retain the right to request deletion in applicable cases. However, as noted by the ECtHR case law in particular, the continued storage of data, especially where the charges against a suspect have been dropped, "without a proportionality assessment of the further storage and motivation for the further storage in each case"[540] violates the rights to private life.[541] The right to restriction, under Art. 16 para. 3, allows data subjects to limit the processing of their biometric data in certain scenarios, such as when they contest the accuracy of the data or when the processing is unlawful, but the individual does not want the data erased. This restriction ensures that data is only processed under controlled circumstances, safeguarding individual privacy while enabling legitimate uses of FRT. For instance, law enforcement agencies must respect restriction requests when handling biometric data under investigation until accuracy or purpose issues are resolved.

These rights collectively emphasise that data subjects maintain significant control over their biometric data, even within high-risk AI applications such as facial recognition. The enforceability of these rights relies on the transparency and accountability of FRT deployers, who must facilitate individuals' ability to exercise their rights effectively.

[539] As underlined by scholarly analysis, this right is closely linked with the retention of data. Diana Dimitrova, 'Limitations to the Right of Access' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[540] Quoting Diana Dimitrova, 'Right to Rectification or Erasure of Personal Data and Restriction of Processing' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[541] Bundesverfassungsgericht, Beschluss vom 01. Juni 2006–1 BvR 2293/03 (Federal Constitutional Court, Decision of 1 June 2006–1 BvR 2293/03); ECtHR, *S. and Marper v. the United Kingdom*, 4 December 2008.

3.6.3 The AI Act framework

The AI Act introduces a distinct regulatory layer specifically targeting prohibited or high-risk AI applications like FRT. As mentioned above in §3.5.1, the Regulation does not explicitly list or recognize the application of high-risk provisions also for prohibited practices, besides the FRIA. It would be counter-intuitive to not see a link; however, the Regulation lacks any cross-referencing, besides the Commission's interpretation in the guidelines published on February 2025.

Art. 26, para. 10, on the obligations for high-risk systems, establishes a framework for their use, specifically post-remote biometric identification technologies, in criminal investigations. Under this regulation, any law enforcement agency intending to use post-remote biometric identification must obtain authorisation before its deployment. This *ex-ante* authorisation must come from a judicial or administrative authority, ensuring that an impartial entity reviews the intended use. If obtaining prior approval is not feasible, the agency has a maximum of 48 hours after the technology's use to secure authorisation. This process introduces a robust layer of oversight, as the authorising body must make a binding, reviewable decision.[542] This oversight mechanism aims to prevent arbitrary or unauthorised use of biometric technology, requiring law enforcement to justify the necessity and appropriateness of deploying such a powerful tool.

However, the provision allows for a limited exception to the authorization requirement. In cases where biometric technology is used to initially identify a potential suspect, an authorization may not be required, provided that there are objective and verifiable facts directly linking the individual to a specific offence. This exception recognizes that certain situations may demand swift action by law enforcement, especially when there is concrete evidence implicating someone in a crime. Nonetheless, even in these cases, the scope and purpose of the technology's use should be restricted to ensure that only the minimum necessary data is collected, in compliance with Directive LED.

Further restrictions address scenarios in which authorisation is ultimately denied. If an authorising body refuses to grant permission, the law enforcement agency must immediately halt the system's use and delete any personal data collected under the denied authorisation. This requirement prevents unauthorised data retention, ensuring that

[542] The topic of whether such a provision is respectful enough of the fundamental rights is analysed in Chapter 5.

individuals' biometric information is handled with the utmost care and deleted promptly in cases of non-compliance.

The regulation also expressly prohibits untargeted or indiscriminate use of post-remote biometric identification systems. The technology can only be employed when directly linked to an ongoing criminal investigation, a specific threat of a criminal offence, or the search for a missing person. By restricting its use to well-defined cases, the provision prevents mass surveillance or the deployment of facial recognition in ways that could infringe upon individuals' privacy without sufficient justification. This limitation ensures that high-risk AI systems are reserved for serious investigations, reducing the risk of privacy violations or potential misuse of biometric data.

In addition, any data output generated by such systems cannot serve as the sole basis for decisions with adverse legal effects on individuals. For instance, law enforcement cannot rely exclusively on AI results to arrest or charge someone, acknowledging the potential for inaccuracies or biases in AI outputs. This safeguard ensures that critical decisions affecting individuals' lives and liberties are based on a broader evidentiary context, not just on the AI's findings, which might produce false positives or errors.

Transparency and accountability measures are also embedded within the regulation. Each instance of post-remote biometric identification must be documented in the relevant police file, with these records available to market surveillance and data protection authorities upon request. Although sensitive operational details are excluded, this documentation enables external oversight, offering transparency about how and when high-risk AI systems are utilised.[543] In addition, law enforcement agencies must submit annual reports to regulatory authorities, summarising their usage of biometric identification technologies. These reports, which can be aggregated to cover multiple deployments, provide a comprehensive overview for regulatory bodies, facilitating ongoing compliance assessments.[544]

Recognising the unique risks that AI-powered surveillance technologies pose, the Act requires controllers to perform a rigorous conformity assessment[545] that encompasses not only a DPIA but also additional measures to ensure system accuracy, transparency, and accountability. For FRT, this includes evaluating the technology's design, the robustness

[543] AI Act, Art. 50.
[544] AI Act, Rec. 133.
[545] AI Act, Art. 9.

of algorithms against errors and biases, and the overall impact of the system on fundamental rights.

Moreover, under Article 27, law enforcement agencies deploying high-risk AI systems like FRT are obligated to conduct a FRIA. This tool is crucial for assessing and mitigating potential infringements on privacy and other rights, as the next Chapter will especially address. Through such a framework, law enforcement agencies must justify their deployment of FRT by demonstrating compliance with fundamental rights standards, a requirement that is especially important given the high risk of privacy invasion and potential discrimination inherent to biometric surveillance.

3.6.4 Integrated obligations across the GDPR, LED, and AI Act

The GDPR, LED, and AI Act together create a robust framework for FRT in law enforcement, requiring controllers to carefully navigate their overlapping yet distinct requirements. Each regulatory framework imposes specific, complementary obligations.

The GDPR provides the baseline for data protection, treating biometric data as a 'special category' requiring stringent handling due to its sensitivity. It mandates that FRT processing must be based on explicit consent or justified public interest, emphasising data minimisation, transparency, and safeguards against misuse. However, the GDPR's broad approach to data protection creates some overlap with the more specific mandates of the LED and the AI Act. For instance, both the GDPR and LED mandate DPIAs but with differing levels of detail and focus. The LED's DPIA requirements are tailored specifically for law enforcement, demanding assessments of necessity, proportionality, and potential bias in FRT use. This specificity can lead to confusion in cases where FRT is deployed for purposes that straddle both general data protection (as regulated by GDPR) and criminal investigations (as governed by LED), as agencies must navigate overlapping DPIA standards that lack clear demarcations for use cases.

Another source of regulatory overlap arises from the AI Act's requirements for high-risk AI systems, which include additional risk assessments, conformity assessments, and FRIA. While the AI Act intends to supplement existing GDPR and LED standards, it introduces new obligations that sometimes duplicate or conflict with those already in place. For instance, while GDPR and LED already enforce transparency and accountability in data handling, the AI Act requires a separate conformity assessment

specifically for AI applications, imposing added documentation and bias mitigation requirements that may be redundant or divergent from GDPR's established data protection principles. This layering of assessments – DPIA under GDPR, an enhanced DPIA under LED, and conformity assessments and FRIA under the AI Act – can create a burdensome compliance landscape, especially for law enforcement agencies tasked with adhering to all three frameworks simultaneously.

As mentioned, a critical gap in the AI Act is the unclear application of high-risk obligations to prohibited practices. The Act lacks specificity on whether stringent high-risk standards extend to practices that are outright prohibited. For instance, real-time FRT in public spaces is largely prohibited except in narrowly defined circumstances, but the regulatory obligations for such high-risk systems remain vague, creating uncertainty for deployers navigating compliance. This ambiguity could undermine the regulatory framework's coherence, as different deployers may interpret compliance requirements differently, potentially leading to inconsistent application and enforcement.

Lastly, the frameworks diverge on the issue of oversight and authorisation for FRT deployment. The LED emphasizes the need for judicial or administrative oversight, particularly for public surveillance, while the AI Act extends this requirement to high-risk AI applications but with a narrower focus. GDPR, in contrast, does not require judicial authorisation but relies on DPA to oversee critical data processing practices and incidents. This divergence in oversight standards creates uncertainty around the role of external vs. internal oversight, especially in high-risk deployments like FRT, where judicial oversight under the LED may conflict with self-regulatory expectations in GDPR and the AI Act. This lack of coherence can reduce the overall effectiveness of accountability mechanisms, as DPA and other agencies under the AI Act and LED may face conflicting expectations regarding who must authorize, review FRT use and potential incidents.

In summary, the GDPR, LED, and AI Act together create a framework for regulating FRT in the EU, establishing layers of accountability and transparency. However, the system is complex and relies heavily on the deployers' own assessments, which may not always align with objective regulatory standards. Addressing these ambiguities – such as clarifying the obligations on high-risk versus prohibited practices, enforcing mandatory empirical evidence of FRT's proportionality, and strengthening oversight mechanisms – would be essential to achieving a balanced framework. With clearer, more harmonized

standards across the GDPR, LED, and AI Act, the EU could enhance public trust in FRT while protecting the fundamental rights of individuals, setting a strong precedent for responsible and rights-centered AI governance globally.

Table 5 – Integrated obligations.

Regulatory Framework	Key elements	Main obligations
GDPR (Reg. (EU) 2016/679)	Protects personal data across sectors, including law enforcement; establishes lawful basis for processing biometric data due to high sensitivity.	- Lawful Basis: Controllers must establish a lawful basis under Article 9 for processing biometric data (usually explicit consent or necessity for public interest). - Data Protection Impact Assessment (DPIA): Required for FRT to assess risks to individuals' rights, detailing purposes, alternatives, and safeguards. - Transparency and Data Minimization: Collect only necessary data; implement retention limits and inform individuals of data use where possible. - Involvement of Data Protection Officer (DPO): DPO to review high-risk aspects, e.g., inaccuracies or bias in FRT.
LED (Dir. (EU) 2016/680)	Tailored to law enforcement's unique needs; applies when the GDPR's general requirements do not fully cover law enforcement's data processing for criminal investigation and prevention.	- Strict Necessity and Proportionality: Processing must be strictly necessary for law enforcement purposes, limited to serious crimes or significant threats to safety. - DPIA with Additional Requirements: DPIA must assess FRT's utility, risks of bias or discrimination, and necessity

		over less invasive tools; restricted use of collected data solely for original investigative purposes. - Judicial Authorization and Oversight: FRT use must have judicial approval to avoid unchecked surveillance, especially in public spaces where privacy rights are prominent.
AI Act (Reg. (EU) 2024/1689)	Focuses on high-risk AI applications, classifying real-time FRT in public spaces as high-risk; aims to address specific risks posed by AI technologies in law enforcement settings.	- Conformity Assessment and FRIA: Comprehensive risk assessment and FRIA to verify compliance. - Restriction to Exceptional Cases: Real-time FRT is restricted to limited circumstances (e.g., counterterrorism, see Annex II), with prior judicial authorization required. - Ongoing Monitoring and Transparency: Continuous monitoring of FRT's performance; documentation and transparency about system metrics (e.g., accuracy rates). - Bias Mitigation: Controllers must address biases, ensuring training/testing datasets are representative; perform DPIA when system is updated or adapted.
Integrated obligations	GDPR's data protection principles provide a base, refined by LED's law enforcement focus on necessity and oversight, with AI Act's targeted AI regulations for high-risk applications. Specifically, emphasis on public transparency, judicial oversight, and	

	continuous monitoring to uphold privacy and fundamental rights while utilizing FRT in law enforcement.

3.7 Conclusion

This chapter has delved into the European Union's multi-layered regulatory framework governing facial recognition technology, with a particular emphasis on its use in law enforcement. By analysing the interplay of the GDPR, LED, and the AI Act, it has revealed the strengths and limitations of the current legal framework in addressing the complex challenges posed by biometric surveillance.

The GDPR establishes the foundation, enshrining data protection principles that ensure biometric data, classified as a special category, is processed only with a lawful basis, such as explicit consent or substantial public interest. It emphasizes data minimisation, transparency, and accountability to mitigate privacy risks. The LED extends these protections to law enforcement contexts, embedding principles of necessity and proportionality into its framework. It requires robust safeguards to balance public security needs with fundamental rights, particularly in high-stakes applications like criminal investigations.

The AI Act, as the newest regulatory layer, builds upon these principles by categorising FRT as a prohibited, upon conditions, or high-risk AI application and introducing targeted obligations for its deployment. These include strict requirements for conformity assessments, judicial or administrative authorisation, and continuous monitoring of the technology's impact on fundamental rights. However, significant challenges remain, particularly in the lack of clarity between high-risk and prohibited practices and the potential inconsistencies arising from self-assessment by deployers. The Act's distinctions between "real-time" and "post-remote" FRT systems also introduce complexities that risk fragmenting compliance efforts and enforcement.

The feeling surrounding FRT regulation, however, is one of being caught "between the 'too late' and the 'not enough.'"[546] On the one hand, the rapid evolution of this technology has often outpaced regulatory measures, leaving gaps in oversight and accountability. On the other hand, the legal frameworks in place, while comprehensive in their ambition,

[546] Uroš Ćemalović, 'Prohibited Artificial Intelligence Practices According to Article 5 of the European Union's Regulation on AI—between the "Too Late" and the "Not Enough"' (2024) 32 International Journal of Law and Information Technology.

often fall short of providing the specificity and harmonisation needed to address the full spectrum of risks posed by FRT. This duality highlights the urgency of creating a more coherent and anticipatory regulatory approach that keeps pace with technological innovation while safeguarding fundamental rights.

As the concluding chapter of the first part of this thesis, this analysis underscores the EU's commitment to regulating FRT in alignment with EU values and fundamental rights. Yet, it also highlights the interpretive and practical burdens placed on practitioners, regulators, and deployers to navigate overlapping legal frameworks. Achieving coherence across the GDPR, LED, and AI Act is not merely an academic exercise; it is a necessary step to uphold the rule of law in an era of pervasive surveillance technologies.

Looking ahead, the transition to the second part of this thesis shifts the focus to a deeper exploration of the obligations surrounding the fundamental rights impact assessment. These tools, mandated under the AI Act, will be examined in the context of their capacity to bridge the gaps identified in this chapter. Chapter 4 will open this discussion, analysing how FRIA can serve as a cornerstone for ensuring compliance, enhancing transparency, and safeguarding individuals' rights in the deployment of FRT and other high-risk AI systems. Through this lens, the thesis will continue to assess the regulatory mechanisms needed to balance innovation with the protection of fundamental rights in the age of artificial intelligence.

II PART

4. FUNDAMENTAL RIGHTS IMPACT ASSESSMENT

SUMMARY: 4.1 Introduction. 4.2. A premise: the protection of fundamental rights in the EU; 4.2.1 The horizontal effect of fundamental rights. – 4.3 Impact assessments as vessels of risks: a taxonomy; 4.3.1 Impact assessments in the international context. – 4.4 The Fundamental Rights Impact Assessment; 4.4.1 The actors; 4.4.2 Time and modalities; 4.4.3 Key elements; 4.4.4 Procedural obligations; 4.4.5 Data Protection Impact Assessment: friend or foe?; 4.4.6 Impact assessments: drawing parallels; 4.4.7 The other impacts assessments under the AI Act; 4.4.8 Critical analysis of the FRIA. – 4.5 Much ado about methodology; 4.5.1 FRIA: borrowing a methodology?; 4.5.2 Utility with the AI Act. – 4.6 Conclusion.

4.1 Introduction

> "The future of AI regulation must be based on the protection of fundamental rights, democracy and the rule of law. Yet, at this stage, we cannot even imagine all potential fundamental rights challenges posed by AI".[547]

The second part of this thesis focuses on the analysis and implementation of a rights-based framework to identify, evaluate, and mitigate potential infringements on fundamental rights.[548] Central to this exploration is the conundrum on effectively assessing the severity and scope of fundamental rights violations in the context of AI systems. The answer to this question should move from understanding the significant, as Pollicino observes, "challenges to the role and tools of constitutional law" posed by the particular context this thesis aims to analyse.[549]

---

[547] Maciej Szpunar, 'New Technologies in the Case Law of the Court of Justice – Lessons Learnt and Lessons to Be Learnt' [2024] ERA Forum.

[548] A premise. The term fundamental right is used in the European Union (EU) to express the concept of 'human rights' within a specific EU internal context. Traditionally, the term 'fundamental rights' is used in a constitutional setting whereas the term 'human rights' is used in international law, as also clarified, *inter alia,* by Eleanor Spaventa, '9. Fundamental Rights in the European Union', *European Union Law* (Oxford University Press); Paul Craig and Gráinne de Búrca, '12. Human Rights in the EU', *EU Law* (Oxford University Press); Koen Lenaerts, Piet Van Nuffel and Tim Corthaut, 'Fundamental Rights and General Principles of Union Law' in Koen Lenaerts, Piet Van Nuffel and Tim Corthaut (eds), *EU Constitutional Law* (Oxford University Press 2021). On the trends of the Court of Justice of the EU and on the specific use of this term, see Gráinne de Búrca, 'The Road Not Taken: The European Union as a Global Human Rights Actor' (2011) 105 American Journal of International Law 649; Jan Wouters and Michal Ovádek, 'Concepts and Language of Human Rights in the EU' in Jan Wouters and Michal Ovádek (eds), *The European Union and Human Rights: Analysis, Cases, and Materials* (Oxford University Press 2021); Steven Greer, Rosie Slowe and Janneke Gerards, *Human Rights in the Council of Europe and the European Union: Achievements, Trends and Challenges* (Cambridge University Press 2018); Allan Rosas, 'The Court of Justice of the European Union: A Human Rights Institution?' (2022) 14 Journal of Human Rights Practice 204.

[549] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Bloomsbury Publishing 2021) cit. p. 190.

The increasing reliance on AI and its power of autonomy[550] in domains such as justice, law enforcement, and public services introduces the risk of perpetuating bias, discrimination, and inequality.[551] These risks not only confront the effectiveness of constitutional protections but also underscore the urgent need for frameworks capable of safeguarding fundamental rights in complex, technology-driven systems.[552]

Therefore, drawing from the premises in the previous Chapters, this section aims to position in between a significant gap that is in the ability to concretely identify which rights are at stake in specific contexts, the nature of the interferences, and the measures necessary to mitigate such risks.[553] As a matter of fact, traditionally, the ability to assess and enforce fundamental rights protections has been dedicated to courts. However, the advent of digital technologies[554] has blurred these lines,[555] in part delegating roles traditionally held by the judiciary to public actors like law enforcement and even private entities:[556] both of them, in their capacity of deployers of AI, are now tasked with assessing the fundamental rights impact of their systems. This shift highlights the need

[550] See, Chapter, 2, in part. §2.3.1.

[551] Specifically, Andrea Simoncini and Erik Longo, 'Fundamental Rights and the Rule of Law in the Algorithmic Society' in Hans-W Micklitz and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021).

[552] Simoncini and Suweis (n 30).

[553] As observed by Pollicino, "digital firms are no longer market participants: rather, they are market makers, which are capable of exerting quasi-regulatory control over the terms on which others can sell goods and services", Pollicino, id. p. 48. In particular, with respect to AI, Pasquale also noted that "as artificial intelligence improves, the tracking of shopping into the Amazon groove will tend to become ever more rational for both buyers and sellers. Like a path through a forest trod ever clearer of debris, it becomes the natural default". See 'From Territorial to Functional Sovereignty: The Case of Amazon' (*LPE Project*, 6 December 2017) <https://lpeproject.org/blog/from-territorial-to-functional-sovereignty-the-case-of-amazon/> accessed 10 November 2024.

[554] The expansion of digital technologies has led to significant shifts in the responsibilities traditionally held by public institutions, with private sector entities now playing critical roles in areas such as data management, online security, and digital rights protection. As private companies collect, process, and control vast amounts of personal data, their actions increasingly impact fundamental rights, effectively placing them in quasi-public roles. This blurring of lines raises questions about accountability and regulatory oversight, particularly in the areas of privacy, security, and ethical AI use. See Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019). Marco Bassini, 'Fundamental Rights and Private Enforcement in the Digital Age' (2019) 25 European Law Journal 182; Woodrow Hartzog, 'Two AI Truths and a Lie' (2024) 26 Yale Journal of Law and Technology 595.

[555] Erik Longo, 'La "Giustizia Digitale" Tra Nuove Forme Di Efficienza e Garanzia Dei Diritti Costituzionali' (2023) 4 La Nuova Giuridica 187.

[556] Giovanni De Gregorio and Simona Demková, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' in Charlotte van Oirsouw and others (eds), *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era* (TMC Asser Press 2024); Giulia Gentile, 'Between Online and Offline Due Process: The Digital Services Act' (24 August 2023) SSRN.

for tools that ensure accountability and protection in these new, uncharted territories, in which the traditional roles are no longer fixed.

In this context, the Fundamental Rights Impact Assessment (FRIA), [557] as mandated by the AI Act, emerges as a critical mechanism. On the one hand, it allows a recalibration and refocusing of fundamental rights considerations within the AI context. On the other hand, it facilitates this shifting of roles, explicitly mandating both public and certain private actors to undertake fundamental rights assessments for their AI systems. Henceforth, the FRIA is positioned as a pivotal mechanism for mitigating risks associated with high-risk AI systems. While its application often involves practical tools and templates,[558] such as checklists, it is essential to move beyond operational elements and engage with the deeper meaning of rights protection. This includes not only reacting to harm once it occurs but also proactively mitigating risks from the outset, as explicitly required by the AI Act.

This chapter argues that the FRIA should not be treated as a technocratic risk-management tool, but rather as a normative mechanism rooted in constitutional law. Its purpose is not simply to detect violations, but to assess whether the legal, procedural, and institutional conditions surrounding AI deployment comply with constitutional principles, particularly those of proportionality, necessity, and accountability. In this light, FRIA becomes a tool for contesting not just specific uses of AI systems like facial recognition, but the legitimacy of the frameworks in which they operate.

Specifically, this thesis seeks to address these critical questions: which fundamental rights are concretely engaged by facial recognition technologies? How can these rights be identified and assessed in practice?

These answers are going to be searched having in mind the FRIA, which must be positioned within the broader framework of the multilevel fundamental rights protection, as will be explained *infra.* These assessments are intended not only to guide the development of AI and digital technologies but also to ensure that these innovations align

[557] AI Act, Art. 27, "1. Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce.".

[558] As mandated by Art. 27(5), of the AI Act.

with European fundamental rights.[559] Nonetheless, the understanding of fundamental rights, their scope, their impact on human lives, and their interpretation, must remain firmly rooted in their essential purpose: to protect human dignity, equality, and freedom.[560] This thesis does not aim to delve into abstract theoretical debates but seeks to situate fundamental rights within the lived realities of individuals and the broader societal values they serve.[561] Such an approach ensures that these rights are not only legally articulated but also meaningfully applied in contexts shaped by technology and human experience.

As observed by Cartabia,[562] to grasp the true colors of fundamental rights the analysis should be based on the essentiality of the human experience. Precisely, rooting the understanding of fundamental rights in the human experience grounds the assessments in the realities and rights of individuals, ensuring that protections are not abstract but directly relevant and meaningful. This assessment should be complemented with the analysis of the judicial dialogue which enriches the process of drawing the insights from cross-jurisdictional interpretations, fostering a nuanced and context-sensitive approach to identifying and mitigating risks.

This approach ensures that the FRIA is not merely a technical tool but a mechanism that engages deeply with the lived realities of individuals and the evolving role of courts, public actors, and private entities.[563] By integrating these principles, the FRIA enables not only a reactive response to rights violations but also proactive mitigation of risks from the outset, as envisioned in the AI Act.

To this end, the sections that follow are structured to transition from general concepts to more specific applications. This structure ensures a logical progression, linking

[559] Especially, the term 'fundamental rights' is used in European Union (EU) to express the concept of 'human rights' within a specific EU internal context. The term 'human rights' refer to the international context, more specifically. Martinico and Pollicino (n 27); Csongor István Nagy, 'The Diagonality Problem of EU Rule of Law and Human Rights: Proposal for an Incorporation à l'européenne' (2020) 21 German Law Journal 838; Stephen Brittain, 'The Relationship Between the EU Charter of Fundamental Rights and the European Convention on Human Rights: An Originalist Analysis' (2015) 11 European Constitutional Law Review 482.

[560] Norberto Bobbio, *L'età Dei Diritti* (Einaudi 1990).

[561] Giuseppe Franco Ferrari, 'Diritti fondamentali: linee evolutive, diffusione e tipologie' (UTET 2023); Cartabia, *I diritti in azione* (n 29); Giandonato Caggiano, 'Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione' 18.

[562] Marta Cartabia, 'Universality of Rights in the Era of "New Rights"' [2009] Quaderni costituzionali.

[563] Vasiliki Kosta, 'Fundamental Rights Mainstreaming in the EU', *The EU and the Proliferation of Integration Principles under the Lisbon Treaty* (Routledge 2014).

foundational principles to the practical challenges and methodologies discussed in subsequent sections. Section 4.2 situates the FRIA within the broader framework of multilevel protection of fundamental rights. Then, Section 4.3, traces the evolution of impact assessments as regulatory instruments, discussing their role, limitations, and adaptation for the AI landscape. Moving to the core elements of the FRIA, Section 4.4 delves into the design, challenges, and interplay of the FRIA with other compliance tools, such as DPIAs, to highlight its distinct contributions. Finally, section 4.5 proposes a methodology for conducting the FRIA, building on the principles described above the unification of the deep meaning of the right together with the analysis of the relevant case law, and emphasising the unique nuances of this tool compared to traditional impact assessments. Finally, this chapter lays the groundwork for Chapter 5, which will elaborate on a comprehensive methodology for conducting Fundamental Rights Impact Assessments on facial recognition technology, while Chapter 6, that concludes the analysis, will then focus on the right to an effective remedy, exploring its critical role in ensuring redress for violations of fundamental rights within the use of FRT.

4.2 A premise: the protection of fundamental rights in the EU

Before delving into the analysis of the contextual challenges in ensuring robust fundamental rights protection, it is essential to recognise the inherent convolution of the European Union's system for safeguarding these rights. This complexity[564] stems from the necessity of addressing what scholars have termed the "multilevel protection" of fundamental rights: a dynamic interplay between EU-level frameworks, national legal systems, and the evolving jurisprudence that connects them.[565]

Conversely, even if "the EU has no general fundamental rights competence, although fundamental rights are clearly woven into its fabric",[566] its multi-layered system reflects

[564] Giuseppe Martinico, *The Tangled Complexity of the EU Constitutional Process: The Frustrating Knot of Europe* (Routledge 2022).

[565] The expression has been seemingly elaborated as *Verfassungsverbund* (translated from German as 'composite constitution') by Ingolf Pernice, in particular in Ingolf Pernice, 'Multilevel constitutionalism and the Treaty of Amsterdam: European constitution-making revisited?' Common Market Law Review (1999) 36 703–5. More recently, Ingolf Pernice, 'Multilevel Constitutionalism and the Crisis of Democracy in Europe' (2015) 11 European Constitutional Law Review 541; Ingolf Pernice, 'Multilevel Constitutionalism in the European Union' (2002) 27 European law review 511.

[566] Eleanor Spaventa, 'Should We Harmonize Fundamental Rights in the EU? Some Reflections about Minimum Standards and Fundamental Rights Protection in the EU Composite Constitutional System' (2018) 55 Common Market Law Review (cit. p.1000).

the "complexity of the relation between the sources of law in which fundamental rights are enshrined".[567] Consequently, this affects the legal relationships among EU institutions, Member States, and private actors.

Hence, even though initially the priorities of the EU did not include the protection of fundamental rights as well,[568] through the proclamation of the Charter of Fundamental Rights (CFREU) and its entry into force with the Lisbon Treaty (hereafter, TEU) gave a clear impetus to the realisation of the Europe of rights,[569] even though "the EU has no general fundamental rights competence, although fundamental rights are woven into its fabric".[570]

Nevertheless, in *Stauder v. City of Ulm,*[571] the ECJ made its first explicit reference to fundamental rights, asserting that such rights were "enshrined in the general principles of Community law and protected by the Court."[572] Shortly thereafter, in *Internationale Handelsgesellschaft*, the Court affirmed that fundamental rights, as general principles, were integral to the validity of EU law, even where conflicts with national constitutional norms arose.[573] The development of these principles continued with *Nold v. Commission*,[574] where the CJEU clarified that the protection of fundamental rights must align with the constitutional traditions common to Member States and international

[567] Chiara Amalfitano, *General Principles of EU Law and the Protection of Fundamental Rights* (Edward Elgar Publishing 2018), in part. p. 1-6.

[568] Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779; Paul Craig, 'The Charter, the ECJ and National Courts' in Diamond Ashiagbor, Ioannis Lianos and Nicola Countouris (eds), *The European Union after the Treaty of Lisbon* (Cambridge University Press 2012).

[569] Marta Cartabia, 'La tutela multilivello dei diritti fondamentali. Il cammino della giurisprudenza costituzionale italiana dopo l'entrata in vigore del Trattato di Lisbona', Incontro trilaterale tra le Corti costituzionali italiana, portoghese e spagnola, Santiago del Compostela 16-18 ottobre 2014. More specifically on the impact of the evolution see Marta Cartabia, *L'ora Dei Diritti Fondamentali Nell'Unione Europea* (Il Mulino 2007).

[570] Eleanor Spaventa, 'Should We Harmonize Fundamental Rights in the EU? Some Reflections about Minimum Standards and Fundamental Rights Protection in the EU Composite Constitutional System' (2018) 55 Common Market Law Review (cit. p.1000).

[571] ECJ*, Erich Stauder v City of Ulm,* Case 29/69, 12 November 1969.

[572] Id., §7.

[573] ECJ, *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermitte,* C-11/70, 17 December 1970. In part. §4, "in fact, respect for fundamental rights forms an integral part of the general principles of law protected by the Court of Justice. The protection of such rights, whilst inspired by the constitutional traditions common to the member states, must be ensured within the framework of the structure and objectives of the community. it must therefore be ascertained, in the light of the doubts expressed by the *verwaltungsgericht*, whether the system of deposits has infringed rights of a fundamental nature, respect for which must be ensured in the community legal system".

[574] ECJ, J. Nold, Kohlen- und Baustoffgroßhandlung v Commission of the European Communities, C-4/73, 14 May 1974.

treaties, particularly the ECHR, among "international treaties for the protection of human rights on which the member states have collaborated or of which they are signatories".[575]

Definitely, the entry into force of the Charter was further strengthened by the role of the Court of Justice, making it a "human rights adjudicator"[576], also in the digital context.

In this respect, it is, for instance, worth mentioning cases like *Digital Rights Ireland*[577] or *Schrems I*,[578] where the CJEU evaluated the laws according to the canon of the Charter. Especially in the first case, the Court annulled the Directive 2006/24, as per a preliminary ruling of the Irish Supreme Court and the Austrian Constitutional Court, for violation of the rights to privacy and the protection of personal data, protected by Articles 7 and 8 of the EU Charter.[579]

Furthermore, the EU's commitment to fundamental rights protection is achieved through several layers, rooted in both the EU Charter of Fundamental Rights (CFREU, or the Charter) and the European Convention on Human Rights (ECHR), as anticipated in *Nold*. Article 6 of the TEU is central to this framework,[580] as it confers binding legal status on the Charter, stating that it "shall have the same legal value as the Treaties."[581] This formal recognition positions the Charter as a cornerstone of EU law, obliging EU institutions and Member States, when implementing EU law, to uphold a uniform standard for fundamental rights across the Union.[582]

In this respect, Article 6 of the TEU further clarifies also the EU's relationship with the ECHR. Article 6(3) TEU explicitly recognises the fundamental rights guaranteed by

---

[575] Id., §13.

[576] Gráinne de Búrca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20 Maastricht Journal of European and Comparative Law 168.

[577] CJEU (Grand Chamber), Joined C-293/12 and C- 594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.

[578] CJEU (Grand Chamber), C-362/14, Maximillian Schrems v. Data Protection Commissioner, 6 October 2015.

[579] For a comment on the doctrine of the essence of the fundamental rights, used by the Court, Lenaerts (n 459).

[580] Ingolf Pernice, 'The Treaty of Lisbon and Fundamental Rights' in Stefan Griller and Jacques Ziller (eds), *The Lisbon Treaty: EU Constitutionalism without a Constitutional Treaty?* (Springer 2008).

[581] The Charter, even before its entry into force with the Treaty of Lisbon, has always been recognised as more as soft law. As a matter of fact, as also recalled by Herzog, the Charter was drafted 'as if' it was meant to acquire the nature of the Treaty. See 'Record of the first meeting of the Body to draw up a draft Charter of Fundamental Rights of the European Union', held in Brussels, 17 December 1999, p. 9.

[582] On the troubles in granting uniform applications of fundamental rights within the 'multilevel' stage of fundamental rights, Spaventa, 'Should We Harmonize Fundamental Rights in the EU?' (n 24). As observed by the author, this difficult achievement is indeed reflected by the Charter, "in particular, the precise scope of application of the Charter, and therefore the boundary between national and European fundamental rights, remains nebulous. And, despite references to national constitutional laws,16 the Charter also failed to solve the age-old problem of "conflicting" standards of rights when the EU provides a lower standard than national (constitutional) law" (p. 1001-1002).

the ECHR as general principles[583] of EU law.[584] This provision not only reinforces the significance of the ECHR within the EU's legal order but also embeds the case law of the European Court of Human Rights (ECtHR) as a key interpretative tool for EU law.[585] The commitment to fundamental rights is thus shared across both the EU's internal framework, i.e., the Charter, and the external framework provided by the ECHR, creating a dual-layered approach to human rights protection.

Moving onto the Member States,[586] the analysis takes into consideration the case of Italy: the relationship between EU law, the Charter, and the ECHR is nuanced and reflects constitutional limits.[587] The Charter's application is closely linked to Article 11 of the Italian Constitution, which allows limitations on sovereignty necessary for ensuring peace and justice among nations. This article facilitates the adoption of EU law in Italy, provided it aligns with the "counter-limits" established by the Italian Constitution, meaning that EU provisions must not conflict with Italy's fundamental constitutional principles.[588]

---

[583] ECJ, Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, C-11/70, 17 December 1970.

[584] This troubled relationship is described by M. Cartabia (n. 23) as the "fatal attraction" of the ECHR in the EU legal systems. The scholar specifies that "strictly excluding that Article 6 requires the direct and immediate application of Convention law in national legal systems, the Court of Justice confirmed that the Lisbon Treaty did not affect the legal regime of the ECHR in national legal systems" (auth. transl.). For a critical comment on the "missed" opportunities of the application of the Convention in the EU Legal system see Lenaerts, Van Nuffel and Corthaut (n 548); Búrca (n 548).

[585] On the relationship between the two legal systems see, *inter alia,* Jean Claude Bonichot and Angelika Nußberger, "Dialogue entre juges européens", in B. Bonnet (eds.), Traité des rapports entre ordres juridiques (Paris, LGDJ, 2016) 1269; Giorgio Repetto, 'The Constitutional Relevance of the ECHR in Domestic and European Law' [2013] Intersentia, Cambridge-Antwerp-Portland; Umberto Lattanzi, 'The Inapplicability of the Bosphorus Presumption to the European Economic Area Agreement: A Risk for the Coherence of Legal Systems in Europe' (2023) 19 European Constitutional Law Review 441.

[586] Koen Lenaerts and Kathleen Gutman, 'The Comparative Law Method and the Court of Justice of the European Union: Interlocking Legal Orders Revisited' in Mads Andenas and Duncan Fairgrieve (eds), *Courts and Comparative Law* (Oxford University Press 2015); Christian Calliess and Gerhard van der Schyff (eds), 'Comparative Constitutional Identity and Multilevel Constitutionalism', *Constitutional Identity in a Europe of Multilevel Constitutionalism* (Cambridge University Press 2019).

[587] Vittoria Barsotti and others, 'Italian Constitutional Justice in Global Context', *Italian Constitutional Justice in Global Context* (Oxford University Press, Incorporated 2015); Mart Cartabia, 'The Italian Constitutional Court and the Relationship Between the Italian Legal System and the European Community' (1990) 12 Michigan Journal of International Law 173.

[588] Italian Constitutional Court rulings, such as judgments 170 of 1984 and 232 of 1989, underscore this position, supporting a separation by areas of competence between national and EU laws. More recently, in judgment 15 of 2024, the Constitutional Court also reinstated this principle by analysing, in a conflict about discriminatory regional laws, the access to the diverse remedies this multilevel framework grants to individuals. As a matter of fact, the Court clarified that the constitutional review of laws, overseen by the Italian Constitutional Court, and the compatibility check of national legislation with EU law, entrusted to national courts and the CJEU do not operate in opposition to one another. Rather, they form a "concorso di rimedi giurisdizionali" (a convergence of judicial remedies) (§8.3 of the decision) aimed at safeguarding fundamental rights. The role of the CJEU in ensuring that national law complies with EU law complements the Constitutional Court's centralised review of constitutional legitimacy, which is "a foundation of

Conversely, Article 117(1) of the Italian Constitution regulates, *inter alia,* the ECHR's relationship with Italian law, which requires it to comply with international obligations, including, then, the ECHR. However, the ECHR's provisions, as interpreted by the ECtHR, hold an "intermediate" status in Italian law, henceforth superior to ordinary legislation but subordinate to the Constitution. This distinction means that while Italian judges interpret national law in light of the ECHR, only the Constitutional Court has the authority to declare national legislation incompatible with the Convention, provided such interpretation does not conflict with core constitutional principles.[589]

Within this multi-layered framework, the application of fundamental rights in the EU operates across three main dimensions:[590] (1) vertically against EU institutions, (2) vertically against Member States when implementing EU law, and (3) horizontally between private parties under certain circumstances.

First, EU institutions are directly bound by the Charter in all their actions, ensuring that fundamental rights are upheld at the Union level. Article 51(1) of the Charter explicitly mandates this, aiming to create a consistent standard of rights protection across the Union. This dimension is relatively uncontroversial, as EU institutions are expected to embody and uphold the values of the Union, including the respect for fundamental rights as defined by the Charter and influenced by the ECHR.[591]

Second, Member States are bound to EU fundamental rights when "either implementing EU law or acting within its scope".[592] Article 51(1) of the Charter reiterates this by binding Member States to uphold the Charter when they "implement Union law." This dimension reflects a balance between EU oversight and national sovereignty, ensuring that EU fundamental rights are upheld even when EU law is enforced through national means. However, this only applies when Member States are engaged in actions

---

constitutional architecture" (§8.2, but also Art. 134 Italian Constitution, as also interpreted in judgment n. 269 of 2017. Together, these judicial remedies, with their distinct features, collectively uphold the protection of fundamental rights, creating a cohesive system that bridges the application of EU and national constitutional principles.

589 The Italian Constitutional Court's judgments 348 and 349 of 2007 established this interpretative framework, ensuring that both EU law and the ECHR are integrated into Italian law in a way that respects national constitutional identity. See also, in this respect, 'Fonti Europee' in Roberto Bin and Giovanni Pitruzzella *Diritto costituzionale* (Ventitreesima edizione, G Giappichelli 2022).

590 This structure is elaborated by Spaventa in Eleanor Spaventa, 'The Horizontal Application of Fundamental Rights as General Principles of Union Law' (Hart Publishing 2011).

591 Eleanor Spaventa, 'The interpretation of Article 51 of the EU Charter of Fundamental Rights: the dilemma of stricter or broader application of the Charter to national measures', Study commissioned by the Policy Department for Citizen's Rights and Constitutional Affairs at the request of the PETI Committee, 2016.

592 Ibid.

directly tied to EU law, maintaining a boundary between national autonomy and EU oversight.[593]

Finally, the horizontal effect of fundamental rights,[594] an evolving concept within EU jurisprudence, allows individuals to assert fundamental rights directly against other private parties.[595] This horizontal application is particularly relevant when private actors hold substantial power over individuals' rights, as in cases involving large technology companies or data controllers.[596] To understand the implications of this doctrine in the digital and especially in the current framework of rights and freedoms further triggered by AI, the next paragraph is devoted to the analysis of the horizontal effect doctrine.

4.2.1 The horizontal effect of fundamental rights

Consider the case of AI systems used to assess the likelihood of reoffending, which are applied in criminal justice contexts to assist judges in making sentencing or parole decisions.[597] These algorithms, designed and owned by private firms, can have profound impacts on individuals' lives by influencing decisions that determine their freedom.[598] The risk here is that AI technologies, operating under private control but within in the performance of their public duties, may lead to biased or unfair outcomes,

[593] Ibid.

[594] *Inter alia,* Mark Tushnet, 'The Issue of State Action/Horizontal Effect in Comparative Constitutional Law' (2003) 1 International Journal of Constitutional Law 79; Przemyslaw Miklaszewicz and Marek Safjan, 'Horizontal Effect of the General Principles of EU Law in the Sphere of Private Law' (2010) 18 European Review of Private Law 475; Dorota Leczykiewicz, 'Horizontal Application of the Charter of Fundamental Rights' (Social Science Research Network, 19 September 2013) <https://papers.ssrn.com/abstract=2328175> accessed 10 November 2024; Eleni Frantziou, '(Most of) the Charter of Fundamental Rights Is Horizontally Applicable: ECJ 6 November 2018, Joined Cases C-569/16 and C-570/16, Bauer et Al' (2019) 15 European Constitutional Law Review 306; Gunther Teubner, 'Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution Essays' (2017) 3 Italian Law Journal 193; Stephen Gardbaum, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102 Michigan Law Review 387.

[595] Also, in this respect, Spaventa, id., distinguishes between conflicts arising due to national rules falling within the scope of the Treaty that are incompatible with a general principle of EU law and are invoked in litigation between private parties; or, the same situation involving a Directive rather than the Treaty. This latter one has been analysed by the Court of Justice in C-144/04 (Grand Chamber), *Werner Mangold v Rüdiger Helm,* 22 November 2005.

[596] Oreste Pollicino, 'L'efficacia Orizzontale Dei Diritti Fondamentali Previsti Dalla Carta La Giurisprudenza Della Corte Di Giustizia in Materia Di Digital Privacy Come Osservatorio Privilegiato' [2024] Rivista di Diritto dei Media - MediaLaws 1.

[597] Lagioia, Rovatti and Sartor (n 194); Simoncini and Suweis (n 30).

[598] On the implications on vulnerable groups, see Sofia Ranchordas and Malou Beck, 'Vulnerability in Kaufmann, Mareile and Lomell, Heidi Mork (Eds) Handbook of Digital Criminology. De Gruyter, Forthcoming' (9 October 2023) <https://papers.ssrn.com/abstract=4596689> accessed 3 December 2024.

disproportionately affecting vulnerable groups.[599] For example, studies have shown that certain AI models used in predictive policing and sentencing can perpetuate racial biases, as these systems often rely on historical data that reflect existing inequalities.[600]

This scenario highlights the need for regulatory tools that require both public and private actors to evaluate and mitigate the potential impacts of AI on fundamental rights. However, if the former one is an easy accomplishment, at least in legal theory terms, the enforcement of fundamental rights vis-à-vis private actors is a more delicate goal.

The scholars' reactions suggested the predictability of the "horizontal effect doctrine", affirming that this approach would enable individuals to assert their rights not only against state actors but also against "social institutions, in particular centres of economic power."[601] This envisions, for instance, the purpose of holding powerful private entities accountable, thus extending the protection of fundamental rights into the private sphere[602], especially thanks to the role of the Court, as unpacked *infra.*

Hence, framing it theoretically, [603] the concept of the horizontal application of fundamental rights, or *Drittwirkung*, has its roots in German constitutional law, where courts first recognised that certain fundamental rights could apply not only in the vertical relationship between the state and individuals but also horizontally, in interactions

[599] As recalled by the European Union Agency for Fundamental Rights (FRA), the term 'bias' can have a different meaning depending on the context in which it is used and the particular discipline it comes from, for example, law or computer science. For the context of this chapter, it is helpful to stress that biases might be generated by i) a differential treatment based on protected characteristics, such as discrimination and bias-motivated crime, ii) differentiation, iii) statistical results, and iv) offset from origin. European Union Agency for Fundamental Rights (FRA), Handbook on European non-discrimination law, 2018. See also Ljupcho Grozdanovski, 'In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law' (2021) 58 Common Market Law Review.

[600] European Union Agency for Fundamental Rights (FRA), 'Bias in algorithms - Artificial intelligence and discrimination', 8 December 2022. Tiffany C Li, 'Algorithmic Destruction' (Social Science Research Network 2022); Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking For' (LawArXiv 2017).

[601] Gunther Teubner, 'Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?', *Luhmann and Law* (Routledge 2017); Teubner, 'Horizontal Effects of Constitutional Rights in the Internet' (n 594).

[602] Marco Bassini, 'Fundamental Rights and Private Enforcement in the Digital Age' (2019) 25 European Law Journal 182.

[603] Although, the scope of this thesis is not to provide a comprehensive analysis of the horizontal application of fundamental rights in EU law. Rather, it aims to highlight how this concept aligns with the requirements of the Fundamental Rights Impact Assessment (FRIA), particularly in the context of the digital age, where private actors increasingly impact individual rights. The primary focus remains on the area of law enforcement, where public authorities, as traditional duty-bearers of fundamental rights obligations, are expected to conduct FRIAs to evaluate and mitigate potential rights impacts. This focus underscores the differentiated responsibilities of public and private actors while recognizing the expanding role of private entities in rights protection

between private parties.[604] This recognition arose from the understanding that private entities, especially in the digital age, can exercise substantial power over individuals' rights, making it essential to ensure that fundamental rights are respected even in private relationships.[605]

As a matter of fact, over time, this concept has become well-established not only in Germany but also across other European constitutional courts, as well as in the case law of the European Court of Human Rights.[606] Within the European constitutionalism,[607] the horizontal applicability of fundamental rights is far from taboo, as anticipated, which is unsurprising given the deeply embedded meta-principle of human dignity – a core value that not only appears in numerous European constitutional provisions and forms the basis of Title I of the Charter of Fundamental Rights but also reflects a collective response to the historical suppression of dignity under authoritarian regimes.[608]

The horizontal effect of fundamental rights within the EU legal system has evolved significantly, with its foundations in early CJEU rulings that initially applied treaty provisions beyond state actions to include private entities.[609] This development emerged

[604] BVerfGE 7, 198, *supra.* The Lüth case concerned a politician who had opposed the distribution of the anti-Semitic film 'Jüd Jüss'. In particular, Lüth was ordered to pay compensation for the damage he had caused through his boycott activities. Following this decision, Luth appealed to the Constitutional Court complaining about the violation of his freedom of expression. The German Constitutional Court then addressed a question concerning the extension of constitutional rights in inter-private relations. On that occasion, the German court for the first time held that constitutional rights do not merely constitute claims of the individual against the state but form a set of values that apply in all areas of law by providing axiological guidance to the legislative, executive and judicial powers. In the present case, the protection of freedom of expression is not only developed vertically vis-à-vis the State but also horizontally, since the rules of civil law must be interpreted according to the spirit of the Constitutional Charter. For a comment in English of the case see Gert Brüggemeier, '6 Constitutionalisation of Private Law-the German Perspective', *Constitutionalisation of private law* (Brill Nijhoff 2006). On the freedom of expression implications, see Marco Bassini, *Internet e Libertà Di Espressione. Prospettive Costituzionali e Sovranazionali* (Aracne 2019).

[605] For a perspective on the influence of private actors in the application of AI, Wachter and Mittelstadt (n 129); Doshi-Velez and others (n 166).

[606] ECtHR [GC], *X and Y v the Netherlands*, n. 8978/80, 26 March 1985.

[607] Aurelia Colombi Ciacchi, 'The Direct Horizontal Effect of EU Fundamental Rights: ECJ 17 April 2018, Case C-414/16, Vera Egenberger v Evangelisches Werk Für Diakonie Und Entwicklung e.V. and ECJ 11 September 2018, Case C-68/17, IR v JQ' (2019) 15 European Constitutional Law Review 294; Oreste Pollicino, 'The Quadrangular Shape of the Geometry of Digital Power(s) and the Move towards a Procedural Digital Constitutionalism' (2023) 29 European Law Journal.

[608] Oreste Pollicino, 'L'efficacia Orizzontale Dei Diritti Fondamentali Previsti Dalla Carta La Giurisprudenza Della Corte Di Giustizia in Materia Di Digital Privacy Come Osservatorio Privilegiato' [2024] Rivista di Diritto dei Media - MediaLaws 1; Gonçalo de Almeida Ribeiro, 'The Effects of Fundamental Rights in Private Disputes' in Hugh Collins (ed), *European Contract Law and the Charter of Fundamental Rights*, vol 2 (Intersentia 2017).

[609] Lorenzo Cecchetti, 'Unravelling Horizontal Direct Effect in EU Law: The Case of the Fundamental Right to Paid Annual Leave between "Myth" and "Practice"' (2023) 42 Yearbook of European Law 42.

from cases like *Walrave and Koch*[610] and *Defrenne II*,[611], where the Court recognised that certain fundamental freedoms and anti-discrimination principles must apply universally to avoid creating inequalities in the internal market.[612] Specifically, in *Walrave and Koch*, the Court ruled that the prohibition of discrimination based on nationality applied to private entities, setting a precedent that private organisations could be bound by fundamental treaty provisions. This decision was grounded not in the wording of the Treaty but in the principle's "mandatory in nature" character, which required it to be applied uniformly across all legal relationships to ensure the effectiveness of EU fundamental freedoms.[613]

Building on this approach, the *Defrenne II* case extended horizontal direct effect by holding that the principle of equal pay for men and women could be invoked against private employers. The Court emphasised that this principle was not merely a directive to the Member States but a directly applicable right that underpinned individual claims.[614] The decision in *Defrenne II* relied on a teleological interpretation, prioritising the principle's purpose and significance in the Treaty's structure over formalistic arguments regarding its wording.[615] This substantive approach to the horizontal effect, which focuses on the intrinsic qualities and the essential role of certain norms, has continued to shape the Court's jurisprudence, allowing fundamental rights to be invoked against private parties where their omission would compromise key EU objectives.

Over time, this substantive approach expanded beyond non-discrimination principles to encompass fully-fledged fundamental rights under the EU Charter. A landmark

---

[610] ECJ, B.N.O. Walrave and L.J.N. Koch v Association Union cycliste internationale, Koninklijke Nederlandsche Wielren Unie and Federación Española Ciclismo, C-36/74, 12 December 1974. For a comment, see Richard Parrish, 'Case C-36/74 Walrave and Koch [1974] ECR 1405' in Jack Anderson (ed), Leading Cases in Sports Law (Springer 2013).

[611] ECJ, *Gabrielle Defrenne v Société anonyme belge de navigation aérienne Sabena,* C-43/75, 8 April 1976. One of the first comments on this famous case is O Stocker, 'Le Second Arret Defrenne. L'égalité de Rétribution Des Travailleurs Masculins e Des Travailleurs Féminin' [1977] Cahier de dr. Eur 180.

[612] As it is noted by Pollicino, id., "the enforcement *inter privatos* of the principle of non-discrimination on the basis of sex is instrumental in ensuring full and effective protection of human dignity, in this case, the dignity of Ms Defrenne, who was evidently injured by such blatantly discriminatory treatment".

[613] §28 of Walrave and Koch.

[614] §68 of Defrenne II, "even in the areas in which article 119 has no direct effect, that provision cannot be interpreted as reserving to the national legislature exclusive power to implement the principle of equal pay since, to the extent to which such implementation is necessary, it may be relieved by a combination of community and national measures".

[615] Cecchetti (n 609). Xenidis, in this respect, speak of a "constitutionalisation" by the Court of the principle of non-discrimination, Raphaële Xenidis, 'Shaking the Normative Foundations of EU Equality Law: Evolution and Hierarchy between Market Integration and Human Rights Rationales' (Social Science Research Network, 2017) <https://papers.ssrn.com/abstract=2925110> accessed 3 December 2024.

decision in this regard is the CJEU's ruling in *Egenberger*,[616], where the Court addressed the issue of the horizontal applicability of the right to equal treatment and non-discrimination based on religion or belief, as enshrined in Article 21 of the EU Charter. The case involved a dispute between Vera Egenberger, who applied for a position with a religious organisation, and the *Evangelisches Werk für Diakonie und Entwicklung eV*, which required applicants to adhere to a specific religious belief.[617] Egenberger argued that this requirement violated her right to equal treatment. The CJEU ruled that, although the Charter is traditionally binding on Member States and EU institutions, fundamental rights like non-discrimination could also be invoked in horizontal relationships, especially when they are expressed in EU legislation, such as Directive 2000/78 on equal treatment in employment.[618] The Court in *Egenberger* asserted that "the prohibition of all discrimination on the grounds of religion or belief is a mandatory general principle of EU law,"[619] applying broadly, including in relationships between private parties.[620] This judgment marked a significant step in expanding the horizontal effect of fundamental rights within the EU, establishing that private employers may be required to respect these rights even in the absence of explicit national legislation transposing EU directives.

This approach in *Egenberger* highlights the CJEU's commitment to ensuring that fundamental rights serve as a structural framework defining the EU's public order. The Court's reasoning underscores that fundamental rights in the EU Charter, particularly those related to dignity, equality, and fair treatment, establish a baseline of protection that transcends the traditional public-private divide.[621] This vision is indeed reflected in the *Egenberger* case, reinforcing the idea that rights protection must adapt to the realities of modern society, where private actors often play roles similar to public entities.

---

[616] CJEU, Case C-414/16, *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung e.V.* 17 April 2018. See, for a comment on the case, Ciacchi (n 607).

[617] §42-59 of the judgment hereby analysed.

[618] "[…] That prohibition, which is laid down in Article 21(1) of the Charter, is sufficient in itself to confer on individuals a right which they may rely on as such in disputes between them in a field covered by EU law", §76.

[619] Id. The principle hereby expressed was indeed confirmed by the CJEU in C-68/17 (Grand Chamber) *IR v JQ.,* 11 September 2018, §69.

[620] Eleni Frantziou, '(Most of) the Charter of Fundamental Rights Is Horizontally Applicable: ECJ 6 November 2018, Joined Cases C-569/16 and C-570/16, Bauer et Al' (2019) 15 European Constitutional Law Review 306.

[621] Legal scholar Dorota Leczykiewicz argues, "the horizontal application of fundamental rights is essential to promoting social justice in the EU, ensuring that private power does not undermine the foundational values of equality and dignity that the Union upholds." Leczykiewicz (n 594).

By prioritising the effectiveness of key principles necessary for the internal market and individual protections, the CJEU has embedded the horizontal effect as an essential aspect of EU law. In the digital age, where private entities wield considerable power, especially over data privacy and digital freedoms, this horizontal applicability of fundamental rights becomes even more crucial. The mandatory nature of certain rights, including data protection and non-discrimination, underscores the need for accountability across both public and private sectors, making impact assessments and compliance tools indispensable for enforcing these rights in the modern context.[622]

Moreover, the horizontal application of fundamental rights, particularly concerning privacy and data protection, has emerged as a critical theme in the EU's legal landscape.[623] Traditionally, rights such as privacy were enforced vertically, meaning individuals could only assert these rights against state actors.[624] However, in the digital age, where private companies often control large volumes of personal data, the CJEU has progressively extended the scope of data protection rights to apply horizontally, allowing individuals to claim their rights directly against private entities.[625] Landmark cases like *Digital Rights Ireland*, *Google Spain*,[626] and *Schrems* illustrate how privacy and data protection rights under Articles 7 and 8 of the EU Charter are increasingly recognised as enforceable against private entities.[627]

The *Schrems* case further cemented this horizontal effect by challenging the adequacy of data transfer agreements between the EU and the U.S. under the Safe Harbor

[622] On the impact of this provider in the mediation of rights, such as 'freedom of expression', see Balkin (n 111); Pollicino, 'Potere Digitale' (n 3).

[623] Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (n 181); Pollicino, 'L'efficacia Orizzontale Dei Diritti Fondamentali Previsti Dalla Carta La Giurisprudenza Della Corte Di Giustizia in Materia Di Digital Privacy Come Osservatorio Privilegiato' (n 596).

[624] This is indeed the original concept of 'privacy' as elaborated by Warren and Brandeis, as an extension of the 4th Amendment of the US Constitution. Warren and Brandeis (n 387). Specifically, on the concept of privacy as negative freedom see Bart van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data' (2014) 5 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 230.

[625] For this reason, scholars started to consider the 'judicial activism' of the CJEU in deciding cases on data protection. See Oreste Pollicino and Giuseppe Martinico, 'Between Constitutional Tolerance and Judicial Activism: The "Specificity" of the European Judicial Law'. Specifically, this holds true for the case, *infra*, acknowledged with the name *Google Spain.*

[626] CGUE, C-131/12, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González (2014).

[627] For a thorough analysis of the impact of the doctrine of the horizontal effect of fundamental rights analysed specifically on the three cases, see Pollicino, 'L'efficacia Orizzontale Dei Diritti Fondamentali Previsti Dalla Carta La Giurisprudenza Della Corte Di Giustizia in Materia Di Digital Privacy Come Osservatorio Privilegiato' (n 596).

framework, under which it was permitted the transfer of personal data between the two countries, through the digital platform at the time named Facebook. The Court ruled that the framework for the data transfer did not provide sufficient protections for EU citizens' data when handled by U.S. companies, leading to the annulment of Safe Harbor and the subsequent creation of the more stringent Privacy Shield – which was later invalidated as well. Thus, this decision emphasised the need for robust protections in transatlantic data flows and reinforced the expectation that private companies adhere to high data protection standards, regardless of jurisdiction, with the need to make such claims enforceable by the users against the platforms themselves.

These decisions further clarified the CJEU's objective: not only to enforce the EU's understanding of fundamental rights and safeguards concerning private actors within the EU but also to export and promote these standards internationally, particularly in the United States.[628] As a matter of fact, through these cases, the CJEU has effectively established that private companies are not merely processors of data but are obligated to respect fundamental rights related to privacy and data protection. This evolution aligns with the EU's recognition that digital rights, given their impact on human dignity and autonomy, require protection that transcends traditional boundaries between public and private sectors. Nonetheless, as the Court of Justice has consistently affirmed, fundamental rights "do not constitute unfettered prerogatives."[629] These rights must be balanced within their societal context and can be subject to limitations, provided that any interference is duly justified and does not infringe upon their essence.[630]

This principle applies equally to the deployment and reliance on AI technologies. Such technologies must operate within the legal boundaries established by the EU, respecting the essence of specific rights while ensuring that any restrictions are proportionate, necessary, and aligned with objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others (Article 52(1) CFREU).

Recognising the need for accountability in these contexts, the CJEU's jurisprudence lays the groundwork for regulatory mechanisms like impact assessments. Requiring both public and private entities to evaluate and mitigate the implications of their operations on

[628] Petkova (n 394).
[629] ECJ, *Nold KG v. Comm'n*, Case C-4/73, Judgment of 11 Jan. 1977, esp. §14.
[630] Takis Tridimas and Giulia Gentile, 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794.

fundamental rights through impact assessments, the horizontal enforcement of fundamental rights might be strengthened via the elaboration of a comprehensive structure of fundamental rights protection that underscores the EU's commitment to ensuring that rights such as privacy, equality, and human dignity are upheld across all areas of governance and private sector activities, creating a robust framework that bridges the public-private divide in fundamental rights protection. These assessments, which will be further analysed *infra,* including the Fundamental Rights Impact Assessment (FRIA) mandated under the AI Act, serve as both preventive and compliance tools, requiring public and private actors alike to consider the broader societal impacts of their operations. The FRIA's requirements highlight the EU's commitment to a holistic approach to rights protection, extending obligations beyond the state to include private companies that wield significant influence over individuals' rights.

4.3 Impact assessments as vessels of risks: a taxonomy

A fundamental rights-centered approach is essential in today's digital age to ensure that technology development respects individual freedoms, promotes equity, and safeguards societal trust. Therefore, to enhance the accountability of public and private actors and encourage decision-making that carefully considers risks to fundamental rights, this analysis will examine the approach to implementing impact assessments.

Impact assessment can be described as a "systematic process for analysing the potential effects or consequences of particular actions, projects, policies, or decisions".[631] By systematically assessing potential impacts, impact assessments serve as a tool to ensure that both public and private decisions prioritise the protection of specific interests at stake.[632] Therefore, impact assessments have emerged as practical options, acting as a bridge between the traditional regulatory oversight applied to public bodies and the new responsibilities faced by private actors. By requiring both public institutions and private companies to conduct evaluations of potential consequences on fundamental rights,

[631] Piergiorgio Chiara and Federico Galli, 'Normative Considerations on Impact Assessments in EU Digital Policy' [2024] MediaLaws.

[632] From a regulatory perspective, impact assessments allow policymakers to evaluate potential social, economic, and environmental consequences of new legislation before implementation, ensuring that proposed laws are designed to protect public interests and minimise risks. As compliance tools, impact assessments require private entities to analyse the impact of their own practices on individuals' rights, thereby enhancing accountability and aligning with regulatory standards. Gauthier de Beco, 'Human Rights Impact Assessments' (2009) 27 Netherlands Quarterly of Human Rights 139.

impact assessments formalise the expectation that private entities take proactive steps to safeguard rights. This evaluation, rooted in fundamental rights considerations, ensures that private actors, now tasked with substantial decision-making authority,[633] are held accountable, *lato sensu,* for the broader societal impacts of their operations while remaining a legal assessment. Especially, de Beco defines impact assessments as "the assessment of both the potential human rights impact of future policies and the actual human rights impact of implemented policies in a way ensuring the participation of various actors".[634]

Henceforth, impact assessment can be divided into two categories: 1) as included as part of a policy-making process or 2) as an instrument to regulate and enforce compliance.[635] As a matter of fact, impact assessments play a dual role as both regulatory and compliance instruments, each serving distinct yet complementary functions in the governance of AI and digital technologies.

Moreover, impact assessments might also be able to operationalise the horizontal protection of fundamental rights, embedding human rights considerations into the core of private sector practices. Through this regulatory mechanism, platforms and AI providers are not only required to be transparent about their processes but also to implement safeguards and provide redress mechanisms when rights are threatened.[636]

As policy-making tools, impact assessments enable legislators to evaluate the potential consequences of proposed policies and regulations, particularly regarding their impact on fundamental rights. For instance, in this context, the purpose of the assessment is to provide an understanding of the implications of a proposed policy in order to make an informed decision. This is an example of the so-called regulatory impact assessments (RIAs).[637] Regulatory impact assessments thus serve as preventive mechanisms, embedding considerations of fundamental rights directly into the policymaking process to reduce the risk of unintended harm. In this respect, the European Union (EU) has

[633] Oreste Pollicino, 'The Quadrangular Shape of the Geometry of Digital Power(s) and the Move towards a Procedural Digital Constitutionalism' (2023) 29 European Law Journal.
[634] Id.
[635] Chiara and Galli (n 631).
[636] de Beco (n 632).
[637] Renda (n 632); Claire A Dunlop and Claudio Maria Radaelli, *Handbook of Regulatory Impact Assessment / Edited by Claire A. Dunlop, University of Exeter, UK ; Claudio M. Radaelli, University of Exeter, UK* (Edward Elgar Publishing 2016). The first, complete procedure for assessing the costs and benefits of a proposed regulation was introduced in 1981 in the US, under Reagan's presidency.

pioneered a comprehensive approach to impact assessments, reflecting its commitment to responsible digital governance. Since the early 2000s, the EU has made impact assessments a cornerstone of its "Better Regulation" agenda, applying them to all significant legislative proposals.[638] More recently, in 2020, the European Commission presented a new Strategy to strengthen the application of the CFREU to ensure that all the strategies proposed are respectful of the fundamental rights framework.[639]

Thee second case regards the use of impact assessments used as regulatory and compliance instruments. This Chapter focuses specifically on this type of assessment.[640] The application of impact assessments for these purposes is not unique to AI; rather, it has roots in the 20th century, originating from virtuous initiatives undertaken by companies to promote accountability and ethical practices.[641] These self-regulatory approaches aims to go beyond mere legal compliance since, in this way, companies aim to demonstrate accountability, transparency, and ethical responsibility, especially in sectors with significant societal impact.

Historically, various forms of impact assessments have already been developed.[642] For instance, Environmental Impact Assessments (EIAs) became a common practice to gauge the environmental implications of projects.[643] Privacy Impact Assessments (PIAs), and

[638] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better regulation: Joining forces to make better laws, COM/2021/219 final; Felice Simonelli and Nadina Iacob, 'Can We Better the European Union Better Regulation Agenda?' (2021) 12 European Journal of Risk Regulation 849; Craig and Búrca (n 548). Particularly, under the EU context, the Regulatory Scrutiny Board is tasked with assessing the quality of impact assessments, evaluations and fitness checks (evaluations of legislation). The latest report has been published in February 2024, for the year 2023.

[639] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strategy to strengthen the application of the Charter of Fundamental Rights in the EU, Brussels, 2.12.2020.

[640] Diana-Maria Danciu, Laura Martens and Wim Marneffe, 'Assessing the Quality of European Impact Assessments' [2024] European Journal of Risk Regulation 1; Andrea Renda, 'From Impact Assessment to the Policy Cycle: Drawing Lessons from the EU's Better-Regulation Agenda' (2016) 9 SPP Technical Papers; Claire A Dunlop and Claudio Maria Radaelli, *Handbook of Regulatory Impact Assessment / Edited by Claire A. Dunlop, University of Exeter, UK ; Claudio M. Radaelli, University of Exeter, UK* (Edward Elgar Publishing 2016).

[641] Dunlop and Radaelli (n 637).

[642] For a taxonomy on the different types of impact assessment, please see Charles D Raab, 'Information Privacy, Impact Assessment, and the Place of Ethics' (2020) 37 Computer Law & Security Review 105404.

[643] A relevant example of EIA is Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment, later amended by Directive 2014/52/EU of the European Parliament and of the Council of 16 April 2014, amending Directive 2011/92/EU on the assessment of the effects of certain public and private projects on the environment. On this specific matter, John Glasson and Riki Therivel, *Introduction To Environmental Impact Assessment* (4th edn, Routledge 2013).

later DPIAs, emerged in the 1990s in countries like Canada, New Zealand, and Australia as tools initially used by public sector bodies and later adopted by private organisations.[644] These assessments were introduced to safeguard privacy-related interests and to demonstrate accountability. Over time, data protection impact assessments have evolved to be recognised as obligations as well as accountability measures under GDPR, demonstrating the broader responsibility organisations have in data protection beyond mere compliance.[645]

This growth of attention towards the use of impact assessment as a regulatory method is particularly interesting since it falls within the broader context of alternative regulatory models considered in the digital realm.[646] Besides the well-known dichotomy of hard law – and soft law, specific policy objectives for the digital sectors have been addressed so far through the use of co-regulatory initiatives.[647] These tools were evaluated by the European Commission as particularly useful for imposing specific obligations over online

[644] David Wright and Paul De Hert, 'Introduction to Privacy Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, vol 6 (Springer Netherlands 2012) <https://link.springer.com/10.1007/978-94-007-2543-0_1> accessed 3 December 2024.

[645] Eleni Kosta, 'Article 35 Data Protection Impact Assessment' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020); Massimo Marelli (ed), 'Data Protection Impact Assessments (DPIAs)', *Handbook on Data Protection in Humanitarian Action* (3rd edn, Cambridge University Press 2024).

[646] Michèle Finck, 'Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy' (Social Science Research Network, 20 June 2017) <https://papers.ssrn.com/abstract=2990043> accessed 3 December 2024.

[647] The EU's approach to using codes of conduct as a tool for co-regulation, particularly in the digital domain, reflects an effort to bridge gaps in regulatory frameworks where binding legislation may not yet exist or where enforcement proves challenging. This strategy is especially evident in the 2018 Code of Conduct aimed at combatting disinformation, which initially relied on self-regulation. However, as noted by Pollicino, the initial version was criticized for vague obligations and the lack of measurable indicators to assess platform accountability in content moderation efforts. To address these limitations, the revised Code introduced in 2022 incorporated more structured guidelines, measurable Key Performance Indicators (KPIs), and introduced the concept of Services Level Indicators (SLIs) to assess platforms' commitments. This shift represents a movement towards co-regulation, where private entities are encouraged to adhere to certain standards while engaging in dialogue with the European Commission. In this sense, the Digital Services Act (DSA) further institutionalizes this approach by recognizing codes of conduct as essential tools for co-regulation, with the potential for enforcement consequences if platforms fail to comply with these voluntary commitments. Oreste Pollicino, 'Asimmetrie Valoriali Transatlantiche Tra Self-Regulation, Hard Law e Co-Regolazione (Ovvero Sul Se e Sul Come Regolamentare Le Strategie Contro La Disinformazione on Line)' [2023] Osservatorio sulle Fonti; Giovanni DI COSIMO and others, 'L'impatto Delle Nuove Tecnologie Sui Processi Di Auto-e Co-Regolazione: Verso Uno Stato Di Diritto Tecnologico' <https://u-pad.unimc.it/handle/11393/279146> accessed 3 December 2024.

platforms since 2016,[648] and further evolved with the elaboration of the Strengthened Code of Practice on Disinformation.[649]

While initiatives such as codes of practice and codes of conduct have been introduced to combat disinformation and ensure that companies are held accountable for their actions, impact assessments do not diverge too much in terms of purpose and goals: to enhance corporate accountability.[650] However, what differs is the approach: instead of co-regulation through standardised codes, impact assessments rely on self-assessment, requiring companies to internally evaluate and address the potential impacts of their operations.[651] This shift from external codes to internal assessments reflects a move towards fostering accountability from within, empowering companies to take proactive responsibility for their influence on society and individual rights.

Secondly, impact assessments are more prone to "risk regulation",[652] meaning the understanding of the "combination of the probability of an occurrence of harm and the severity of that harm".[653] Saying it differently, risk regulations have the goal of shaping regulation by taking into consideration the impact of policies in terms of risks, indeed. Henceforth, it is to be distinguished between risk regulation – which broadly refers to governmental actions designed to manage and mitigate potential adverse consequences in social and market processes[654] – and risk-based approach, particularly evident in regulations like the GDPR, the AI Act, and the DSA. Each of these uses risk assessments

[648] European Commission, 'Communication on Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe' COM (2016) 288 final, 5 (hereafter European Commission, 'Communication on Online Platforms and the Digital Single Market').

[649] For an analysis of the code and its impact on tackling online disnformation, see Oreste Pollicino and Pietro Dunn, 'Disinformazione e Intelligenza Artificiale Nell'anno Delle Global Elections: Rischi (Ed Opportunità)' (2024) 12 Federalismi.

[650] It is not a case that both these models, code of conducts and impact assessments, are derived from the experience of the 'corporate social responsibility'. One of the most accurate definitions of the concept can be found in the Commission's Green Paper on Corporate Social Responsibility as 'a concept whereby companies integrate social and environmental concerns into their business operations and their interaction with their stakeholders on a voluntary basis'. Commission of the European Communities, Green Paper Promoting a European Framework for Corporate Social Responsibility, 2001. See, in part., Marco Fasciglione, 'An International Mechanism of Accountability for Adjudicating Corporate Violations of Human Rights? Problems and Perspectives' [2019] Judicial Power in a Globalized World: Liber Amicorum Vincent De Gaetano 179.

[651] This is the case, for instance of the EIA, when it is mandated for companies to evaluate the impact of their operations in the so-called "reports", as described by Damiano De Felice, 'Business and Human Rights Indicators to Measure the Corporate Responsibility to Respect: Challenges and Opportunities' (2015) 37 Human Rights Quarterly 511.

[652] Jonathan B Wiener, 'Risk Regulation and Governance Institutions' (OECD 2010).

[653] AI Act, Art. 3, para. 1, no. 2).

[654] Jeroen van der Heijden, 'Risk as an Approach to Regulatory Governance: An Evidence Synthesis and Research Agenda' (2021) 11 Sage Open.

to tailor compliance obligations based on the potential harm to individual rights and societal interest,[655] "striking a proportionate balance between risks and costs of regulation",[656] which is the purpose of the EU risk-based policies in the digital age. In this sense, impact assessments have a crucial role in promoting the adoption of frameworks of compliance that are based on the concrete 'threats' to the enjoyment of a particular right and, at the same time, are responsive to the potential risks.[657]

To conclude this brief overview, impact assessments function as indispensable tools for anticipating, identifying, and mitigating potential human rights impacts. They address a wide range of issues, from data privacy to non-discrimination, and are versatile enough to be implemented across sectors, including private organisations and government agencies. In recent years, the EU has increasingly relied on these instruments to solidify its dual approach to governance: fostering innovation while ensuring that fundamental rights, as enshrined in the EU Charter, are protected. This balanced approach is exemplified by the integration of impact assessments in the AI regulatory framework, where they play a central role in aligning technological development with European values, as the next sections will unpack.

4.3.1 Impact assessments in the international context

In recent years,[658] started to emerge at the global level with various proposals for conducting an impact assessment of human rights, more broadly, besides the renowned

[655] Pietro Dunn and Giovanni De Gregorio, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review; Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502.

[656] Dunn and Gregorio (n 207).

[657] This is, for instance, the case of the DPIA under the GDPR's risk-based regulatory framework. DPIAs require organisations to proactively identify, assess, and mitigate risks to individuals' rights and freedoms arising from data processing activities that are likely to result in high risks. This approach reflects the GDPR's principle of proportionality in compliance obligations, where regulatory requirements are tailored based on the level of risk posed by the data processing activity. By focusing on risk identification and mitigation, DPIAs enable organisations to implement safeguards that align with the GDPR's fundamental objectives of protecting privacy and ensuring accountability in data processing. Working Party Article 29, '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' (4 October 2017); Irene Kamara, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 European Journal of Law and Technology; Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, vol 6 (Springer Netherlands 2012).

[658] Raab (n 642).

examples in the environmental context, as mentioned *supra.* The significant example of the FRIA in the AI Act, as a matter of fact, stems from a broader framework for impact assessments that can be found in the Human Rights Impact Assessments (HRIA), which go beyond data protection[659] to consider a wide array of human rights potentially affected by AI.[660]

Unlike data protection-specific assessments like DPIAs, HRIAs are "instrument(s) for examining policies, legislation, programs and projects to identify and measure their effects on human rights".[661] In doing so, they embrace a holistic approach,[662] addressing a wide array of human rights potentially affected by a specific externality. For the sake of this research, the analysis is strictly focusing on the use of HRIA in the context of AI.

Therefore, the European Union's journey toward FRIAs is rooted in earlier regulatory and ethical initiatives. For instance, the Ethics Guidelines for Trustworthy AI, developed by the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), laid a foundational framework for AI governance. Published in April 2019, the Guidelines emphasised principles such as human autonomy, fairness, transparency, and the prevention of harm.[663] These principles were operationalised through seven key requirements for trustworthy AI, including privacy and data governance, societal and environmental well-being, and accountability. These principles paved the way for inserting the concept of human rights evaluation of AI impact, even though they lacked a clear operationalisation. Thus, the work of the HLEG rested on guidelines and did not go

[659] Alessandro Mantelero, 'Regulating AI' in Alessandro Mantelero (ed), *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (TMC Asser Press 2022).

[660] Céline Castets-Renard, 'Human Rights and Algorithmic Impact Assessment for Predictive Policing' in Amnon Reichman and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021).

[661] The World Bank, 'Study on Human Rights Impact Assessments A Review of the Literature, Differences with other Forms of Assessments and Relevance for Development', study commissioned by the Nordic Trust Fund, February 2013, available here <https://documents1.worldbank.org/curated/en/834611524474505865/pdf/125557-WP-PUBLIC-HRIA-Web.pdf>, accessed November 14, 2024.

[662] HRIAs developed in the late 1990s bear most resemblance to social impact assessments and are part of a wide-ranging family of impact assessment work. HRIAs enable an objective analysis of the ways and the extent to which a policy project, intervention, legislation or measure affects human rights, negatively or positively. See United Nations Human Rights Office of the High Commissioner, 'Taxonomy of Human Rights Risks Connected to Generative AI Supplement to B-Tech's Foundational Paper on the Responsible Development and Deployment of Generative AI', 2024.

[663] European Commission, 'Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence' COM (2019) 168 final. See also, more recently, the UNESCO, 'Ethical Impact Assessment. A Tool of the Recommendation on the Ethics of Artificial Intelligence' (2023).

further on creating a model for inserting the impact assessment on human rights in the AI life cycle.

At the same time, at the global level, started to emerge different propositions: e.g., Canada and the Netherlands have led the way in adopting robust HRIA frameworks, showcasing diverse methodologies for embedding human rights considerations into governance. Canada's Algorithmic Impact Assessment (AIA) tool,[664] developed[665] at the federal level, evaluates the societal impacts of automated decision-making systems used by government bodies. Similarly, Ontario's Human Rights AI Impact Assessment Tool[666] integrates broader human rights commitments by addressing potential algorithmic discrimination and ensuring alignment with national frameworks like the Canadian Charter of Rights and Freedoms. These tools underscore stakeholder engagement as a cornerstone of governance, ensuring that affected communities actively participate in decision-making processes.[667]

Another example comes from the Netherlands, where the Government applied a Fundamental Rights and Algorithms Impact Assessment (FRAIA) to map the risks envisaged while utilising AI systems in the public sector.[668] This framework, in particular, emphasises transparency, accountability, and stakeholder engagement, ensuring that AI systems align with fundamental rights, particularly in areas such as law enforcement and social welfare.[669]

---

[664] Government of Canada, 'Algorithmic Impact Assessment', <https://www.canada.ca/en/government/system/digital-government/digital-governmentinnovations/responsible-use-ai/algorithmic-impact-assessment.html>, accessed 11 November 2024. The tool, of a mandatory nature, is specifically built to support the Treasury Board's *Directive on Automated Decision-Making*. The tool is a questionnaire that determines the impact level of an automated decision system. It is composed of 51 risk and 34 mitigation questions. Assessment scores are based on many factors, including the systems design, algorithm, decision type, impact and data.

[665] The model is available at <https://open.canada.ca/aia-eia-js/?lang=en>, and the methodological note at <https://www.canada.ca/en/government/syst em/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html> accessed 11 November 2024.

[666] Law Commission of Ontario and Ontario Human Rights Commission, 'Human Rights AI Impact Assessment', November 2024. Differently from the previous one, "this tool is relevant and applicable to any organization, public or private, intending to design, implement, or rely on an AI system" (p. 5). Hence, it has a scope of application that is broader in the intention and the actors.

[667] Heleen Janssen, Michelle Seng Ah Lee and Jatinder Singh, 'Practical Fundamental Rights Impact Assessments' (2022) 30 International Journal of Law and Information Technology 200; Chiara and Galli (n 631).

[668] Ministry of the Interior, The Netherlands, 'Impact Assessment Fundamental rights and algorithms', March 2022.

[669] Here is an analysis of the pilot project of the Province of Friesland, Rijks ICT Gilde-part of the Ministry of the Interior and Kingdom Relations (BZK) (both in The Netherlands) and a group of members of the Z-Inspection® Initiative. Marjolein Boonstra and others, 'Lessons Learned in Performing a Trustworthy AI

Finally, the Danish Institute for Human Rights elaborated guidance and a toolbox for industries in conducting an HRIA in the corporate context, focusing on identifying, mitigating, and addressing human rights impacts in business operations.[670] The guidance emphasizes participatory approaches and aligns with the UN Guiding Principles on Business and Human Rights.

In general, all these frameworks stand out for their commitment to 'multistakeholderism' and accountability, engaging human rights experts, policymakers, and impacted communities to address risks comprehensively. However, they also reveal significant variations in their scope, methodologies, and implementation practices. For instance, while some models, such as the Dutch HRIA framework, emphasise participatory governance and continuous monitoring, others, like Canada's AIA, lean more toward procedural compliance with structured checklists. Furthermore, certain frameworks prioritise specific rights, such as privacy or non-discrimination, while others adopt a broader, more holistic approach, addressing societal and ethical considerations alongside legal requirements, like the HLEG Guidelines. These differences highlight the challenges of harmonising human rights protections across diverse regulatory and cultural landscapes, raising questions about the scalability and adaptability of these frameworks in a rapidly evolving technological context.

Building on these international examples, the Council of Europe, together with the elaboration of the Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law,[671] a principle-based document aimed at fostering international consensus, also started to work, together with the Alan Turing Institute on the elaboration of its own "branded" impact assessment method, HUDERIA (Human Rights, Democracy, and the Rule of Law Impact Assessment).[672] Only on 28 November 2024, the Committee on Artificial Intelligence (CAI) eventually published its 'HUDERIA

---

and Fundamental Rights Assessment' (arXiv, 22 April 2024) <http://arxiv.org/abs/2404.14366> accessed 17 November 2024.

[670] Danish Institute for Human Rights, 'Human rights impact assessment guidance and toolbox', available here <https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox>, accessed 11 November 2024.

[671] See Chapter 2 of this thesis, and, specifically for a comparison with the EU framework, Francesco Paolo Levantino and Federica Paolucci, 'Advancing the Protection of Fundamental Rights Through AI Regulation: How the EU and the Council of Europe Are Shaping the Future' (27 June 2024).

[672] The Alan Turing Institute, 'Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems: A proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence' (2021) 46-49 and 72-125.

Methodology', which however is described as a "stand-alone, non-legally binding guidance" that neither carries legal or mandatory effects nor serves as "interpretive aid" for the Framework Convention.[673] Nonetheless, the CoE's approach, unlike general HRIA methodologies, integrates a multidimensional methodology by combining the evaluation of human rights, democracy, and the rule of law into a cohesive framework tailored to AI governance. With its emphasis on ex-ante impact assessments, stakeholder engagement, and algorithmic transparency, HUDERIA is particularly suited to high-stakes applications such as public administration and criminal justice.[674] This approach reflects the Council of Europe's commitment to balancing technological innovation with the preservation of democratic principles.[675] Hence, HUDERIA's inclusion of democratic accountability and institutional oversight distinguishes it from frameworks like Canada's AIA, which relies heavily on procedural tools, or the Netherlands' participatory models, which focus on societal inclusion. By incorporating a broader perspective that examines societal impacts and potential democratic erosion, HUDERIA bridges the gap between ethical considerations and legal mandates.[676]

Nevertheless, the need for multidimensional impact assessments in AI governance reflects an acknowledgement of the technology's complexity and the diversity of its

[673] CAI, Methodology for the risk and impact assessment of Artificial Intelligence systems from the point of view of Human Rights, Democracy and the Rule of Law (HUDERIA Methodology), CAI(2024)16rev2, 28.11.2024. at p. 3.

[674] Specifically, the aims of the HUDERIA are three: 1) to improve upon the fragmented character of the the current state of knowledge in AI technology policy by integrating distinctive tasks of risk analysis, stakeholder engagement, impact assessment, risk management, impact mitigation, and innovation governance into a coherent and integrated whole; 2) to ensure a risk-based and proportionate approach to impact assessment that responsibly optimizes agility and innovation across the AI ecosystem by not creating excessive administrative burdens; 3) to take a sufficiently procedural approach to formulating the base-line requirements of the methodology so to safeguard a significant margin of appreciation for the unique circumstances of domestic authorities, which are better placed to make relevant policy and regulatory choices, taking into account their country's specific political, economic, social, cultural, and technological contexts. Committee on Artificial Intelligence (CAI), 'Outline Of HUDERIA Risk And Impact Assessment Methodology', CAI-BU(2022)03, 17 May 2022.

[675] Chiara and Galli (n 77); Alessandro Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template'.

[676] The list is not exhaustive but is the most representative set of frameworks on the HRIA applied to AI. It is to mention, from an academic level point of view, the methodology proposed by Mantelero. He created the HRESIA (Human Rights, Ethical, and Social Impact Assessment) model, which seeks to transcend traditional HRIA frameworks by incorporating ethical and social values alongside human rights considerations. Unlike conventional assessments, HRESIA employs an *ad hoc* committee of experts to contextualise rights and values based on specific socio-technical conditions and local dynamics. This approach allows for a deeper exploration of conflicting interests, enhancing the robustness of impact assessments. See Alessandro Mantelero, 'Human Rights Impact Assessment and AI' in Alessandro Mantelero (ed), *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (TMC Asser Press 2022).

potential impacts. Unlike traditional regulatory assessments, AI impact assessments are often iterative, requiring periodic re-evaluation as technologies evolve and as new risks emerge. This iterative nature allows for adaptive governance, where assessments can respond dynamically to the rapidly advanced characteristics of AI technologies. Hence, it is not a chance that most of them reiterate concepts like fostering accountability, transparency, and ethical responsibility.[677]

Therefore, the lessons learned from HRIA and HUDERIA provide critical groundwork for understanding the EU's introduction of FRIA under the AI Act. While HRIA frameworks broadly assess societal and human rights impacts, FRIA specialises in evaluating high-risk AI systems' alignment with the EU Charter of Fundamental Rights.

Unlike HUDERIA's expansive focus on democracy and governance, FRIA zeroes in the protection of fundamental rights such as privacy, non-discrimination, and access to justice within a structured regulatory framework.

The European Union Agency for Fundamental Rights (FRA) has long emphasised the need for such assessments.[678] This marks a critical shift toward embedding rights considerations into AI governance. As the EU transitions from guidelines to the imposition of FRIA, these global and regional frameworks provide a valuable foundation for operationalising fundamental rights in the digital era. Nonetheless, FRIAs build upon the participatory governance and accountability principles central to HRIA while addressing the unique regulatory challenges posed by high-risk AI applications in the context of the CFREU.

4.4 The Fundamental Rights Impact Assessment

The FRIA, as mandated by Article 27 of the AI Act, is a pivotal component of the EU's regulatory approach to governing AI. As anticipated, it is a specialised framework designed to ensure that high-risk AI systems comply with fundamental rights as enshrined in the CFREU. Therefore, "in order to efficiently ensure that fundamental rights are

[677] Bryson (n 89); Yeung, 'Constitutional Principles in a Networked Digital Society' (n 42); Smuha and Yeung (n 151).

[678] In its 2020 report, "Getting the Future Right – Artificial Intelligence and Fundamental Rights," the FRA identified risks associated with predictive policing, medical diagnostics, and social services, highlighting the importance of conducting fundamental rights impact assessments to mitigate harm, together with emphasising the need for an impact assessment that takes into consideration the precise risks on fundamental rights.

protected",[679] the FRIA has a more specific application than broader frameworks like the Human Rights Impact Assessments (HRIAs), which assess a wide range of rights across international contexts. Indeed, the FRIA is specifically tailored to the EU legal framework and focuses on evaluating the direct and indirect implications of AI on fundamental rights. Therefore, due to its more tailored and regionally specific focus, the FRIA framework stands out as a potentially effective tool for addressing the unique challenges posed by artificial intelligence applications within the European Union. Embedding fundamental rights protections into the governance and deployment of AI systems, it holds the promise – at least on paper – of not only identifying but also mitigating risks in practice, thereby ensuring alignment with EU values and legal standards.

This instrument was not originally included in the AI Act but was introduced later during the deliberations and amendments made by the European Parliament, [680]and represents an advancement in making the AI Act a Regulation less product-oriented, and more prone to the protection of fundamental rights.[681] Specifically, this assessment is a rights-based one, meaning that the deployer is asked to consider the risks that an AI system may pose by pondering every right in the Charter of Fundamental Rights of the European Union (CFREU), especially those "in the areas of education, healthcare, social services, housing, administration of justice".[682]

---

[679] AI Act, Rec. 96.

[680] The introduction of the FRIA into the AI Act reflects a convergence of calls from various civil society organizations, international initiatives, and institutional opinions advocating for stronger human rights safeguards in AI governance. In this respect, see the 'Open Letter', drafted and coordinated by the Civil Liberties Union for Europe (Liberties), the European Civic Forum (ECF), and the European Center for Not-for-Profit Law (ECNL), available here <https://www.statewatch.org/news/2023/september/civil-society-calls-on-legislators-to-ensure-the-ai-act-upholds-the-rule-of-law/>, accessed 3 December 2024.

In particular, civil society groups, alongside the international momentum highlighted earlier, consistently emphasised the need for a dedicated framework to assess and mitigate the fundamental rights risks posed by high-risk AI systems. Moreover, the joint opinion of the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) drew attention to the FRA guidelines (*supra)*, underscoring the importance of aligning AI governance with established fundamental rights frameworks. See, 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)', 18 June 2021, in part. p. 9-10. These efforts culminated in significant amendments proposed during the European Parliament's deliberations, such as Amendment 622, which outlined the essential elements of a FRIA, including its purpose, scope, and focus on marginalized and at-risk groups. Similarly, Amendment 1671 introduced Article 9a, further institutionalizing the FRIA's role within the AI Act, initially linked to Article 9 provisions but later expanded to address high-risk systems comprehensively. The author, in part., refers to Amendments 310- 538 to the 'Harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, Proposal for a regulation', in the Draft report curated by Brando Benifei and Dragoş Tudorache, IMCO-LIBE committees, 13.6.2022.

[681] Palmiotto, 'The AI Act Roller Coaster' (n 303).

[682] AI Act, Art. 27, to be read together with Art. 1, Rec. 93 and 96. The quote comes from Rec. 96.

Therefore, the analysis that follows breaks down every element of Art. 27 to deeply understand the application of this crucial requirement under Regulation (EU) 2024/1689.[683]

4.4.1 The actors

The AI Act, being first and foremost a Regulation oriented to the specific use of a product, better AI, focuses indeed, but not exclusively, on who utilises the product. Therefore, FRIA is mandatory for developers of high-risk AI systems, including essential requirements and due diligence obligations distributed between providers (hence, developers) and deployers. Providers are tasked with ensuring compliance with essential requirements and undergoing relevant conformity assessments,[684] while deployers must adhere to provider instructions and conduct a FRIA prior to deploying high-risk AI systems.[685] This obligation applies to three key categories of actors: 1) deployers governed by public law, such as public authorities, like law enforcement using face recognition; 2) private operators providing public services, including education, healthcare, social services, housing, and justice administration;[686] 3) operators deploying high-risk AI systems intended for creditworthiness evaluation, credit scoring, or risk assessment and pricing in life and health insurance contexts, as per Annex III AI Act, points 5, lett. b) and c). By mandating FRIAs for these actors, the AI Act emphasises the importance of anticipating and mitigating risks to fundamental rights before deploying high-risk AI technologies.

4.4.2 Time and modalities

The FRIA must be performed prior to the initial deployment of the high-risk AI system and should be continued during the whole AI life cycle.[687] This entails a thorough

[683] AI Act, Art. 27 para. 1, lett. a).
[684] AI Act, Art. 43.
[685] AI Act, Rec. 96.
[686] Note that even though art. 27 para. 1 is vague in defining this category, Rec. 96 specifies that it is mandated to perform a FRIA also, "services important for individuals that are of public nature may also be provided by private entities. Private entities providing such public services are linked to tasks in the public interest such as in the areas of education, healthcare, social services, housing, administration of justice".
[687] AI Act, Rec. 96, "Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the

evaluation of the system's potential to adversely affect fundamental rights. For this reason, deployers may rely on previously conducted assessments, including those provided by the system's developer, provided the system's context of use remains unchanged.[688] However, should any significant modifications arise during the system's use, such as changes in its purpose, affected populations, or identified risks, the deployer is obligated to update the assessment to reflect the new circumstances.[689]

4.4.3 Key elements

The assessment must comprehensively address the following aspects:

- System use and purpose: a detailed description of how the AI system will be integrated into the deployer's processes, ensuring alignment with its intended purpose.
- Operational parameters: an outline of the timeframe and frequency of the system's deployment.
- Affected Individuals and Groups: an identification of the categories of natural persons and communities likely to be impacted by the system, particularly marginalised or vulnerable groups.
- Risk analysis: a detailed evaluation of specific risks of harm that may arise from the system's use, with reference to information provided by the developer in compliance with Article 13 of the AI Act.
- Oversight and governance: a description of the human oversight measures that will be implemented, following the developer's guidelines.
- Mitigation measures: strategies to address the materialisation of identified risks, including internal governance mechanisms and accessible complaint procedures.

From the breakdown of the essential requirements, there emerges a potential information asymmetry between deployers and providers: much of the information hereby requested, such as the operational parameters must be shared by the provider with

provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the persons or groups of persons likely to be affected, including vulnerable groups.".

[688] AI Act, Art. 27 para. 2.

[689] Id.

the deployer in order to make the assessment work. As noted by scholars, "providers possess key knowledge about system properties and technical limitations, impacting risk assessments from during deployment".[690] Therefore, a crucial element, even though not specifically listed in the AI Act formulation, is indeed that of a collaboration between the provider and the deployer. As it will be further highlighted *infra,* the assessments that respectively these actors are requested to perform – the FRIA in the case of the deployer and the risk management system, in the case of the provider – will serve their purpose only if integrated together, as also suggested by Art. 13 of the AI Act.

This collaborative approach is particularly critical in scenarios such as the use of FRT by law enforcement authorities. Given that providers are often private entities, effective collaboration and coordination between these private actors and public authorities are essential to ensure a thorough and coherent assessment.

Moreover, the success of these assessments relies heavily on the transparency and reliability of the information exchanged. Providers must supply accurate and comprehensive data regarding the design, functionality, and potential risks of the AI systems, enabling deployers to evaluate their broader societal and rights-based impacts effectively. This mutual reliance underscores the importance of trust and accountability in the assessment process, ensuring that both parties contribute to safeguarding fundamental rights while maintaining the system's intended purpose.

4.4.4 Procedural obligations

Once the FRIA is completed, deployers are required to notify the relevant market surveillance authority, submitting the assessment results through a standardised template. The AI Office is tasked with developing this template, which may include an automated tool to streamline compliance. Public sector deployers may, in certain circumstances, be exempt from this notification obligation, as outlined in Article 46 para. 1 of the AI Act; therefore, in case of "public security or the protection of life and health of persons, environmental protection or the protection of key industrial and infrastructural assets", the Market Surveillance Authority can authorise the placing on the market or the putting into service of specific high-risk AI systems, even though the *ex ante* procedure has not been completed yet.

[690] Chiara and Galli (n 631).

4.4.5 Data Protection Impact Assessments: friend or foe?

One of the core elements of Art. 27 of the AI Act is its necessary integration with other impact assessments present in other digital regulations of the EU, as §4.4.6 will further highlight. Such a link is further reinstated by Art. 27 para, 4, where it establishes that

> "If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment".

Therefore, when a DPIA[691] has been conducted under the General Data Protection Regulation (GDPR) or Directive (EU) 2016/689, the FRIA should complement, rather than duplicate, that assessment. Even though, this is a positive aspect from an objective – since it means that the FRIA extends the border beyond data protection concerns, encompassing broader fundamental rights considerations, such as non-discrimination, equality, and access to justice, to align with the AI Act's objective of safeguarding fundamental rights comprehensively – and methodological perspective – since it will be possible to build the creation of the FRIA methodology on the consolidated framework of the DPIAs – it has a crucial drawback with respect to understanding who must comply with these obligations.

Henceforth, Art. 27 establishes that, in case the deployer needs to perform a DPIA, the fundamental rights impact assessment referred to shall complement it. Hence, the two compliance measures will be mixed up. Thus, if a deployer is classified as a "data controller", meaning the subject that determines the purpose and the meaning of the processing under data protection law, it is also responsible for conducting the DPIA under Article 26 par. 9 of the AI Act. Instead, the provider is regarded as a "data processor", being the subject who processes data on behalf of the controller.[692] Differently, if a

[691] See Chapter 3, §3.6.1.

[692] EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR', 7 July 2020; Article 29 WP, 'Opinion 1/2010 on the concepts of "controller" and "processor"', 00264/10/EN, WP 169, 16 February 2010.

provider is portrayed as having real control over an AI system, as with foundation models, data protection authorities would consider the provider as a data controller or potentially a joint controller with the entity deploying the AI system. However, if the provider is perceived as having significant control over the AI system, its classification under GDPR may be altered. Being labelled as a data controller or joint controller comes with additional responsibilities and obligations under data protection laws.[693]

There is no cutting-edge answer as to what degree of control of the AI system the provider must have to be considered a data processor.

This issue reflects future challenges of the compatibility of the AI Act with the existing laws and remedies under EU and national laws. This clarification is crucial to establish legal certainty and to understand the distribution of responsibilities among different entities involved in data processing. This clarity is seen as necessary not only to uphold the principle of legal certainty but also to specify the duties of the involved parties and to ensure the protection of individual rights – i.e., Articles 15-22 of the GDPR.[694]

As we delve into comparisons with existing tools, such as the GDPR's Data Protection Impact Assessment and the risk assessment requirements under the Digital Services Act, it becomes clear that while the FRIA represents an incremental improvement, it does not yet signify a transformative shift in addressing the specific challenges posed by AI.

4.4.6 Impact assessments: drawing parallels

Due to the mentioned issues, the FRIA must also be seen in conjunction with other regulatory frameworks like the DPIA under the GDPR and the risk assessments required by the Digital Services Act (DSA).[695] The overlapping nature of these assessments could lead to confusion among deployers, especially when AI systems affect both data protection and content moderation.

The DPIA,[696] required under the GDPR, serves as a mechanism to assess risks associated with the processing of personal data, focusing on the protection of privacy and

[693] As noted by the EDPB, *supra,* the importance of this distinction lies in the fact that there different and distinctive compliance measures characterising the processor and the controller.

[694] Issues that are not new in the data protection panorama, but that risk to be further reinforced by the use of AI systems. See, Gabriela Zanfir-Fortuna, 'Article 15 Right of Access by the Data Subject' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[695] Chiara and Galli (n 631).

[696] GDPR, Art. 35.

data security. DPIAs emphasize human oversight, particularly in cases where automated decision-making processes impact individuals' data rights, ensuring that the balance between innovation and fundamental rights is maintained.[697] The message is quite simple: if you use automated decision-making systems, this activity is risky and should be detailed in the DPIA.

In contrast, the FRIA starts from the premises of a broader approach by assessing risks posed by AI systems to fundamental rights; however, as mentioned, it struggles to fully grasp the unique risks posed by the autonomy of AI systems, which may affect fundamental rights in ways that extend beyond traditional data protection concerns covered by the DPIA. The shift from focusing solely on individual rights to broader societal impacts requires a more stringent and transparent framework, one that FRIA currently lacks.

The Risk Assessment under the DSA further expands the regulatory scope by focusing on systemic risks posed by VLOPs, particularly those involving automated content moderation and the spread of illegal content.[698] More importantly, the DSA contains a list of the CFREU's rights to be considered by the platform when conducting the assessment.[699] Henceforth, it is much more precise than the FRIA, it excludes the issues related to the horizontal application of fundamental rights and does not pose a duty to such actors in identifying the risks alone.

The purpose, method and structure are the main shortcomings that make the FRIA a more complete tool in power, but in practice not very easy to handle, imposing a great organisational effort on deployers.

These three impact assessments, while designed for different regulatory contexts, reflect a common regulatory trend in the EU: an over-reliance on risk-based categorization and self-regulation. This approach often lacks the rigour needed to address the specific challenges posed by highly autonomous systems, particularly AI. Furthermore, the AI Act and DSA's frameworks, while recognizing the need for human oversight, often treat the human factor as peripheral, emphasizing potential harms without adequately ensuring that human judgment remains integral to decision-making processes.

[697] GDPR, Art. 35, para. 3, lett. a).
[698] DSA, Art. 34.
[699] DSA, Art. 34, para. 1, lett. b).

As the Chapter transitions into a deeper analysis of the FRIA applied to the case study of this thesis, the comparison is highlighted by the table, *infra.*

Table 6 – Impact assessments comparison.

Aspect	DPIA (GDPR, Article 35)	RA (DSA, Article 34)	FRIA (AI Act, Article 27)
Scope and purpose	Focuses on data protection and privacy risks related to personal data processing.	Addresses risks of very large online platforms, including content moderation and algorithmic systems.	Focuses on fundamental rights impacts, especially for high-risk AI systems used in public and private services.
Key elements	Evaluates necessity, proportionality, risks, and includes consultation with a DPO.	Assesses systemic risks such as illegal content dissemination and impacts on democratic processes.	Evaluates impacts on the fundamental rights of the CFREU, and only for some high-risk systems.
Human in the loop	Strong emphasis on human oversight, with mandatory human review of automated decisions.	Balances automation in content moderation with transparency and accountability through human review processes.	Acknowledges human oversight in high-risk AI but lacks clear mechanisms for ongoing supervision and operationalization.
Remedies and accountability	Provides individual remedies for data protection violations, with judicial and administrative redress.	Focuses on procedural accountability for platforms, with mechanisms for user appeals and risk mitigation.	Emphasizes systemic safeguards and risk management but lacks robust individual remedies and relies on self-assessment.
Constitutional principles	Classical constitutionalism focused on privacy, human dignity, and proportionality.	Procedural constitutionalism emphasizing transparency, fairness, and platform accountability.	New phase of digital constitutionalism grappling with AI's autonomy. Emphasis is placed on identifying potential harms, but less attention is given to proposing concrete solutions or operationalizing human oversight.

The table highlights the EU's incremental approach to managing the complexities of automation and AI through different legislative tools: the DPIA, the DSA's risk assessment, and the FRIA. Each of these instruments reflects varying levels of maturity in the way they deal with risk management, human oversight, and the protection of fundamental rights.

While the DPIA revolves around the necessity and proportionality of personal data processing in the context of privacy, it limits its focus to privacy–data protection concerns. The DSA's risk assessment, on the other hand, expands this scope, targeting systemic risks tied to platforms, including concerns over illegal content and democratic processes. While both the DPIA and DSA's risk assessment involve human oversight, their reliance on risk management principles positions them as procedural safeguards rather than tools ensuring substantive oversight of automated decisions.

The FRIA takes the conversation forward by acknowledging AI's ability to affect a broad spectrum of fundamental rights beyond just data privacy, such as non-discrimination and bias. However, despite its wider mandate, the FRIA's dependence on self-assessment, lack of individual remedies, and absence of a strong, built-in human supervisory framework bring it closer to the DPIA and DSA's risk assessment. These gaps raise concerns about the practical enforceability of fundamental rights protections, particularly in high-risk AI applications.

Although the FRIA's conceptual scope is broader, in practice, it faces similar limitations as its predecessors, necessitating stronger oversight mechanisms to truly address the challenges posed by autonomous AI systems. Thus, while the FRIA represents a significant regulatory advance, this comparison underscores a critical gap in ensuring ongoing, robust human involvement. Without clear enforcement and operationalization mechanisms, these assessments may fall short of offering the comprehensive governance needed in today's AI-driven digital landscape. There is a need for an integrated approach that ensures AI technologies are properly scrutinized, with human involvement playing a central, proactive role rather than a mere procedural one. This broader perspective sets the stage for further analysis, particularly the need for impact assessments to not only anticipate risks but also offer specific safeguards and remedies, especially in areas where AI autonomy has direct consequences for fundamental rights.[700]

[700] Palmiotto, 'The AI Act Roller Coaster' (n 303).

4.4.7 The other assessments under the AI Act

Having analysed the framework within the FRIA should be analysed in the context of the EU digital regulations, this section is further confronting this tool with the other provisions in the AI Act requiring an evaluation of risks to fundamental rights.[701]

Essentially, rticle 9 establishes a risk management system[702] as a core requirement for all high-risk AI systems, emphasising the identification and mitigation of risks to health, safety, and fundamental rights.[703] Whereas, article 43's conformity assessment[704] ensures compliance with the AI Act's requirements through external validation "in order to ensure a high level of trustworthiness of high-risk AI systems".[705]

As mentioned, the FRIA is a targeted assessment specifically applied to certain high-risk AI systems deployed by public bodies, private entities providing public services, or operators involved in high-stakes applications, such as credit scoring or health insurance. In contrast, Article 9 applies universally to all high-risk AI systems, covering risks across health, safety, and fundamental rights during the design and development phases.[706] Article 43, meanwhile, focuses on compliance at the pre-market stage, ensuring the system meets essential requirements for lawful deployment.[707]

---

[701] See Chapter 2, specifically, §2.4.7-2.4.10.

[702] The definition of a risk management system is a process that "specifies how providers of high-risk AI systems must identify, assess and respond to risks", cit. Schuett (n 275).

[703] AI Act, Art. 9, para. 2: ". The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;
(b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
(c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
(d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a)."

[704] A conformity assessment, in particular, is "a legal obligation, which must be fulfilled before a high-risk AI system is placed on the market. It aims at fostering accountability of AI providers", cit. Thelisson and Verma (n 323). It is also proposed, in literature, a system of conformity assessment that establish "a procedure to implement ethics-based auditing", as in Luciano Floridi and others, 'capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act' (Social Science Research Network 2022).

[705] AI Act, Rec. 123.

[706] AI Act, Rec. 65.

[707] AI Act, Rec. 125, "however, given the current experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products".

In terms of actors that are responsible for complying with the obligations, the FRIA places responsibility on deployers – entities deploying the AI system in real-world contexts. These deployers must consider risks specific to the operational setting, including impacts on marginalised groups. Conversely, risk management under Article 9 is the obligation of providers that incorporate risk identification and mitigation measures into the system's design, adhering to essential requirements.[708] Conformity assessment under Article 43, however, often involves third-party notified bodies, ensuring an independent review of compliance with the AI Act before the system can be marketed or used.[709]

Providers under Article 9 may adhere to harmonised standards to fulfil their risk management obligations. These standards, while voluntary, offer structured methodologies for compliance.[710] Conversely, the FRIA requires a context-specific assessment tailored to the intended use of the system. Deployers must evaluate how the system will function in its specific deployment environment,[711] including risks to privacy, non-discrimination, and human oversight. Article 43's conformity assessment, by contrast, focuses on verifying compliance with the Act's essential requirements through standardised testing and certification processes.

The interplay between providers and deployers highlights a significant information asymmetry. Providers possess technical knowledge about the system's design and limitations, which they disclose under Article 13. Deployers can and should rely on this information to perform their FRIA but also contribute unique insights from the deployment context, identifying risks specific to operational scenarios. This feedback loop requires deployers to inform providers of emerging risks or incidents, enabling providers to update their risk management systems and improve compliance mechanisms.

The following grid aims at comparing the different assessments of the AI Act.

---

[708] AI Act, Art. 9, para. 5, specifies that identifying the essential requirements for performing the risk management system are "(a) elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system; (b) where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated; (c) provision of information required pursuant to Article 13 and, where appropriate, training to deployers. With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used".

[709] Id.

[710] AI Act, Rec. 61. For the role of standards in the AI Act, see Mélanie Gornet and Winston Maxwell, 'The European Approach to Regulating AI through Technical Standards' (2024) 13 Internet Policy Review.

[711] AI Act, Rec. 93, "Deployers […] can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use […]".

Table 7 – Comparison between the FRIA, risk management system and conformity assessment.

Aspect	Art. 27, FRIA	Art. 9, RMS	Art. 43, CA
Objective	To assess the impact of deploying high-risk AI systems on fundamental rights in specific contexts.	Manages broader risks to health, safety, and fundamental rights posed by high-risk AI systems.	Verifies compliance with all essential requirements of the AI Act.
Legal framework	Applies only to high-risk AI systems as defined in Article 6(2), excluding some areas like Annex III (point 2). Focused on systems used by public bodies or private entities in public services.	Part of the AI Act's requirements for high-risk AI systems.	AI Act-specific compliance process, often conducted by a third party.
Actors	Deployers (e.g., public bodies or private entities providing public services).	Providers of high-risk AI systems throughout the lifecycle.	Third-party notified bodies or, in some cases, the provider itself.
Timing	Performed prior to the use of a high-risk AI system and updated as needed during its lifecycle.	Ongoing and iterative throughout the system lifecycle.	Conducted before the system is placed on the market or put into service.
Outcome	Comprehensive report detailing risks, mitigation measures, and human oversight strategies; notification to market surveillance authority required.	Reduction of risks to health, safety, and fundamental rights to an acceptable level.	Certification or declaration of conformity, enabling market placement.
Focus on Fundamental Rights	Indirectly addresses fundamental rights by focusing on data protection as a component.	Directly addresses fundamental rights alongside other risks.	Evaluates compliance with essential requirements, including those related to fundamental rights.

Despite their differences, the FRIA, risk management system, and conformity assessment are highly complementary. The merge of this instrument, as also mentioned in §4.4.3, is a goal that must be pursued while enforcing the AI Act.

Together, they reflect the layered regulatory approach of the AI Act. Essentially, as the analysis that precedes and the grid highlights, there is no repetition of instruments or doubling of the efforts, but, instead, these obligations return the picture and the frame of the different roles served by the provider and the deployer. Therefore, if, on the one hand, the provider "develops an AI system or a general-purpose AI model […] and places it on the market or puts the AI system into service"[712], and, consequently, has access to the information related to the programming of the system and its 'technical' assessment, on the other hand, the deployer, "using an AI system under its authority",[713] is in the best-placed position for conducting an assessment based on fundamental rights. Deployers are intimately involved in the operational context, including the specific purposes, reasons, and environments in which the system is deployed. This vantage point makes the deployer better equipped to evaluate the real-world implications of the AI system on fundamental rights, including its potential effects on individuals or groups, as well as the risks of harm or incidents arising from its use.

Such an assessment cannot remain theoretical. While the provider's role is critical in designing a system that is ostensibly neutral and safe from a technical perspective, it is the deployer who must assess how the system interacts with specific operational contexts, societal factors, and populations. The provider cannot fully anticipate the ways in which an AI system will be used or the nuanced risks that may emerge during deployment. Consequently, the FRIA is indispensable at this stage, as it addresses the unique and context-specific risks that only the deployer can evaluate. This division of responsibilities ensures a more comprehensive regulatory approach, balancing technical oversight with practical accountability. By aligning the provider's pre-deployment responsibilities with the deployer's operational assessments, the AI Act underscores the necessity of collaboration to safeguard fundamental rights effectively throughout the lifecycle of AI systems.[714]

This holistic framework ensures that AI systems safeguard fundamental rights at every stage of their lifecycle. To avoid redundancy and ensure clarity, it is crucial to align the

[712] AI Act, Art. 3, para. 1, n. 3).
[713] AI Act, Art. 3, para. 1, n. 4).
[714] Eleanor Spaventa, 'Fundamental Rights in the European Union' (Oxford University Press 2020); Johan van der Walt, *The Horizontal Effect Revolution and the Question of Sovereignty* (De Gruyter 2014); Lenaerts (n 21); Eleni Frantziou, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle' (2020) 22 Cambridge Yearbook of European Legal Studies 208.

methodologies for these assessments. Overlapping obligations, such as the FRIA and risk assessments under Articles 9 and 43, could burden actors, discouraging compliance and undermining the Act's objectives. Harmonising these tools through standardised templates, guidance, or automated support tools could streamline compliance while maintaining rigorous rights protections.

Without such alignment, there is a risk that the FRIA will remain a theoretical exercise, failing to achieve its goal of safeguarding fundamental rights in practice.

4.4.8 Critical analysis of the FRIA

De iure condendo, after this overview, is impossible to not underline some critical aspects of the FRIA that should be modified by the European legislator. In this section, three particular ones are going to be dissected.

First, a key issue arises in that the AI Act does not clearly specify which fundamental rights must be considered in the FRIA process. Differently, while the CFREU provides a comprehensive list of rights that are legally binding within the EU framework, the vagueness of the FRIA requirement leaves deployers without explicit guidance on the scope of the rights to evaluate. For instance, should deployers focus solely on privacy, non-discrimination, and data protection, rights traditionally linked to AI applications,[715] or should they also assess broader rights like freedom of expression, social equality, or even environmental considerations? This ambiguity risks creating inconsistencies in assessments and may lead to fragmented protection across Member States. Moreover, this lack of specificity could conflict with the multi-level protection of fundamental rights in the EU legal framework, *supra*. For example, while the Charter emphasises digital privacy and data protection (Articles 7 and 8), certain national constitutions might prioritise economic rights or the right to dignity in different ways. This fragmented approach could lead to conflicting interpretations of rights impacts, particularly in cross-border AI applications, thereby undermining the coherence and effectiveness of the FRIA as a regulatory tool.[716] Thus, it becomes necessary think to a tiered approach that prioritises rights most vulnerable to AI-driven harm; otherwise, the FRIA risks diluting

[715] *Ex multis,* Andrea Renda et al., 'Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe', April 2021; Casaburo and Marsh (n 48).

[716] Wachter (n 140); Nathalie A Smuha and Karen Yeung, 'The European Union's AI Act: Beyond Motherhood and Apple Pie?' (24 June 2024).

its focus and failing to adequately protect those rights most frequently and severely affected. Moreover, the lack of specificity in the FRIA's scope may conflict with the EU's multi-level protection framework, as the emphasis placed on different rights varies across Member States, leading to fragmented protection and inconsistent implementation

This latter aspect is connected with a pressing issue: the FRIA's applicability to private actors providing public services and the horizontal protection of fundamental rights. By requiring private entities to conduct fundamental rights assessments, the FRIA implicitly extends the scope of fundamental rights obligations beyond their traditional vertical dimension (state-to-individual) into horizontal relationships (private-to-private).

This extension raises two important challenges. While private entities are increasingly involved in delivering public services – such as healthcare, education, and credit scoring – the FRIA assumes that these actors have the capacity to fully evaluate the fundamental rights implications of their AI systems. However, private deployers may lack the legal expertise, resources, or institutional structures to properly assess and mitigate fundamental rights risks. This could lead to superficial or inconsistent assessments, weakening the overall protection of rights. Secondly, the horizontal applicability of fundamental rights, traditionally contentious in EU law, adds another layer of complexity. While the CJEU has gradually expanded the horizontal effect of certain fundamental rights (e.g., non-discrimination in cases like *Egenberger* and *Bauer*), the FRIA places a proactive responsibility on private actors to identify and mitigate risks. This doctrinal aspect, which has faced criticism from multiple perspectives[717] brings with it significant practical implications. It requires private actors to undertake a comprehensive assessment, even though fundamental rights traditionally function to limit the powers of state actors.[718] As such, it remains debatable how effective fundamental rights assessments will be in mitigating the risks posed by high-risk AI systems in the private sector, where these rights do not historically serve the same regulatory purpose.[719]

This shift could blur the lines between public and private accountability, creating legal uncertainties. For example, if a private deployer fails to adequately assess risks to fundamental rights, it is unclear whether liability would fall on the deployer, the state

[717] Philipp Hacker, 'Comments on the Final Trilogue Version of the AI Act' (23 January 2024) <https://papers.ssrn.com/abstract=4757603> accessed 3 December 2024.
[718] Ibid.
[719] Spaventa, 'Fundamental Rights in the European Union' (n 714).

overseeing the deployment, or the provider of the AI system; as a consequence, it is not clear in which position would be left the individual impairing, as the next Chapter will underline, the access to remedies.

Moving on to the assessment, the FRIA's reliance on a risk-based approach mirrors the DPIA and the other risk assessments used by the EU in the digital context, but it lacks a clear methodology tailored to AI's specificities. This lack of specificity is concerning, particularly because AI systems, by their nature, introduce unpredictable and evolving risks, which are not always fully captured by traditional impact assessments – and, for this reason, apparently, added an *ad hoc* method to measure it. While the FRIA introduces a more comprehensive regulatory tool in theory, it shares many of the same shortcomings as previous frameworks. It does not fully account for the increasing autonomy of AI systems, nor does it emphasise the human factor beyond viewing individuals as potential victims of AI harm.

These aspects must be carefully considered to develop a clear and practical methodology for implementing the FRIA. Without a well-defined and streamlined framework, informed by comparisons with other tools like the DPIA and the DSA's risk assessment, the FRIA risks remain a theoretical exercise with limited practical impact. To fulfil its intended purpose, the FRIA must avoid unnecessary procedural duplication while encouraging standardisation and simplification. If the process is overly complex or burdensome, actors may fail to comply, undermining the very objective of protecting fundamental rights. Clarifying these elements is essential to ensure that the FRIA can move beyond theoretical ambition to become a practical instrument that effectively safeguards fundamental rights in AI governance.

4.5 Much ado about methodology

There is already much ado about what type of method applying to the FRIA[720] on the topic has focused on the various modalities to perform the assessment; nonetheless, some indications arrive from the AI Act itself, since Rec. 96 expressly says that

[720] The paper relies especially on the following proposed methodologies: Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 48); Alessandro Mantelero and Maria Samantha Esposito, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review 105561; Mantelero, 'Human Rights Impact Assessment and AI' (n 676); Castets-Renard (n 660); Heleen L Janssen, 'An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making' (2020) 10 International Data

> "The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected, identify measures to be taken in the case of a materialisation of those risks."

Therefore, the FRIA can be divided at least into two distinct phases: a quantitative analysis of risks and a qualitative assessment of contextual impacts. The first quantitative phase involves the identification and measurement of the potential risks posed by the biometric system to fundamental rights. According to the AI Act, deployers must evaluate factors such as the likelihood and severity of harm,[721] focusing on measurable risks such as unauthorized data collection, algorithmic biases, or systemic discrimination.[722] The scholars[723] and the tool adopted by the Netherlands[724] propose the use of quantitative instruments that can be used to assign values to the risks identified: in this way, it would be ensured a structured and transparent process for identifying potential harms.

Secondly, the consequent phase requires a contextual and qualitative evaluation of how the identified risks may materialise in real-world scenarios.[725]. This process involves grasping the true essence of what constitutes an impact on fundamental rights – a task that is neither straightforward nor easily resolved.[726] This complexity is heightened by the fact that the responsibility for conducting such analyses is being entrusted also to actors who are not traditionally tasked with this role, as anticipated in the Introduction to this Chapter.

Privacy Law 76; Heleen Janssen, Michelle Seng Ah Lee and Jatinder Singh, 'Practical Fundamental Rights Impact Assessments' (2022) 30 International Journal of Law and Information Technology 200; Casaburo and Marsh (n 48).

721 These two elements are comprised in the definition of risk contained in the AI Act, and are used by Mantelero to calculate "the combination of the variables relating to these two dimensions provides a risk index that is assessed for each of the rights and freedoms potentially affected", as in Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 153, id.).

722 These evaluations are contained in the so called 'risk matrix', both in Mantelero, id., and Casaburo and Marsh (n 158).

723 Id.

724 Ministry of the Interior, The Netherlands, 'Impact Assessment Fundamental rights and algorithms', id.

725 Since it is not possible to assign "scores" to the balancing of rights, this aspect is of crucial importance. As also recalled by the study conducted by A. Renda, *et al.,* id.

726 Gianclaudio Malgieri and Cristiana Santos, 'Assessing the (Severity of) Impacts on Fundamental Rights' (Social Science Research Network, 25 June 2024) <https://papers.ssrn.com/abstract=4875937> accessed 3 December 2024.

Consequently, this qualitative assessment should delve also into the social, cultural, and legal contexts in which the AI system will be deployed. While the quantitative phase may flag a high probability of biased outcomes, the qualitative phase focuses on how these biases might affect specific groups, such as marginalized communities or individuals participating in public protests. It also extends to evaluating broader societal implications, such as the potential chilling effect on democratic participation or the erosion of public trust in critical institutions like law enforcement. By accounting for these contextual factors, this phase ensures that the assessment moves beyond abstract metrics to capture the lived realities of those directly impacted by the deployment of such systems.

The methodology proposed by the literature, therefore, systematically calculates risks using both quantitative and qualitative approaches that are usually structured in recurring phases:[727] 1) mapping rights and risks; 2) data and system evaluation; 3) risk matrix; 4) quantification models; 5) stakeholder engagement. However, empirical analyses of these proposed models highlight the necessity for meticulous attention in operationalising the FRIA. Particular care must be taken in developing indices and indicators, defining variables, and designing the risk matrix.[728] Nonetheless, many models propose mathematical estimation of risks in weighting the impact and likelihood. Saying it differently, the impact is calculated in a range from insignificant to extreme, whilst the likelihood level of the risk range is in between rare and almost certain, in order to understand the probability of occurrence as well as the severity of the impact.[729] Other

[727] Other proposed methods, like the FRAIA (Netherlands) adopt also scenario-based analysis, contextualizing the assessment. Boonstra and others (n 669).

[728] The risk matrix is used in many models for calculating the assessment of AI on fundamental rights. As explained by Mantelero, "a risk matrix is a graph that combines two dimensions using colours to reflect different levels of risk, they are useful for assessing indices generated by different variables. For this reason […], they are used in the FRIA to define the level of impact on each right concerned". Janssen et al., instead, speak of "risk factors", meaning "technical, organisational and legal" factors that can "help determine the severity of risks to rights". See Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 675); Janssen, Seng Ah Lee and Singh (n 667).

[729] This is, in particular, the case of Casaburo and Marsh (n 48). The authors explain that "the user should estimate both the severity of the prejudice (in negligible, critical, or catastrophic) and the number of affected individuals (in low, medium, or high). Based on the estimations, the user finds the impact level (low, medium, high, or very high) in the square where the severity of the prejudice and the number of affected individuals meet", in Donatella Casaburo and Irina Marsh, 'ALIGNER D4.2 Methods and guidelines for ethical & law assessment', 2023.

approaches, instead, advocate for the use of "qualitative matrices", in which each component is the expression of a "scale along a continuum".[730]

The methodology for FRIA cannot rest solely on abstract principles or generic approaches. A robust model must operationalise the assessment by integrating specific dimensions of risk and rights.[731] This entails identifying and combining relevant variables, ensuring proportionality in weightings, and avoiding unjustified overlaps or duplications in evaluating rights impacts. Moreover, when employing matrices or frameworks for FRIA, it is critical to examine the relationships between risk components and their interaction with fundamental rights. The scaling of risks, whether quantitative or qualitative, must avoid overly simplistic approaches, such as purely numerical indices, which might fail to capture the nuanced and contextual nature of rights interferences. Instead, transparency in defining scaling criteria and the interplay between risk factors is essential for ensuring assessments are credible and aligned with fundamental rights principles.[732]

Moreover, all of the recalled proposals present in literature from the assumption that a Fundamental Rights Impact Assessment does not exist yet in the European context and we need to establish – almost – from scratch a methodology for actually conducting it. However, this is not perfectly true.

As briefly mentioned above, the EU Commission, within the context of the better regulation agenda adopted on 19 October 2010, set out the "Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union", whose main aims are to "make the fundamental rights provided for in the Charter as effective as possible" and to "to identify fundamental rights liable to be affected, the degree of interference with the right in question and the necessity and proportionality of the interference in terms of policy options and objectives".[733]

---

[730] Instead of quantitative measurement, Mantelero propose a qualitative one that measures the potentially adverse impact for each of the rights and freedoms considered, combined with a radial graph that charts bt representing the overall impact on them, considering, once again, the risk from low to high. The methodology is proposed in Mantelero, 'Human Rights Impact Assessment and AI' (n 676).

[731] On the contrary, this might result in what Ignacio Cofone calls "a reductionist view of the world where people's privacy is only worth protecting to prevent material harm happening to them. This mistaken conception has enormous practical implications: it interferes with the right to sue and obtain compensation". The author speaks specifically of privacy, but the discourse might be translated also to other fundamental rights.

[732] Malgieri and Santos (n 726).

[733] Communication from the Commission Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM/2010/0573 final. The quotes come from the same text.

The strategy was complemented in 2011 with the "Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments"[734] sets forth the Commission staff preparing impact assessments and for impact assessment support units.[735] This guidance is particularly helpful since it addresses the structure and the practical framework to make effective use of the FRIA and, moreover, can be replicated not only for internal purposes but can make a real impact on national states and citizens as well.[736] Hence, while the EU does not possess a distinct or explicitly defined competence under its treaties to legislate broadly on fundamental rights, this does not imply a lack of authority to adopt positive measures aimed at enhancing their implementation.[737] On the contrary, the EU consistently integrates both direct and indirect references to the analysis and protection of fundamental rights within its legislative framework. A clear example of this is found in Article 27 of the AI Act, which explicitly mandates the assessment and mitigation of fundamental rights impacts in the deployment of high-risk AI systems, demonstrating the EU's commitment to embedding fundamental rights considerations into its regulatory practices.

Limiting this approach solely to the legislative and policy-making process overlooks its potential for broader application, particularly in the regulatory context of the AI Act where the AI Office first and the deployers, secondly, are tasked with finding a way to make the FRIA an operative and efficient instrument. For this reason, this thesis argues

[734] Commission Staff Working Paper. Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC(2011) 567 final. The paper is also part of the Smart Regulation in the European Union, COM(2010) 543 final, in which the Commission announced that to reflect the new legal status of the EU Charter of Fundamental Rights, the Commission would reinforce the assessment of impacts on fundamental rights and would develop specific guidance on the methodology to be adopted.

[735] It is to specify that in the 'Strategy to strengthen the application of the Charter of Fundamental Rights in the EU', published in 2020, the EU Commission, after confirming the importance of conducting assessments that are highly anchored to the Charter, stated that the intent is to "update its 2011 guidance for its staff on applying the Charter in impact assessments and disseminate it as a source of information for policymakers at national and local level". EU Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions', Brussels, 2.12.2020, COM(2020) 711 final.

[736] "The EU has progressively given greater prominence to fundamental rights through its institutional framework, legal standards and policies. Good practices that are already in place can be replicated and systematised to form an overarching fundamental rights strategy. Such a strategy would not require new institutions, new legislation, or changes to the EU treaties. Rather it requires a change in practice and culture, both in the EU and national governments", Israel Butler, 'A Fundamental Rights Strategy for the European Union' (Open Society Foundations 2014) <https://www.jstor.org/stable/resrep43002> accessed 21 November 2024.

[737] Spaventa, 'The Horizontal Application of Fundamental Rights as General Principles of Union Law' (n 590).

that his adaptation is necessary and justified for several reasons that are going to be unpacked in the next paragraph.

4.5.1 FRIA: borrowing a methodology?

The reasons why this thesis argues that the methodology adopted by the Commission in its FRIA framework is useful, to some extent, for delineating the FRIA specific to AI are essentially twofold. First, it aligns with the imperative to explicitly identify and "name" the fundamental rights at stake, thereby rendering them visible and actionable. This visibility is critical for ensuring that these rights are not abstractly referenced but are concretely recognized in their practical implications within specific AI contexts. By clearly articulating which rights are engaged, the framework facilitates a more targeted and effective evaluation of risks and interferences.

Second, the Commission's approach provides a structured pathway for integrating these identified rights into a systematic assessment process. By combining the FRIA for legislation with the parameters and methodologies for evaluating how AI systems impact fundamental rights, the framework might offer a practical starting point for translating theoretical commitments into actionable safeguards. This dual focus on naming and assessing rights ensures that the FRIA for AI is not only comprehensive but also deeply attuned to the specificities of this technological domain.

More in depth, the methodology is deeply embedded in the Charter of Fundamental Rights, which is a binding legal framework for the EU. By systematically assessing the impacts of AI systems on fundamental rights, the methodology ensures compliance with the Charter. It explicitly incorporates key principles such as necessity and proportionality[738], and it is designed to prevent violations of absolute rights, such as human dignity and the prohibition of torture, by mandating their prioritisation in the initial screening stages.[739] This strict alignment with the Charter provides a robust legal and ethical foundation for conducting FRIA, ensuring that deployers of high-risk AI systems

[738] CFREU, Art. 52. *Inter alia,* Aharon Barak (ed), 'The Components of Proportionality', *Proportionality: Constitutional Rights and their Limitations* (Cambridge University Press 2012).
[739] CFREU, Articles 1 and 4.

respect the fundamental values of the EU by essentially guiding them on ascertaining the 'shades' of the different rights and their concrete meaning.[740]

This a critical challenge for the industry and, we argue, for deployers in general, as highlighted by network reports such as the Future for Privacy Forum on Impact Assessment.[741] The report, in fact, underlines that

> "Organisations often find it difficult to assess risk management strategies' efficacy due to the subjective nature of and the lack of standardized metrics for measuring certain risks, and the indeterminate nature of some AI systems operational environments".[742]

In this sense, the Commission methodology, while incorporating the interpretations of fundamental rights as developed in the case law of the CJEU,[743] is capable to ensuring that rights are not only abstractly acknowledged but are also assessed in line with established legal precedents.[744] By relying on these legal interpretations, the methodology provides a practical framework that is grounded on EU Law to balance competing rights in compliance with EU law.[745]

Furthermore, the added value of the methodology proposed by the Commission is the Fundamental Rights Checklist, a tool designed to systematically assess whether fundamental rights are impacted. This checklist includes the following questions:[746]

---

[740] As the "Operational Guidance" put it, "An initial screening of fundamental rights aspects should first check whether absolute rights are likely to be affected, as any objectives or options that violate such rights should be avoided from the very beginning. The initial screening should next identify whether there are any non-absolute Charter rights which the policy options might limit. Through consultation and analysis, the extent to which potential limitations are necessary, proportionate and impossible to replace by a less intrusive alternative will then need to be assessed", see p. 11.

[741] Future of Privacy Forum, 'AI Governance behing the Scenes. Emerging Practices for AI Impact Assessments', December 2024.

[742] Id., p. 20.

[743] The same approach, including sanctions and notable cases of violations of fundamental rights, was also applied by Andrea Renda et al., 'Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe', id. See, in particular, Annex I where any fundamental rights of the Charter are associated with a few potential cases of violations.

[744] For instance, the proportionality and necessity tests embedded in the methodology reflect the CJEU's requirement for legislative and regulatory measures to justify any limitations on rights, as seen in cases like Melloni, CJEU (Grand Chamber), *Stefano Melloni v Ministerio Fiscal,* C-399/11.

[745] As also the Guidance put it "the Impact Assessment should be used to identify fundamental rights liable to be affected, the degree of interference with the right(s) in question, and the necessity and proportionality of the interference in terms of policy options and objectives".

[746] See the Guidance, p.3-4.

1. What fundamental rights are affected?

2. Are the rights in question absolute rights (which may not be subject to limitations, examples being human dignity and the ban on torture)?

3. What is the impact of the various policy options under consideration on fundamental rights? Is the impact beneficial (promotion of fundamental rights) or negative (limitation of fundamental rights)?

4. Do the options have both a beneficial and a negative impact, depending on the fundamental rights concerned (for example, a negative impact on freedom of expression and a beneficial one on intellectual property)?

5. Would any limitation of fundamental rights be formulated clearly and predictably?

6. Would any limitation of fundamental rights be necessary to achieve an objective of general interest or to protect the rights and freedoms of others (which)?; be proportionate to the desired aim? Preserve the essence of the fundamental rights concerned?

This step, on the one hand, ensures that all rights under the CFREU are considered comprehensively and early in the assessment process; on the other hand, it frames exactly the specific rights at stake and determines the nature of interference.[747] Thus, to answer the questions, it should be understood which are the absolute rights,[748] like human dignity, which are absolute, and, therefore, not subject to any balancing test.[749] Differently, rights

[747] Therefore, measures taken by public authorities that interfere with a non-absolute right can be justified under certain conditions. The interference will only amount to a violation of such a right when the justifying conditions cannot be fulfilled. The requirements for a justified limitation are set out in Article 52 of the Charter. On this, see Malgieri and Santos (n 726).

[748] The Charter does not explicitly identify the rights that are absolute. Based on the Charter explanations, the ECHR and the case law of the European courts, it is submitted that human dignity (Article 1 of the Charter), together with the prohibition of torture and inhuman or degrading treatment or punishment (Article 4 of the Charter), are to be considered absolute rights. Especially consider at EU law level, Article 52(1) CFREU states that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others". In general, it should be remembered that the rights which are considered absolute under the ECHR and the ECtHR jurisprudence apply to corresponding rights in the Charter due to Art. 52 para. 3 – the so-called "equivalence clause". See Francesco Viganò, 'Rethinking the Proper Role of Proportionality in the Limitation of Fundamental Rights', Draft text of the intervention at the international conference (Riga, 2-3 September 2021): 'EUnited in Diversity: Between Common Constitutional Traditions and National Diversities' 4th Panel: 'Limitation on the exercise of fundamental rights'; Spaventa, 'Fundamental Rights in the European Union' (n 714); Craig and Búrca (n 548).

[749] Lenaerts (n 459). As noted by Viganò, *supra*, "in practice, Article 52 (1) CFREU should not apply to those 'absolute rights', which apparently do not lend themselves to limitations under the general umbrella of proportionality".

like privacy, freedom of expression, and equality may be limited if the limitations.[750] Hence, this stage requires mapping all rights affected by the policy or deployment and justifying any potential limitations based on these criteria.

As a consequence, it is requested to draw a roadmap and conduct consultations with stakeholders in order to identify affected parties, such as civil society organisations, rights experts, and oversight bodies like the Fundamental Rights Agency; or create targeted questionnaires and consultations to gather input on specific rights concerns. This collaborative effort ensures that the assessment reflects diverse perspectives and builds legitimacy for the proposed measures. After identifying the potential rights affected, the next step is to evaluate various policy or deployment options. This aspect can be recalled under the umbrella of the principle of necessity and minimization, since, compared with the obtained results, any option that would violate absolute rights or excessively interfere with non-absolute rights without justification is discarded.[751]

While proportionality is often cited as a formal requirement in the governance of AI systems, this thesis advocates for a substantive engagement with proportionality as a constitutional test. A normative FRIA must assess whether the deployment of an AI system genuinely meets a pressing social need, whether less intrusive alternatives exist, and whether the interference with fundamental rights is justifiable in light of the overall legal and institutional context. This goes beyond compliance with sectoral rules and requires alignment with the deeper logic of constitutional rights adjudication.

For these reasons, anchoring the FRIA on the methodology used by the European Commission is a helpful structure that is capable of clarifying to the deployers how to perform concretely the obligation under Art. 27. Without a solid and truly rights-based approach, the risk is that the FRIA will remain an obligation that lacks the operative means to function. Finally, the proposed methodology is strictly complying with the AI Act answering to all the *desiderata* of the Regulation, as the next paragraph will argue.

---

[750] As specified by the CJEU, neither privacy nor data protections are absolute rights; therefore, "the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society". CJEU (Grand Chamber), *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems,* C-311/18, 16 July 2020, §172.

[751] As the Guidance specifies, the options are assessed not only for their compliance with rights but also for their impact balance. The goal is to retain only those options that are both effective in achieving the policy's objectives and least intrusive to fundamental rights.

4.5.2 Utility with the AI Act

As described, the Commission process aligns closely with the methodological structure proposed in the AI Act for conducting FRIA, specifically, to streamline the identification and prioritisation of risks, making the Charter – and, consequently of the FRIA – a live instrument and not an abstract monad.[752]

Thus, the adaptation of the Commission's methodology to regulatory impact assessments addresses one of the core challenges deployers face: operationalising abstract legal principles into actionable steps. By translating the Commission's approach into the AI Act's compliance framework, deployers can effectively assess risks: it is worth repeating that one of the main issues with the FRIA, as per under Art. 27 AI Act, is the exact identification of the fundamental rights at stake, not only in terms of knowing the "what" but, moreover, the "how" their impact can be concretely assessed.

At the heart of this alignment is the identification and assessment of fundamental rights. Article 27 mandates deployers to evaluate potential interferences with the fundamental rights,[753] without specifying which rights specifically. Hence, the Commission's Fundamental Rights Checklist can directly support this process, guiding deployers in systematically identifying the rights at risk, distinguishing between absolute and non-absolute rights, and determining the nature and justification for any interference. This structured approach ensures that rights are neither overlooked nor inadequately protected.

Furthermore, the AI Act underscores the importance of proportionality and necessity in evaluating any interference with fundamental rights.[754] The Commission's methodology integrates these tests into the framework, operationalizing them as part of

[752] Or, as the Strategy of 2010 put it "the Charter is not a text setting out abstract values, it is an instrument to enable people to enjoy the rights enshrined within it when they are in a situation governed by Union law", p. 4-5.

[753] It is worth recalling the Rec. 96 of the AI Act, "to identify the specific risks to the rights of individuals or groups of individuals likely to be affected, identify measures to be taken in the case of a materialisation of those risks".

[754] This is more in general the whole approach of the Regulation, as clearly mentioned in Rec. 176 of the AI Act: "since the objective of this Regulation, namely to improve the functioning of the internal market and to promote the uptake of human centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection against harmful effects of AI systems in the Union and supporting innovation, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective".

the FRIA process. By embedding proportionality and necessity analyses, it ensures that any limitations on fundamental rights are justified, and minimal, and preserve the essence of the rights affected, thereby upholding both the letter and spirit of EU law, as per Art. 5 TUE.

Another critical requirement of Article 27 is stakeholder consultation and engagement, particularly in cases where AI systems may disproportionately impact vulnerable populations. The Commission's methodology emphasises the use of roadmaps and consultations, which might serve as guidance for the deployers to actively involve stakeholders, such as affected communities and civil society organizations, in the assessment process, to identify potential interferences with the rights. This participatory approach ensures that risk identification and mitigation measures are not only comprehensive but also reflective of diverse perspectives.[755]

In conjunction with assessing impacts, Article 27 requires deployers to implement safeguards that effectively address identified risks. The Commission's structured methodology includes robust strategies for designing mitigation measures, such as transparency mechanisms, human oversight provisions, and procedural safeguards. These tools align directly with the AI Act's goals of minimizing harm while promoting accountability.[756]

From this overview, we can understand that the Commission's methodology fits with the framework established by Article 27 of the AI Act. It provides deployers with a comprehensive toolset to identify, assess, and address fundamental rights impacts, translating abstract regulatory obligations into clear, actionable steps. By adopting this approach, deployers not only fulfil their legal requirements but also promote accountability, transparency, and public trust, contributing to the broader goal of fostering trustworthy and rights-compliant AI systems.

For this reason, it is deemed essential to integrate this approach, especially for the qualitative part of the FRIA, because it will serve as a guideline, as also the next Chapter

[755] Once again, Rec. 96 of the AI Act states that "where appropriate, to collect relevant information necessary to perform the impact assessment, deployers of high-risk AI system, in particular when AI systems are used in the public sector, could involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations in conducting such impact assessments and designing measures to be taken in the case of materialisation of the risks".

[756] Also in this respect, the mitigation measures are clearly addressed both in Rec. 93 and 96, as well as in Art. 27 of the AI Act.

will demonstrate, to highlight and frame the interferences, concrete or just potential, with the enjoyment of fundamental rights.

Lastly but maybe more importantly, the connection between the Commission's methodology and the FRIA process lies in their shared goal: embedding fundamental rights considerations into governance frameworks "to build mutual trust".[757] Therefore, adopting the Commission's proven methodology for FRIA in the AI Act context is not only practical but vital. It offers deployers a robust, systematic approach to navigating the complexities of fundamental rights, ensuring compliance while fostering public trust in AI governance.

4.6 Conclusion

In conclusion, Chapter 4 has shown that FRIA must be developed not as a mere risk-scoring exercise, but as a constitutional practice of justification. By embedding the principles of proportionality and normative legality, the FRIA becomes a framework through which deployers, particularly public authorities, must demonstrate not only that a system functions lawfully, but that its deployment context respects the core tenets of fundamental rights protection. The next chapter applies this model concretely to FRT, testing its capacity to reveal structural risks and legal inadequacies in real-world contexts.

Essentially, the FRIA represents a shift from traditional, vertical enforcement of fundamental rights by public authorities to a horizontal framework that extends responsibilities to both public and private actors. This evolution reflects the increasingly blurred lines between public and private accountability in the deployment of AI systems.

While the FRIA holds substantial promise as a structured mechanism for identifying, evaluating, and mitigating risks to fundamental rights, this chapter has revealed critical gaps that must be addressed to ensure its effective implementation. The reliance on self-assessment, the lack of harmonised and concrete methodologies, and the limited integration of FRIA with existing tools like DPIAs under GDPR highlight the pressing need for a more comprehensive and coordinated approach. Moreover, the chapter has introduced the necessity of prioritising "higher risk fundamental rights" to address the

[757] COM(2010) 573 final, p. 5.

differentiated impacts AI systems pose, particularly in contexts where risks to privacy, democratic freedoms, and access to remedies intersect.

A recurring theme throughout the chapter is the importance of operationalising the analysis of rights interferences. Moving beyond a binary understanding of rights violations, the FRIA must incorporate a multidimensional methodology that combines quantitative and qualitative assessments. This approach ensures not only legal rigor but also sensitivity to the specific operational contexts of AI deployments. Such a nuanced framework is particularly vital for facial recognition systems, where overlapping risks to fundamental rights necessitate robust and proactive safeguards.

This chapter has laid the groundwork for the subsequent analysis. Chapter 5 will focus on biometric systems, particularly facial recognition technology, as a case study for the practical application of the FRIA. It will delve into the deployment of these systems by public authorities, particularly law enforcement, and their profound implications for fundamental rights. Special attention will be given to Article 47 of the CFREU, to which Chapter 6 is devoted, examining how to ensure effective remedies and due process in this context. This exploration aims to bridge theoretical insights with practical applications, advancing a regulatory framework that is both adaptive and effective in protecting fundamental rights.

5. THE FRIA IN PRACTICE: APPLYING A NORMATIVE FRAMEWORK TO FACIAL RECOGNITION

SUMMARY: 5.1 Introduction. – 5.2 FRIA: building a model for facial recognition technology; 5.2.1 Elaboration of the model; 5.2.2 All rights are equal, but some are more at risk. 5.3 FRIA for FRT; 5.3.1 Fundamental right's checklist; 5.3.2 Which fundamental rights are affected?; 5.3.2.1 Case analysis: *Glukhin v. Russia* – A practical application of FRIA. 5.4 Test: Art. 8, CFREU, data protection; 5.4.1 Cluster 1: training and modeling – are these personal data?; 5.4.2 Cluster 2: the use of publicly available data; 5.4.3 Cluster 3: data retention and erasure; 5.4.3.1 The right to erasure: who wants to live forever?; 5.4.3.2 Data retention: it's now or never?. 5.5 Conclusion.

5.1 Introduction

How risky is it to stand with a sign in a bustling metro station? How much greater is the risk when that sign is held to protest for justice and solidarity in an authoritarian regime?

To find the answers to these questions, consider the story of a protester standing silently in a crowded metro, holding a banner advocating for human rights. Without their knowledge, surveillance cameras capture their image, which is then circulated in Telegram groups. Facial recognition technology silently scans their face and matches it against a government database. Days later, this data is weaponised by authorities to locate and arrest the individual, accusing them of violating public assembly laws.

Far from being a hypothetical scenario, this is the story of Nikolay Sergeyevich Glukhin, whose protest in Moscow led to his prosecution and ultimately became the subject of the first ruling at the international level, decided by the ECtHR.[758] In the ruling, it emerged that the practice used by the police in the metro against the applicant was a violation of Articles 10 (freedom of expression) and 8 (right to respect for private life) of the European Convention on Human Rights (ECHR);[759] however, the implications of this case and the practice hereby condemned can extend far beyond these specific rights, undermining a broader spectrum of human rights.[760]

[758] ECtHR (III Chamber), Application No. 11519/20, *Glukhin v. Russia,* 4 July 2023.

[759] §82 "the Court considers that it is essential in the context of implementing facial recognition technology to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards will be all the greater where the use of live facial recognition technology is concerned.".

[760] The case for its importance and for being the first one at the international level on FRT attracted the attention of many scholars. This research especially relied on the analysis of Giuseppe Mobilio, 'La Corte EDU

Glukhin's story represents just an example of a paramount assault on the right to protest, the right to freedom of assembly and broader principles of democratic participation. Moreover, highlights what profound dangers might be posed by a critical intersection of crucial elements: authoritarian regimes, advanced surveillance technologies and the curtailment of democratic rights.

This combination constitutes indeed a "perfect storm"[761] that not only impact the enjoyment of fundamental rights but has 'chilling effects'[762] on public dissent, stifles political participation, and erodes the foundational freedoms essential to a democratic society. The unchecked deployment of facial recognition technology, absent robust safeguards, enables regimes to weaponise these tools for surveillance and control. This practice infringes on individual rights such as privacy, freedom of expression, and assembly, while simultaneously being capable of creating a destabilised environment for the proliferation of democratic governance, facilitating the entrenchment of authoritarianism under the guise of security and order.

Hence, in this scenario, biometric technologies, like facial recognition, "extend[ed] the ability of government authorities to monitor, identify, and track individuals in public areas, but their indiscriminate, biased, and opaque nature has the potential to deter protesters from exercising their right to assembly".[763] As analysed in Chapter 3, this technology exemplifies the dual-edged nature of artificial intelligence: it holds the potential to enhance security and operational efficiency, yet simultaneously poses significant threats to fundamental rights when deployed without robust legal safeguards that account for its profound societal impact.

Condanna Il Ricorso Alle Tecnologie Di Riconoscimento Facciale per Reprimere Il Dissenso Politico: Osservazioni a Partire Dal Caso Glukhin c. Russia' [2024] DPCE ONLINE 695; Francesca Palmiotto and Natalia Menéndez González, 'Facial Recognition Technology, Democracy and Human Rights' (2023) 50 Computer Law & Security Review 105857; Monika Zalnieriute, 'Glukhin v. Russia. App. No. 11519/20. Judgment' (2023) 117 American Journal of International Law 695; Costanza Nardocci, 'Il riconoscimento facciale sul "banco" degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia' [2024] BioLaw Journal - Rivista di BioDiritto 279; Isadora Neroni Rezende, 'Glukhin and the EU Regulation of Facial Recognition: Lessons to Be Learned?' (*European Law Blog*, 19 September 2023) <https://europeanlawblog.eu/2023/09/19/glukhin-and-the-eu-regulation-of-facial-recognition-lessons-to-be-learned/> accessed 30 September 2023.

[761] The term perfect storm is used to mean "an event whose consequences far exceed the combined impact of the individual circumstances that brought it about", as in Massimiliano Malvicini and Erik Longo, 'Il decisionismo governativo: uso e abuso dei poteri normativi del Governo durante la crisi da COVID-19' (2020) Federalismi 28.

[762] See, *infra,* §5.2.2.

[763] Margaret Warthon, 'Artificial Intelligence and Freedom of Assembly' in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023).

For these reasons, scholars have described FRT as "a direct challenge to democratic society,"[764] due to its unprecedented capacity to identify, track, and profile individuals on a massive scale.[765] These risks are particularly pronounced in regions such as the Global South, where weak governance frameworks often fail to provide sufficient protections, allowing such technologies to deepen systemic inequalities and suppress political participation and dissent.[766]

Building on the theoretical framework established in Chapter 4, this chapter applies the FRIA not merely as a tool for evaluating the practical effects of biometric systems, but as a normative instrument to interrogate the constitutional legitimacy of the legal framework in which such systems are deployed. The aim is to show that a FRIA, when conducted by public authorities, must assess whether the deployment of technologies like facial recognition takes place within a legal and institutional setting that genuinely upholds fundamental rights. In this sense, the FRIA is not only about evaluating technical risk or procedural safeguards: it is about determining whether the broader regulatory environment satisfies the structural requirements of democratic legitimacy, legal certainty, and the rule of law.[767]

Hence, the chapter begins by employing the FRIA methodology to identify the fundamental rights most at risk from biometric technologies, such as privacy, data protection and freedom of expression and assembly. Using case studies, including

---

[764] Daragh Murray, 'Facial Recognition and the End of Human Rights as We Know Them?' (2024) 42 Netherlands Quarterly of Human Rights 145.

[765] As noted by scholars advocating for the total ban of FRT, "the introduction of biometric mass surveillance in publicly accessible spaces reduces lively public spaces to spaces where technology is monitoring". Cit. Lotte Houwing, 'Reclaim Your Face and the Streets. Why Facial Recognition, and Other Biometric Surveillance Technology in Public Spaces, Should Be Banned' in Sven Quadflieg, Klaus Neuburg and Simon Nestler (eds), *(Dis)Obedience in Digital Societies: Perspectives on the Power of Algorithms and Data* (transcript Verlag 2022).

[766] Malcolm Katrak and Ishita Chakrabarty, 'Privacy, Political Participation, and Dissent: Facial Recognition Technologies and the Risk of Digital Authoritarianism in the Global South' in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023).

[767] For the purposes of this thesis, the FRIA conducted herein adopts a general framework rather than focusing on any specific artificial intelligence system used for biometric purposes. No particular company or proprietary system is under examination. Instead, the assessment is designed to provide a broader analysis applicable across various contexts where biometric technologies, such as facial recognition systems, may be deployed. Given the author's area of expertise, the assessment is confined to the fundamental rights checklist component, specifically within the pre-deployment phase of such technologies. This approach reflects the importance of proactively identifying and addressing potential rights infringements before these systems are implemented. Moreover, this limitation aligns with the current legal landscape, as at the time of writing, the obligations under Article 5 of the AI Act, which governs the use of high-risk AI systems, have not yet come into effect. By focusing on the pre-deployment phase, this thesis aims to contribute to the development of a rights-based framework that can guide the responsible and compliant deployment of biometric technologies in the very next future.

Glukhin v. Russia, and broader global examples, it delves into the far-reaching consequences of biometric surveillance, particularly in contexts where legal safeguards are inadequate. It then demonstrates how the FRIA framework can be operationalised to mitigate these risks, offering a structured means of aligning technological deployment with fundamental rights protections. By focusing on the application of this methodology, the chapter not only advances the discourse on biometric technologies but also lays the groundwork for the subsequent exploration of effective remedies and accountability mechanisms necessary to address violations stemming from their misuse.

5.2 FRIA: building a model for facial recognition technology

This section introduces the tailored FRIA methodology proposed by this thesis for evaluating the impact of facial recognition technology, addressing both real-time and post-factum use cases. This methodology responds to the urgent need for frameworks that go beyond generalist approaches, providing safeguards and risk evaluations tailored to high-stakes applications like biometric surveillance.

The paragraph starts by explaining how the model has been created, including the rationale underlying its structure. The model is grounded in the need for a practical and actionable tool to evaluate rights interference, particularly in contexts where biometric technologies amplify tensions between operational goals (such as public safety) and the protection of fundamental rights. The absence of explicit guidance within the AI Act on which rights to consider or to prioritise and the lack to any referral to the multi-level framework of fundamental rights, described in Chapter 4, has necessitated a rethinking of how deployers approach their obligations. The methodology proposed here bridges this gap, offering clarity on the rights most at risk and proposing a systematic approach to evaluating their impact.

Secondly, this section introduces what we call a "higher risk" methodology. As anticipated in Chapter 4, this concept acknowledges that while all fundamental rights are equally important in principle, not all rights are impacted to the same degree across AI use cases.[768] This differentiation is essential to ensure that the FRIA framework is not

[768] This aspect evocates the reasoning of the CJEU based on the principle of proportionality. As recalled, for instance, in many decisions with respect to non-absolute rights like data protection, "it must be considered

merely theoretical but deeply embedded in practical realities. For instance, in the case of law enforcement's deployment of facial recognition technologies, rights such as privacy, data protection, and access to an effective remedy emerge as the most vulnerable. Conversely, in contexts like healthcare, the risks shift towards more equitable access to care and non-discrimination, whilst all the 50 rights of the Charter might be also impacted at least in theory.

Therefore, as will be expanded *infra,* the methodology integrates two key dimensions: the operational context, which determines the specific risks posed by the AI system, and the systemic safeguards needed to mitigate these risks. This dual focus ensures that the FRIA framework not only aligns with the general principles of necessity, proportionality, and accountability but also adapts to the unique challenges of high-risk technologies.

5.2.1 Elaboration of the model

Biometric systems, such as facial recognition, are inherently high stakes:[769] they process sensitive personal data,[770] operate in public or semi-public spaces and carry profound implications for privacy, non-discrimination,[771] and democratic freedoms.[772] As scholars highlighted,

> "While the risk-based, cost/ benefit rationale already underlying many fields, from the environment to data protection, could entertain utilitarianism-advocates, it cannot and should not replace the logic of the 'fundamental'. There are certain sensitive areas where financial interests and security must not be over-prioritised; where fundamental

in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality", i.e., CJEU, *GC and Others*, C-136/17, 24 September 2019, §57.

[769] AI Act, Art. 5, para. 3, establishes that, prior to the put into place of such technologies, should be granted authorization from a judicial authority or an independent administrative authority. However, this authorization can be surpassed in case of urgency.

[770] Paul Quinn and Gianclaudio Malgieri, 'The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22 German Law Journal 1583.

[771] Raphaële Xenidis and Linda Senden, *EU Non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination* (Kluwer Law International 2020).

[772] *Inter alia,* such risks have been framed by the European Union Agency for Fundamental Rights FRA.: Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement. (2019).

human rights cannot be outweighed by being attributed numerical values in a mathematical fashion".[773]

Then, what makes biometric technologies particularly compelling as a focal point is their ability to magnify existing tensions between regulatory objectives, such as the protection of fundamental rights, and operational goals, such as public safety or efficiency.[774] Positioned at the crossroads of high-risk and prohibited AI categories, these systems demand nuanced methodologies to assess their impact.[775] Consequently, the elaboration of a model for FRIA must necessarily take into consideration the very features of facial recognition systems, and to be clear, this approach should be applied also for any other AI system.[776]

This line was also adopted by Working Party 29 in the context of conducting a Data Protection Impact Assessment (DPIA). As discussed in Chapter 4, the obligation to perform a DPIA – an obligation that should intersect with the FRIA at certain points – requires an assessment of the impact of high-risk processing of personal data. In this regard, the guidelines issued by WP29 were explicit in stating that, as long as the template included the essential elements mandated by law, various tailored methodologies could be employed to support the effective implementation of the DPIA and that "sector specific" frameworks development were indeed encouraged.[777]

Hence, while most of the scholarly analysis on FRIA elaborated approaches that are prone to the adoption of general frameworks without focusing on sector specific

[773] Cit. p. 5, Paul De Hert and Georgios Bouchagiar, 'European Biometric Surveillance, Concrete Rules and Uniform Enforcement: Beyond Regulatory Abstraction and Local Enforcement', *Cambridge Handbook on Facial Recognition in the Modern State* (Cambridge Univ Press 2024).

[774] This is a tension that is not only typical of FRT but can be extended more in general to the integration of automated systems in the panorama of the public sector, as highlighted in Marya Akhtar and Rikke Frank Jørgensen, 'Chapter 4: A Rights-Based Approach to Automated Decision-Making in the Public Sector' (2024).

[775] See Chapter 3, §3.5.

[776] The necessity to focus on the use of AI and not generically on AI as a monad is well argued in Luciano Floridi, 'Present: AI as a New Form of Agency, Not Intelligence' in Luciano Floridi (ed), *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities* (Oxford University Press 2023).

[777] Specifically, "the WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures). This means the DPIA can address the issues that arise in a particular economic sector, or when using particular technologies or carrying out particular types of processing operation". See Article 29 Data Protection Working Party, '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', 4 October 2017, in part. p. 17.

instances,[778] this thesis sustains that the true effectiveness of FRIA lies in tailoring the analysis to the specific use and deployment of AI systems.[779] Thus, that is the key innovation proposed by this thesis: tailoring the analysis to the specific use and deployment of AI systems.

This is particularly critical in the context of law enforcement, where the connection between state power and individual rights demands a comprehensive approach that transcends mere compliance. Law enforcement entities must adopt a nuanced perspective that considers not just procedural adherence but also the broader societal implications of their actions.[780] Unlike private actors, whose responsibilities and regulatory concerns differ significantly, public authorities act as intermediaries between state power and the rights of individuals.[781]

Summarising these thoughts, with FRT the necessity of developing a sector specific method lies also on two factors: i) biometric systems, especially FRT, present a particularly compelling case due to their substantial presence in markets and law enforcement; ii) for FRT, a robust body of case law exists, with systems actively deployed and generating real-world data about their risks and societal impacts.[782] This contrasts with other AI applications where legal and societal implications remain speculative and where technology's integration into public or private sectors is nascent.

Therefore, the unique role of law enforcement requires leveraging FRIA not only as a compliance mechanism but also as a privileged observatory that enables a broader evaluation: this includes not only procedural adherence but also an in-depth assessment of the regulatory framework encompassing FRT use. In particular, for law enforcement agencies, the focus of evaluating AI systems must address two key aspects: the use of the technology itself and the broader regulatory system in which it operates. This means that the assessment must go beyond mere compliance with existing rules to also consider how

[778] *Inter alia,* Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 48).
[779] This theory is sustained also by the approaches proposed by Casaburo and Marsh (n 48); George Bouchagiar, 'A Fundamental Rights Impact Assessment for Dlt-Programmes Targeted at the Public Sphere' (12 January 2024) <https://papers.ssrn.com/abstract=4693577> accessed 3 December 2024.
[780] EDPB, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, 26 April 2023.
[781] Ruotolo (n 40); Leiser and Custers, 'The Law Enforcement Directive' (n 459); Purtova (n 367).
[782] ECtHR (III Chamber), Application No. 11519/20, *Glukhin v. Russia,* 4 July 2023; Italian DPA, decisions no. 105, 106, 107, 108 and 109, 22 February 2024; Giulia Gentile, 'Does Big Brother Exist?: Facial Recognition Technology in the United Kingdom' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024); Palmiotto and González (n 3).

the normative framework can adapt to the specific risks posed by these technologies.[783] Such an approach ensures not only that the deployment of AI systems aligns with fundamental rights but also that the regulatory environment evolves to address the challenges and complexities of these high-risk applications.

Having explained the rationale behind the methodological development[784] – starting from a general framework and narrowing to specific contexts – it is worth specifying that this structure is not a mere stylistic choice but reflects the essence of the work being proposed. For this reason, as introduced in Chapter 4, we now move to analyse the specific relevance of the Commission's FRIA methodology within this tailored approach.

As a matter of fact, the Commission's methodology is particularly valuable in this context. Specifically, for public authorities such as law enforcement agencies, this methodology ensures that deployed systems comply with fundamental rights in a holistic manner. As analszed in Chapter 4, its origin lies in its design for evaluating EU legislation, which grants it dual applicability. This dual function makes it particularly suited to assessing the mentioned critical dimensions: i) whether the regulatory context is sufficiently robust, evaluating factors such as the safety of the deployment environment, the adequacy of procedural safeguards, authorisation processes, and oversight mechanisms; and (ii) the broader impact of the technology on fundamental rights.

By addressing both dimensions of rights protection – the normative (regulatory context) and the applicative (practical implementation) – the FRIA methodology, borrowd by the European Commission, operationalises the Charter in a way that reflects the realities of AI deployment in diverse contexts.[785] This dual-layered approach ensures that the system's compliance with fundamental rights is not evaluated in isolation but rather within the evolving socio-legal framework that governs its use.[786]

---

[783] This would be also the mechanism to avoid that Monika Zalnieriute calls the procedural fetishism in 'Against Procedural Fetishism in the Automated State' in Monika Zalnieriute and Zofia Bednarz (eds), *Money, Power, and AI: Automated Banks and Automated States* (Cambridge University Press 2023). Zalnieriute specifically critiqued the scholars' approaches that focus solely on ensuring that legal procedures are compliant with the law. The challenge, therefore, is to complement this aspect with an understanding of the broader implications of procedural compliance, particularly its interaction with the socio-legal contexts in which technologies like FRT are deployed. This entails not only verifying legal adherence but also evaluating whether such compliance adequately safeguards fundamental rights and mitigates systemic risks inherent to the deployment environment. This is the aim of the methodology that is described *infra.*

[784] As explained in Chapter 4, this is also reflected in the structure of this thesis.

[785] See also the wording use by the AI Act, in Art. 27 and Rec. 93 and 96.

[786] See, also the analysis of the industry perspective as in Future of Privacy Forum, 'AI Governance behing the Scenes. Emerging Practices for AI Impact Assessments', December 2024.

Such an approach is particularly critical for evaluating the safety of the environment where FRT is deployed, considering both the authorization procedures and the mitigation strategies in place. This holistic perspective allows for a more thorough understanding of how FRT systems operate within their legal and societal context.

5.2.2 All rights are equal, but some are more at risk

Paraphrasing Orwell's well-known quote from his masterpiece 'Animal Farm', the point we wish to make here is explicitly that, while all CFREU rights are 'fundamental' in every sense, some, in specific contexts, may be more at risk than others, and therefore need to be analysed even more fully. [787]As introduced in Chapter 4, the concept of "higher risk" acknowledges that AI systems do not impact all rights equally. Each operational context amplifies certain risks, necessitating tailored safeguards that balance competing priorities while ensuring rights are upheld.

For instance, in the context of law enforcement, facial recognition technology amplifies risks to privacy, data protection, and access to an effective remedy due to extensive surveillance and sensitive personal data processing.[788] These rights are particularly vulnerable in this context, requiring robust safeguards such as judicial oversight, transparency, and proportionality in system deployment.

Instead, in other sectors, like healthcare, AI systems may predominantly affect access to healthcare and non-discrimination.[789] Algorithmic biases in diagnostic tools, for

[787] This is also witnessed by the fact that in the Guidelines published by the European Commission on the intepretation of Art. 5 in which a list of the "specific risks of harms is provided", see §377.

[788] Andrea Pin and Lucia Scaffardi, 'Tra Protezione Dei Dati e Intelligenza Artificiale, in Europa e Oltre' (2024) 64 DPCE Online; Paolo Francesco Levantino, 'Framing the Picture: A Human Rights-Based Study on AI, the Case of Facial Recognition Technology'; Nardocci (n 759); Rolando Tarchi and Andrea Gatti, 'Intelligenza Artificiale e Protezione Dei Dati Personali: Problemi Di Metodo e Di Procedura' (2024) 64 DPCE Online; Ferguson (n 385); Gabriela Villafuerte-Guerrero, 'Facial Recognition Systems under the European Union's Artificial Intelligence Act Seccion III: Dossier' (2024) 15 Revista de la Facultad de Jurisprudencia (RFJ) 173; Elizabeth McClellan, 'Facial Recognition Technology: Balancing the Benefits and Concerns' Journal of Business 19.

[789] Ludovica Durst, 'Il Trattamento Dei Dati in Ambito Sanitario, In', *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, a cura di Rocco Panetta.* (Giuffrè Francis Lefebvre 2019); Felix Busch and others, 'Navigating the European Union Artificial Intelligence Act for Healthcare' (2024) 7 npj Digital Medicine 1; Fidelia Cascini and others, 'Personalized Medicine Through Artificial Intelligence: A Public Health Perspective' in Alfredo Cesario and others (eds), *Personalized Medicine Meets Artificial Intelligence: Beyond "Hype", Towards the Metaverse* (Springer International Publishing 2023).

instance, can lead to unequal treatment of patients based on socio-economic or demographic factors, exacerbating healthcare inequities.[790]

Thus, one of the primary risks of horizontal or overly broad methodologies is that they may obscure the real rights at stake, treating all rights as equally affected across all use cases.

While fundamental rights are equal in principle,[791] their practical vulnerabilities vary significantly depending on the context and purpose of AI deployment. Ignoring this differentiation risks diluting the protection of the most at-risk rights and may lead to superficial evaluations that fail to address the real impacts of these technologies.

Additionally, such methodologies might inadvertently encourage deployers to assign relative importance or "grades" to different fundamental rights in order to navigate this overly broad framework.[792] This can result in an infringement of the Charter and in creation of dangerous precedent where certain rights are deprioritised or even breached in practice.

Instead, the proposed FRIA framework avoids this reductionist pitfall by emphasizing the concept of "higher risk." This ensures that rights are not compared or hierarchised but are instead addressed based on the specific and contextual threats they face.

The concept of "higher risk" also pushes the FRIA beyond a binary framework that focuses solely on identifying violations of fundamental rights. Instead, it encourages a more dynamic understanding of "interferences" with rights, recognising that risks often exist on a spectrum rather than as absolutes. As scholars[793] and the jurisprudence of the CJEU have noted,[794] most cases involve degrees of interference rather than outright violations.[795] This shift allows the FRIA to engage with the inherent complexity of

[790] Shirley Kempeneer, Sofia Ranchordas and Simone van de Wetering, 'AI Failure, AI Success, And AI Power Dynamics in the Public Sector' (Social Science Research Network, 11 October 2024) <https://papers.ssrn.com/abstract=4983622> accessed 3 December 2024.

[791] See Chapter 4, §4.2.

[792] The paper describes an industry approach but serves as a critical example to underline the risks entailed with giving grades to rights, Samuele Bertaina and others, 'Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act' (Social Science Research Network, 18 January 2024) <https://papers.ssrn.com/abstract=4698609> accessed 3 December 2024.

[793] Malgieri and Santos (n 179); Simona Demkova, 'The EU's Artificial Intelligence Laboratory and Fundamental Rights' (Social Science Research Network, 31 August 2023).

[794] For instance, as quoted by Malgieri, the CJEU in *Digital Rights Ireland*, para. 60, highlighting the importance of proportionality, emphasized the "extent and seriousness of the interference with the fundamental rights when assessing the validity of data retention measures".

[795] A concept widely used also by the ECtHR, as in *Roman Zakharov v. Russia*, 2015.

fundamental rights protection, ensuring that interferences are addressed in proportion to their severity and likelihood.[796]

Furthermore, an integral aspect of this methodology is its ability to address the chilling effects that may arise from AI deployment, particularly in public surveillance contexts, where the presence of AI systems might deter individuals from exercising their rights to freedom of expression, assembly, or association, as will be unpacked *infra.*

Such an approach also acknowledges that fundamental rights are not static or rigid towers but flexible constructs, that must adapt to the specific contexts in which they are applied.[797] Balancing these rights requires a framework that draws from diverse legal sources and traditions, ensuring that competing interests and values are accommodated while maintaining the essence of the rights concerned.

Therefore, the higher-risk methodology ensures that the FRIA framework aligns with the realities of AI deployment while preventing reductionist practices that could undermine the very rights it seeks to protect. It establishes a clear focus on actionable safeguards, balancing theoretical principles with practical solutions. These themes will be expanded upon in Chapter 6, which will address remedies and oversight mechanisms for FRT deployment, with a particular focus on the interplay between state authority and individual right. [798]

5.3 FRIA for FRT

Having explained the choices and the methods, and borrowing on the Commission's FRIA methodology, it is the moment for introducing the FRIA for FRT.

The first step involves mapping the potential risks to fundamental rights using the Fundamental Rights Checklist. This initial phase requires a thorough understanding of the legal foundations, primarily the CFREU, alongside other relevant human rights instruments. For instance, this might result in an evaluation of how law enforcement

[796] As noted by Malgieri, "the concept of interference is more appropriate than the term harm because not all interferences with fundamental rights can lead to quantifiable harm. Analogously, the concept of interference is more appropriate than "violation": the first is a gradual notion, while the latter is a yes-or-no notion", in Gianclaudio Malgieri, Vulnerability and Data Protection Law (Oxford University Press 2023).

[797] Kindt, 'The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing' (n 453).

[798] Bart van der Sloot and Sascha van Schendel, 'Procedural Law for the Data-Driven Society' (2021) 30 Information & Communications Technology Law 304.

agencies deploy FRTs in public spaces and the societal consequences of such deployments, such as chilling effects on public participation.

This could include Art. 7 and 8 of the CFREU, respectively, the right to privacy and data protection, and the right to non-discrimination under Art. 21. This list must be complemented with other secondary and related rights that may be indirectly affected (e.g., freedom of assembly in public surveillance contexts).[799] This mapping exercise ensures that the scope of rights at risk is fully understood before proceeding further.

The second step involves establishing a contextual understanding of the AI system and referencing historical precedents where similar systems have led to rights interferences.[800] For example, documented cases of facial recognition systems used in public surveillance may highlight risks of racial bias, privacy infringements, or chilling effects on public participation. Deployers of FRT must answer key guiding questions, such as:

- What is the system's intended purpose and operational context?
- Which populations or groups are most likely to be affected?
- What are the known risks from similar deployments in comparable environments?

This phase moves beyond theoretical concerns by anchoring the legal analysis in real-world applications. It provides a factual basis for evaluating potential interferences, their severity, and their likelihood, ensuring that the FRIA reflects both legal principles and practical implications. For instance, in the context of a law enforcement agency deploying facial recognition for public surveillance, the analysis should consider how such technology may deter individuals from exercising their right to protest, a fundamental right enshrined in Article 12 CFREU.[801]

Once risks are identified, mitigation measures must be designed and implemented to address them. For facial recognition systems, this entails ensuring transparency and

[799] Giuseppe Mobilio, 'L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?' (La democrazia della società digitale Tensioni e opportunità Atti del Convegno 3 dicembre 2021 Università di Milano-Bicocca 2023).

[800] Andrea Renda et al., 'Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe', April 2021.

[801] Monika Zalnieriute, 'Power and Protest: Facial Recognition and Public Space Surveillance' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

providing affected individuals with accessible information about the system's functioning, decision-making processes, and potential implications for their rights.[802]

Specific safeguards include but are not limited to:

- Granting individuals the right to be informed about the collection and use of their biometric data.
- Allowing individuals to contest decisions made using the system, ensuring access to fair trial and due process mechanisms.
- Establishing accessible remedies for violations of fundamental rights.
- Creating robust oversight frameworks, such as independent monitoring bodies, to ensure compliance with legal and ethical standards.
- Mandating prior authorisation from appropriate authorities, such as judicial oversight, to align system deployment with the principles of the rule of law and democratic accountability.

The last phase involves monitoring and reporting phases ensure the FRIA is not a one-time exercise but an ongoing process. Monitoring frameworks should track the actual impact of the system throughout its lifecycle, identifying any unforeseen risks or rights violations. Transparent documentation and regular reporting provide accountability, demonstrating that the deployer is meeting legal and ethical obligations.[803]

Once these steps are brought together, the FRIA for facial recognition systems is capable of not only identifying risks but also evaluating their severity and likelihood, ensuring alignment with fundamental rights, as well as flagging aspects of the normative framework that can be implemented to create a safer environment where the technology is deployed.

This is particularly crucial for biometric technologies, which have a history of significant privacy, non-discrimination implications and have been weaponised for anti-democratic purposes.

By embedding lessons from case law, integrating stakeholder perspectives, and employing dual-phase assessments, the FRIA achieves a comprehensive evaluation. The following table visualise the structured methodology and prepares the ground for

[802] See, the measures suggested by the Italian DPA, decisions no. 105, 106, 107, 108 and 109, 22 February 2024.

[803] 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), 24 May 2024.

implementing tailored safeguards that balance public security needs with the protection of fundamental rights.

Table 8 – Practical FRIA workflow.

Phase	Objective	Key Activities	Outputs
Contextual Analysis	Identify fundamental rights likely to be affected.	Review legal frameworks (e.g., CFREU and CJEU case law); Analyse the operational context and intended purpose of the AI system; Identify populations or groups most likely impacted.	Comprehensive rights mapping; Contextual risk scenarios (linked to real-world implications).
Case law integration	anchor the assessment in legal precedents.	Analyse relevant case law (e.g., Big Brother Watch and other CJEU cases); Extract patterns and lessons from similar deployments to guide risk analysis.	Case-informed risk models; Precedent-based understanding of interferences.
Risk assessment	Qualify and evaluate risks to fundamental rights.	Use risk matrices to combine likelihood and severity of potential rights interferences.	Detailed risk profiles.
Mitigation Measures	Develop and implement safeguards to address risks.	Design and evaluate safeguards, such as bias audits, technical adjustments, and transparency mechanisms; Establish oversight committees and independent monitoring processes; Ensure the involvement of stakeholders in mitigation design.	Comprehensive mitigation plan. Residual risk assessment identifying remaining vulnerabilities of the system.
Transparency and Reporting	Ensure accountability, adaptability, and stakeholder trust.	Publish public reports on risk identification and mitigation strategies; Conduct stakeholder consultations and incorporate feedback; Provide periodic compliance updates to oversight authorities.	Final FRIA report with detailed findings and actions. Real-time compliance and monitoring data for ongoing accountability.

By anchoring the FRIA process in both legal principles and practical realities, this approach ensures that sensitive AI systems, like facial recognition, are deployed responsibly and in compliance with EU law. It not only mitigates risks but also builds public trust in the technology by demonstrating a commitment to transparency, accountability, and rights protection.[804]

Thus, having established the critical need for evaluating the impact of biometric systems on fundamental rights, the next logical step is to systematically identify the specific rights at stake and assess the potential risks associated with these technologies. To this end, the FRIA framework introduced in Chapter 4 provides a structured methodology for mapping these risks. In this section, the focus shifts to operationalising the Fundamental Rights Checklist, a key component indeed of the FRIA methodology, by applying said checklist to biometric systems such as FRT. Furthermore, this analysis aims to pinpoint the rights most vulnerable to interference, including privacy, non-discrimination, and freedom of expression and assembly. Hence, the application of the checklist enables a nuanced understanding of how these rights are impacted in practice, as well as the safeguards required to mitigate these risks.

While the operational steps of FRIA are instrumental in assessing and mitigating the risks posed by FRT, its constitutional significance is often underappreciated. The FRIA, particularly as mandated for public authorities under Article 27 of the AI Act, must be understood as a normative mechanism, not only describing *how* FRT should be used, but delineating *whether* and *under what legal framework* it can be deployed in the first place.

The AI Act's requirements, clarified in the Commission's recent interpretation guidance, highlight that the FRIA must include a granular articulation of legal bases, a specification of the reference biometric databases, and a mapping of all categories of affected individuals, ranging from targets and suspects to bystanders in public. This makes the FRIA a *precondition* for deployment, not a retrospective accountability tool.

[804] As it is well specified by scholars with respect to the DPIA, but applies also here, these models should be considered as live resources that are tailored on the basis of the observed problem or technology. Hence, "providing a targeted, sector-specific knowledge base and method could be helpful with respect to the assessment of particularly complex or delicate processing operations, or to reduce the degree of discretion available to the assessor with respect to certain kinds of personal data processing". Lorenzo Dalla Corte and Rosamunde van Brakel, *Data Protection Impact Assessment Methods for the Urban Environment: A Report for the Commissie Persoonsgegevens Amsterdam (CPA)* (2022).

This thesis frames the FRIA, therefore, as a *normative constitutional safeguard*: an obligation aimed at ensuring that the entire context of AI use is legally permissible, proportionate, and necessary. This goes beyond the individual risk analysis: it anchors the deployment of biometric systems within a rights-respecting governance architecture. Public authorities are thus compelled not only to measure harm but to critically reflect on the legal and democratic legitimacy of their technological choices.

Following, the next section begins by examining each fundamental right in detail, integrating relevant case law and examples to illustrate the real-world implications of biometric systems.

5.3.1 Fundamental right's checklist

The main component of the FRIA analysis that will be assessed is the 'Fundamental Rights Checklist', which serves "to ensure the development of a truly mainstreamed approach to fundamental rights and provide guidance".[805]

Introduced in Chapter 4, this checklist is grounded in the principles of necessity, proportionality, and accountability, providing a structured methodology for the deployers to evaluate how AI systems impact fundamental rights.[806] By identifying rights at risk and proposing tailored safeguards, the checklist offers practical guidance for ensuring compliance with human rights standards in the deployment of these technologies. Moreover, this checklist integrates the concept of "higher risk," introduced in Chapter 4, which emphasises that AI systems do not impact all fundamental rights equally. Instead, the severity and likelihood of interferences vary depending on the operational context and technology deployed, such as biometric surveillance.

Especially, when applied to biometric technologies, deployed for law enforcement purposes, the checklist guides the deployers on finding the rights that are particularly vulnerable to interference. Incorporating the "higher risk" framework, this methodology

[805] Communication from the Commission Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM/2010/0573 final.

[806] The checklist is also assessed as a positive element, among other elements to implement the promotion of fundamental rights, in a survey conducted by the European Agency of Fundamental Rights (FRA), which was answered by European Agencies. See FRA, 'Challenges and opportunities for the implementation of the Charter of Fundamental Rights Opinion of the European Union Agency for Fundamental Rights', Opinion 4/2018, 24 September 2018.

identifies rights most vulnerable to interference, particularly in high-stakes deployments like biometric surveillance.

Therefore, to address the key question, "What fundamental rights are affected?", the analysis of case law identifies a core set of rights that are most impacted by biometric technologies: these include the rights to privacy and data protection, non-discrimination, and freedom of expression and assembly.[807] These rights emerge not only as frequent points of contention in court decisions but also as areas where the societal and individual impact of such technologies is most visible and consequential. While these rights are not exhaustive, they represent a critical starting point for understanding the broader implications of these systems.

Furthermore, it is important to distinguish that these rights, privacy, non-discrimination, and assembly, are not absolute in nature.[808] Unlike the prohibition of torture[809] or the protection of human dignity,[810] the "mother-right",[811] which cannot be subject to limitations under any circumstances,[812] these rights can be restricted under the conditions set out by the Charter.[813] However, any such limitation must adhere to clear

[807] While these rights represent a starting point for analysis, they are by no means exhaustive. A comprehensive evaluation must take into account the potential ripple effects on other fundamental rights, as the interplay between these rights often reveals complex, context-specific challenges.

[808] Eleanor Spaventa, 'The Horizontal Application of Fundamental Rights as General Principles of Union Law' (Hart Publishing 2011); Koen Lenaerts, Piet Van Nuffel and Tim Corthaut, 'Fundamental Rights and General Principles of Union Law' in Koen Lenaerts, Piet Van Nuffel and Tim Corthaut (eds), *EU Constitutional Law* (Oxford University Press 2021); Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779. Especially, on the link between Art. 7 and 8 of the Charter and the absence of absolute nature, see Gloria Gonzalez Fuster, *The Essence of the Fundamental Right to Data Protection: Background Paper Commissioned by the European Data Protection Supervisor (EDPS)* (European Data Protection Supervisor (EDPS) 2023); Gloria González Fuster and Raphaël Gellert, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' [2012] International Review of Law, Computers & Technology.

[809] European Parliament, Directorate General for Internal Policies, Citizen's Rights and Constitutional Affairs, Justice, Freedom and Security, Implementation of the EU Charter of Fundamental Rights and its impact on EU Home Affairs Agencies, Frontex, Europol and the European Asylum Support Office, 2011; Fundamental Rights Agency and Council of Europe, Fundamental rights of refugees, asylum applicants and migrants at the European borders, 2020.

[810] Eleanor Spaventa, 'Fundamental Rights in the European Union' (Oxford University Press 2020); Paul Craig and Gráinne de Búrca, '12. Human Rights in the EU', *EU Law* (Oxford University Press).

[811] Aharon Barak, *Human Dignity: The Constitutional Value and the Constitutional Right* (Cambridge University Press 2015).

[812] Pierfrancesco Grossi, 'Dignità umana e libertà nella Carta dei Diritti Fondamentali dell'Unione Europea' in M Siclari (ed.), *Contributi allo Studio della Carta dei Diritti Fondamentali dell'Unione Europea* (Torino, G Giappichelli, 2003) 41–46; Marco Ruotolo, 'Appunti Sulla Dignità Umana' (2010) 4 Direitos Fundamentais & Justiça 123; Catherine Dupré, 'Human Dignity in Europe: A Foundational Constitutional Principle' (2013) 19 European Public Law.

[813] CFREU, Art. 52, Lenaerts (n 459).

legal standards, ensuring that it is necessary to achieve a legitimate aim, proportionate to that aim, and preserve the essence of the rights concerned.[814]

When examining the impact of biometric systems, it becomes evident that these technologies often present a dual effect on fundamental rights. For instance, while they may enhance public safety by aiding law enforcement in identifying real or just potential threats, they simultaneously risk infringing on individual privacy, and, in the worst-case scenarios, also discouraging democratic participation.[815] This tension highlights the need for a nuanced evaluation of both the beneficial and detrimental effects these systems can have, particularly when their use could advance some rights (e.g., security and public order) while limiting others (e.g., freedom of expression).

Moreover, any limitation of fundamental rights through the use of biometric technologies must be carefully scrutinised. Such limitations must be formulated in a clear and predictable manner, providing individuals with transparency about how and why these systems are used. Beyond clarity, as mentioned, limitations to privacy, data protection, and freedom of expression must meet strict criteria: they should be necessary to achieve objectives of general interest or to protect the rights and freedoms of others, proportional to the desired aim, and respectful of the fundamental essence of the rights affected.

By applying the FRIA methodology hereby elaborated, the aim is to preemptively address the risks associated with the deployment of biometric technologies, particularly FRT. However, the practical application of this framework becomes most evident when juxtaposed with real-world cases. Thus, the ECtHR's judgment in *Glukhin v. Russia* provides an exemplary case study of the profound implications of deploying FRT without sufficient safeguards. The following paragraph, therefore, is going to frame this case in order to extract the critical fundamental rights that are particularly triggered by the

[814] "Article 52(3) of the Charter is intended to ensure that the rights listed in the Charter have the necessary consistency with the corresponding rights guaranteed in the ECHR, which must be taken into account as the minimum threshold of protection. […] [Therefore], any interference with the rights guaranteed by Article 8 can only be justified under Article 8(2) if it is in accordance with the law, pursues one or more of the legitimate aims to which Article 8(2) refers and is necessary in a democratic society in order to achieve any such aim. The measure must also be compatible with the rule of law, which is expressly mentioned in the preamble to the ECHR and inherent in the object and purpose of Article 8 thereof", Opinion of Advocate General Pitruzzella delivered on 27 January 2022, in C-817/19, Ligue des droits humains ASBL v Conseil des ministers.

[815] Among the most skeptics, Daragh Murray and Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 Israel Law Review 31.

deployment of FRT – which will be in-depth analysed as follows – highlight the risks but also propose the critical importance of the FRIA in safeguarding fundamental rights.

5.3.2 Which fundamental rights are affected?

Building upon the principles and methodology elaborated in the previous sections, the *Glukhin v. Russia* case provides a quintessential example of the key elements that should be considered when conducting a FRIA. It encapsulates the multi-faceted evaluation required to balance the deployment of AI systems with the protection of fundamental rights. This case ties directly to the foundational aspects discussed earlier, specifically: i) the dual need to evaluate both the specific use of the technology and the legal framework governing its deployment; ii) the importance of analysing interferences with fundamental rights, which, as highlighted, often occur across a spectrum rather than as outright violations; iii) the necessity of addressing chilling effects, particularly in high-stakes scenarios like public surveillance, where these effects can deter individuals from exercising their freedoms of expression and assembly.

The Glukhin case serves as a practical manifestation of the FRIA methodology in action. It underscores how a comprehensive evaluation must not only account for procedural compliance but also engage with the broader societal and legal implications of AI systems. This ensures that the rights most at risk are prioritized and safeguarded within their specific contexts.

Crucially, this case illustrates the interwoven nature of legal frameworks and practical applications, emphasizing that neither can be adequately addressed in isolation. By bridging theoretical principles with real-world applications, the Glukhin case demonstrates the critical value of FRIA as a tool for navigating the complexities of AI deployment in a manner that upholds fundamental rights.

The following analysis will unpack the Glukhin case in detail, demonstrating how its facts align with the FRIA framework and providing insights into the practical challenges and opportunities of safeguarding fundamental rights in high-risk AI deployments.

5.3.2.1 Case analysis: *Glukhin v. Russia* – A practical application of FRIA

Glukhin v. Russia[816] is the first case decided by an international court,[817] namely the ECtHR, about the use of face recognition technology by law enforcement that analysed the compatibility of such systems with the human rights enshrined in the ECHR.[818] As anticipated in the introduction to this chapter, the case, which involved the use of FRT to identify and arrest a protester, highlights fundamental rights infringements under Articles 8, 10, and 11 of the ECHR relating to privacy, freedom of expression, and freedom of assembly.[819]

First of all, the Court identified two distinct applications of FRT in this case. The authorities used images shared on Telegram and matched them with CCTV footage to retrospectively identify Glukhin as a protest participant. This might fall within the *ex post* use of face recognition, as per under Art. 6 of the AI Act; henceforth, those uses are classified just as "high risk" since there is a latency between the moment when the pictures are collected and matched with the individual.[820] Secondly, after the police identified Mr. Glukhin, they searched him through the use of "real-time" biometric systems to identify the location of the applicant in Moscow. The applicant was arrested on the same day at an underground station. Even though the Russian Government never

[816] Id. note no. 1 of this Chapter.

[817] As a matter of fact, previous cases regarded the use of wiretapping systems or the use of biometric data by the police, as in the famous *S. and Marper v. UK,* id. Indeed, in another case, the ECtHR, *Gaughran v. The United Kingdom*, App no 45245/15, 3 June 2020, para 37, the Court found that the UK's police ability to upload the facial images of the claimant 'from forces' local custody IT systems onto the Police National Database (PND) from which they could be enrolled in "the facial recognition gallery making them searchable using facial recognition software" constituted a violation of Article 8 of the Convention. Nonetheless, such a use of the data is not at all a face recognition *per se*, as it is in the case at hand. See also for this distinction Palmiotto and González (n 760).

[818] See §59 of the judgment on the admissibility.

[819] §88 "The Court observes that the applicant was prosecuted for a minor offence consisting of holding a solo demonstration without prior notification – an offence classified as administrative rather than criminal under the domestic law. He was never accused of committing any reprehensible acts during his demonstration, such as the obstruction of traffic, damage to property or acts of violence. It was never claimed that his actions presented any danger to public order or transport safety. The Court has already found that the administrative-offence proceedings against the applicant breached his right to freedom of expression. It considers that the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect in relation to the rights to freedom of expression and assembly".

[820] §71-73. However, as Mobilio has well noted, the Court remains on the surface of the distinction between 'a posteriori' and 'real-time' TRFs, without grasping the different legal implications arising therefrom, and, "nevertheless, the too general nature of these passages exposes the Court to a risk of abstractness and equivocality". Mobilio, 'La Corte EDU Condanna Il Ricorso Alle Tecnologie Di Riconoscimento Facciale per Reprimere Il Dissenso Politico: Osservazioni a Partire Dal Caso Glukhin c. Russia' (n 760).

explicitly admitted their use of FRT in real-time,[821] the Court accepted, in light of the particular circumstances of the case, that FRT was used as claimed by the application.[822] Therefore, such use would fall under Art. 5 of the AI Act, 'prohibited risk', which use is permitted under the conditions set out by the Regulation.[823]

It is true that the distinction between these applications is essential because they demonstrate varying levels of intrusiveness. *Ex post* analysis often focuses on specific individuals and may be defensible under stricter safeguards, whereas real-time applications transform surveillance from targeted monitoring into potentially universal scrutiny; therefore, as noted by the ECtHR, such uses require more robust justification as per their authorisation and procedural safeguards to avoid disproportionate infringements on rights.[824] However, as scholars as well as the scholarship affirmed, the impact on rights does not necessarily depend on the length of time in which biometric data are processed, given that a mass identification system is capable of identifying thousands of people in a matter of hours.[825] Therefore, if one really wants to grasp the danger of TRFs, one has to consider the policies and actual uses that are made of these means of biometric surveillance as a whole, since, as explained in Chapter 3, we are talking about just one type of technology: what differs is the use that is made of it.[826] However, the court in delimiting its *thema decidendum* does not go so far as to consider more broadly the risks associated with this technology in the broader framework of the fight against crime, but

[821] §60-63 of the judgment.
[822] §37, 69, 76, 87 of the judgment.
[823] Although these aspects were extensively discussed in Chapter 3 of this thesis, it is worth reiterating the key conditions outlined in the AI Act for the use of real-time biometric recognition tools in public spaces. Such systems may only be deployed to confirm the identity of specific individuals for law enforcement purposes and must adhere to strict criteria. These include considerations related to the nature of the situation, such as the severity, likelihood, and scope of harm that would arise if the system were not used, and the consequences for rights and freedoms, particularly evaluating the seriousness, likelihood, and extent of the impact on the rights and freedoms of all individuals affected.
[824] §89, "the use of facial recognition technology to identify the applicant from the photographs and the video published on Telegram – and *a fortiori* the use of live facial recognition technology to locate and arrest him while he was travelling on the Moscow underground – did not correspond to a "pressing social need".
[825] 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. In part., §31.
[826] As explained by Fussey et al., "AFR simultaneously expands and constrains spaces for police discretion and suspicion. These varied articulations challenge more deterministic readings of police technology and also the kinds of discursive frames promoted by the commercial developers and suppliers of these systems". See Pete Fussey, Bethan Davies and Martin Innes, '"Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing' (2021) 61 The British Journal of Criminology 325.

merely "whether the processing of the applicant's personal data was justified under Article 8 § 2 of the Convention in the present case".[827]

On the merits of the case, the ECtHR expands the scope of the right to private life, clarifying its contours when linked to the use of artificial intelligence technologies, such as biometric identification systems.[828] Drawing on its established jurisprudence regarding the collection and retention of individual data and images,[829] the Strasbourg Court seamlessly applies these principles to the case at hand, ultimately finding the interference suffered by the applicant to be unlawful. Facial recognition systems were evidently used both to identify the applicant during the protest and subsequently to locate him for the purpose of his arrest.

However, as required by Article 8 of the ECHR determining whether the interference violates the Convention necessitates an assessment of whether it meets the criteria outlined in the second paragraph of the provision.[830] In this regard, the Court places particular emphasis on the necessity for adequate regulatory frameworks to govern the use of such technologies. This insistence on robust regulation gains even greater urgency in light of the rapid and increasingly sophisticated development of artificial intelligence technologies.[831] In this sense, the Court's explicit and unequivocal stance highlights the need for legal systems to keep pace with technological advancements to safeguard individual rights effectively. This leads towards the concept of a 'minimum standard of guarantees essential for the protection of fundamental rights', which the Court deems indispensable.[832]

---

[827] §85. On the critics of this choice, see Monika Zalnieriute, 'Glukhin v. Russia. App. No. 11519/20' (2023) 117 American Journal of International Law 695.

[828] Nardocci (n 760).

[829] *Ex multis,* ECtHR (Grand Chamber), *S. and Marper v. the United Kingdom*, App. nos. 30562/04 and 30566/04, 2008; ECtHR (Grand Chamber) *Rotaru v. Romania*, no. 28341/95, 2000.

[830] William A Schabas, 'Right to Respect for Private and Family Life/Droit Au Respect de La Vie Privée et Familiale' in William A Schabas (ed), *The European Convention on Human Rights: A Commentary* (Oxford University Press 2015) <https://doi.org/10.1093/law/9780199594061.003.0013> accessed 12 January 2025; Mart Susi, 'European Convention on Human Rights - Freedom of Expression - Right to Privacy - Responsibility of Internet News Portal for Defamatory Comments Posted by Readers' (2014) 108 The American journal of international law 295.

[831] §83, "the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, supervisory control mechanisms and available remedies".

[832] §77, "in the context of the collection and processing of personal data, it is therefore essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data, and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness".

Hence, the automated identification of Glukhin and the lack of legal safeguards in Russian law rendered the surveillance unlawful. Specifically, the Court highlighted the absence of mandatory documentation of FRT use, the failure to notify individuals subjected to surveillance, and the lack of clear, accessible rules governing such measures. A crucial point is indeed the emphasis on the "quality of law" standard under Article 8, which, as a criterion elaborated by the ECtHR, requires that any limitation on fundamental rights must be clearly defined and provide adequate procedural guarantees.[833] Scholars, looking at how the Strasbourg Court applied this criterion, underscore how it arbitrarily especially in cases regarding surveillance and interpretation of Art. 8 ECHR.[834] Thus, in *Glukhin,* the Court noted that the Russian law was "widely formulated" and did not contain "any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or the processing of sensitive personal data".[835]

However, this procedural focus has drawn criticism. Scholars[836] argue that the Court's emphasis on procedural safeguards overlooks the substantive legality of surveillance regimes, potentially legitimising FRT use in more severe policing scenarios, such as combating violent crimes. This critique suggests that by focusing on procedural failings, the Court inadvertently left open the possibility for FRT to be used under stricter procedural frameworks, even in cases where substantive rights are at risk. Frankly, in defence of its approach, the Court balanced procedural and substantive considerations when assessing whether FRT use was "necessary in a democratic society."[837] It explicitly considered factors such as the peaceful nature of the protest, the lack of violent conduct

[833] The doctrine of "quality of law," as developed by the ECtHR under Article 8 ECHR, underscores that any interference with the right to privacy must be not only lawful but also meet specific qualitative standards of accessibility, foreseeability, and necessity in a democratic society. Accessibility requires that the law be publicly available and understandable, while foreseeability mandates that individuals can predict the implications of the law and adjust their behaviour accordingly. Necessity demands proportionality, ensuring that any interference aligns with legitimate aims and is justified within a democratic framework. This analysis is particularly relevant in the context of emerging technologies like FRT, where the potential for misuse and overreach underscores the need for robust legal and procedural protections. For further details, see ECtHR judgments in *Centrum för Rättvisa v. Sweden*, App. no. 35252/08, 25 May 2021.

[834] Bart van der Sloot, 'The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases' (2020) 11 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 160.

[835] §83.

[836] Monika Zalnieriute, 'Against Procedural Fetishism: A Call for a New Digital Constitution' (2023) 30 Indiana Journal of Global Legal Studies 227.

[837] §80-83.

by Glukhin, the potential for a chilling effect on public dissent, and the sensitive nature of biometric data. The ruling therefore underscores that procedural safeguards must be tailored to the gravity of the underlying offenses, the extent of automated processing, and the broader democratic implications.[838]

Exactly on this delicate balance, it is really to underline how the Court broads the focus not only on the interferences on the right to privacy, but also considers what legal scholars refer to as the 'chilling effects' generated by the widespread use of facial recognition technologies.[839] These effects arise from individuals becoming aware that their actions are being monitored through public surveillance systems, which can lead to changes in their behaviour and habits.[840] In essence, the mere presence of such surveillance may discourage people from exercising their freedoms fully, particularly their rights to freedom of expression and assembly. Interestingly, while the Court only briefly touches on the implications for these additional rights,[841] its reasoning suggests that the large-scale deployment of facial recognition technologies could have far-reaching consequences beyond privacy. By highlighting this, the judgment serves as a broader warning about the risks such technologies pose to democratic principles, including the fundamental freedoms of expression and assembly.[842] Even if facial recognition systems could, in theory, be used in compliance with the Convention under specific circumstances, the judgment underscores the inherent dangers they pose to fundamental rights if left unchecked.

From this brief analysis, it emerges that this case provides significant lessons for the application of the FRIA framework, especially in evaluating the deployment of FRT.

[838] Mobilio, 'La Corte EDU Condanna Il Ricorso Alle Tecnologie Di Riconoscimento Facciale per Reprimere Il Dissenso Politico: Osservazioni a Partire Dal Caso Glukhin c. Russia' (n 760).
[839] Nardocci (n 760).
[840] Moritz Büchi and others, 'Chilling Effects of Profiling Activities: Mapping the Issues' [2019] Available at SSRN 3379275.
[841] §49-57.
[842] The Court focused plainly just on Article 10 ECHR alone, declaring the violation of Article 11 ECHR absorbed in it, stating that it includes in the review of the alleged violation of Article 10 ECHR also the principles enshrined under Article 11 ECHR according to the orientation inaugurated in ECtHR, *Novikova and Others v. Russia*, [Third Chamber], nos. 25501/07, 26 April 2016, § 91, in which the Court expresses the view that it is not necessary to proceed to an examination of the invoked infringement of Article 11 ECHR since these were individual protests and not carried out together with other subjects and, however, at the same time emphasises the need not to exclude a broad reading of Article 10 ECHR that would also enhance, if relevant, the principles enshrined in Article 11 ECHR.

Henceforth, departing from the Strasbourg context and then moving towards the Brussels environment, it is possible to draw helpful lessons from this case.

By dissecting the Court's analysis, it becomes evident that an effective FRIA must strike a balance between procedural safeguards and substantive considerations, ensuring that biometric systems align with democratic principles and do not disproportionately infringe on fundamental rights.

Nonetheless, one of the most critical takeaways from *Glukhin* is the emphasis on necessity and proportionality as cornerstones of lawful interference with fundamental rights. First, the Court's decision underscored that for FRT to be justified, its deployment must be indispensable to achieving a legitimate aim, such as ensuring public safety. However, the Russian authorities failed to demonstrate that the use of FRT was essential in this case. The protest was peaceful, and there was no indication of imminent threats that would have warranted such intrusive measures. This highlights the need to stress in the FRIA whether alternatives were rigorously evaluated, or less intrusive means could achieve the same objective, thereby minimising harm to privacy, freedom of expression, and assembly, as seen *supra.*

Finally, the case highlights the need for substantive proportionality assessments that go beyond mere procedural compliance. While the Court has been criticised for focusing heavily on procedural safeguards, it implicitly reinforced the principle that procedural safeguards must be paired with substantive evaluations of whether the surveillance aligns with democratic values and respects the essence of fundamental rights. Frankly, it is not overseen and enforced correctly, also from a procedural perspective, the norms risk being substantially perfect, but poorly applied. Though, it is true that the two aspects should go hand in hand: this dual approach is essential for FRIA to serve as an effective tool in mitigating the risks associated with biometric technologies.

The *Glukhin* case ultimately reinforces the importance of embedding both procedural and substantive safeguards into the deployment of FRT. Procedural safeguards ensure that the technology is used transparently and accountably, while substantive assessments evaluate whether its use is necessary, proportionate, and aligned with democratic principles. These insights will guide the subsequent sections, where the FRIA methodology will be applied to analyse the specific rights most at risk from FRT deployment, including data protection, and democratic freedoms.

5.4. Test: Art. 8 CFREU, data protection

This section is, hence, devoted to the testing of the model with one of the fundamental rights mostly triggered by the use of facial recognition technology: data protection.[843]

As a matter of fact, the rise of data protection as a fundamental right, particularly within Europe, reflected the growing need to address concerns related to data-determinism and the protection of individuals' autonomy.[844] This holds true in the very text of Article 8 of the CFREU:[845] while para. 1 guarantee that personal data concerning individuals must be protected, the second one establish the core principles of the data processing – hence, that personal data must be processed fairly, for specified purposes, and on the basis of consent or another lawful basis. Finally, the third paragraph requires compliance with data protection principles to be monitored by an independent authority, reinforcing accountability and trust.

In a nutshell, the aim of this right is, on the one hand, to concentrate control over data to individuals,[846] and, on the other, to make data controllers accountable and compliant with their obligations.[847]

---

[843] Simone Kuhlmann, 'Government Use of Facial Recognition Technologies under European Law' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

[844] Orla Lynskey, *The Foundations of EU Data Protection Law* (University Press 2015); Orla Lynskey, 'Article 8: The Right to Data Protection', *The EU Charter of Fundamental Rights in the Member States* (Hart Publishing 2020); Maximilian von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (2020) 6 European Data Protection Law Review 509; Paul de Hert and Juraj Sajfert, 'Regulating Big Data in and out of the Data Protection Policy Field: Two Scenarios of Post-GDPR Law-Making and the Actor Perspective' (2019) 5 European data protection law review (Internet) 338.

[845] Article 8: "1. Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. 2. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority." Simone van der Hof and others, 'Articles 7 and 8 Fundamental Rights Charter and Article 16 TFEU – Commentary', *Concise European Data Protection, e-Commerce and IT Law* (Kluwer Law International 2018); Orla Lynskey, 'Article 8: The Right to Data Protection', *The EU Charter of Fundamental Rights in the Member States* (Hart Publishing 2020); Bart van der Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?', *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International Publishing 2017).

[846] GDPR, Articles from 15 to 22. Michèle Finck, 'The Maturation of European Data Law: From Fundamental Rights to Economic Rights' in Jeremias Adams-Prassl and others (eds), *The Internal Market Ideal: Essays in Honour of Stephen Weatherill* (Oxford University Press 2024); Fuster and Gellert (n 51).

[847] That is the case, for instance of the widely discussed DPIA. Refer also to Christopher Docksey, 'Article 24 Responsibility of the Controller' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020); Lee A Bygrave, 'Article 25 Data Protection by Design and by Default' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

Historically, privacy was understood as a negative right – the "right to be let alone," [848] as famously articulated by Warren and Brandeis in 1890.[849] However, data protection goes beyond merely shielding individuals from interference; it has evolved into a positive right, requiring proactive regulatory measures to safeguard personal data.[850] This shift is particularly evident in the European Union, where privacy and data protection are enshrined as distinct but complementary rights in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[851]

Therefore, Europe's emphasis on data protection is deeply rooted in its historical experience, particularly the trauma of the Second World War. During this period, vast amounts of personal data – collected and categorised based on ethnicity, political beliefs, and other attributes – were weaponised to oppress and marginalise individuals.[852] These historical lessons underpin Europe's commitment to dignity and human rights, contrasting sharply with the U.S. approach, which prioritizes liberty and adopts a more fragmented, sectoral framework for privacy regulation.[853]

The protection of personal data has reached a new step of consolidation not only in the aftermath of Lisbon thanks to the role of the CJEU,[854]but also with the adoption of the GDPR. Developing the framework that empowers the data subjects with rights and poses

[848] Bart van der Sloot, 'The Right to Be Let Alone by Oneself: Narrative and Identity in a Data-Driven Environment' (2021) 13 Law, Innovation and Technology 223.

[849] Warren and Brandeis (n 387).

[850] Maria Tzanou, *The Fundamental Right to Data Protection : Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017).

[851] Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009); Giuseppe Martinico, 'Art. 7. Rispetto Della Vita Privata e Della Vita Familiare', *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè, 2017); Oreste Pollicino and Marco Bassini, 'Art. 8. Protezione Dei Dati Di Carattere Personale', *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè 2017).

[852] Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864; Michèle Finck, 'The Maturation of European Data Law: From Fundamental Rights to Economic Rights' in Jeremias Adams-Prassl and others (eds), *The Internal Market Ideal: Essays in Honour of Stephen Weatherill* (Oxford University Press 2024).

[853] Woodrow Hartzog and Neil Richards, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 Boston College Law Review 1687; James Q Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2003) 113 Yale Law Journal 1151. Specifically, Whitman speaks of a "transatlantic clash", more recently also reaffirmed by Oreste Pollicino, 'The Transatlantic Dimension of the Judicial Protection of Fundamental Rights Online' (Brill 2024).

[854] Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (n 5).

them in control of their data, the GDPR)[855] served this scope. It is not merely a regulatory tool; it represents the EU's broader commitment to upholding human dignity, autonomy, and privacy in the face of emerging digital technologies.[856]

The entire structure of the GDPR is based on general principles which orbit around the accountability of the data controller, who should ensure and prove compliance with the system of data protection law.[857] Even when the data controller is not established in the Union,[858] the GDPR increases the responsibility of the data controller which, instead of focusing on merely complying with data protection law, is required to design and monitor data processing by assessing the risk for data subjects.[859]

However, as scholars explain, the digital age has heightened the need for individuals to actively control their personal data, making data protection an essential counterbalance to the pervasive collection practices of both state and private actors.[860] In particular, van der Sloot notes that traditional data protection – like consent, control, and transparency – are challenged by AI:[861]

> "For a long time, two strategies to privacy and data protection have been deployed: control over personal data by citizens or legal obligations on data controllers with governmental control. Both worked relatively well, often in a mixed form, for decades. Yet, new data technologies that have emerged since the beginning of this millennium and the data infrastructure that exists today make both strategies virtually unable to

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

[856] Pollicino, 'The Transatlantic Dimension of the Judicial Protection of Fundamental Rights Online' (n 96); Giovanni De Gregorio (ed), 'Digital Constitutionalism, Privacy and Data Protection', *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022); Edoardo Celeste and Giovanni De Gregorio, 'Digital Humanism: The Constitutional Message of the GDPR' (2022) 3 Global Privacy Law Review.

[857] Ibid, Art 5.

[858] Ibid, Art 3(2).

[859] Raphaël Gellert, 'Risk and the Risk-Based Approach: Between Data Protection Risks and Compliance Risks' in Raphaël Gellert (ed), *The Risk-Based Approach to Data Protection* (Oxford University Press 2020) ; Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502; Giandonato Caggiano, 'Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione' 18.

[860] Lynskey, *The Foundations of EU Data Protection Law* (n 87).

[861] Bart van der Sloot, 'The Production of and Control over Data in the AI-Era: The Two Failing Approaches to Privacy Protection' in Alberto Quintavalla and Jeroen Temperman (eds), *Artificial intelligence and human rights* (Oxford University Press 2023).

provide adequate protection in the twenty- first century. Citizens do not have the knowledge, power, and time to control their data, and an additional problem is that their autonomy is affected by modern data practices. Governments do not have the knowledge, power, and time to control all data processes, and an additional problem is that if they would, this might lead to a totalitarian infrastructure."[862]

These holds true also when FRTs are deployed: the risk is high of collecting data without the actual knowledge of the data subject.[863] Therefore, unlike voluntary data collection practices, i.e., those based on consent, these systems rely heavily on non-consensual biometric data capture.[864] Individuals in public spaces are often unaware that their faces are being recorded, processed, and matched against expansive databases.[865] This creates a pervasive surveillance environment that disrupts the balance between ensuring public safety and safeguarding personal rights.[866]

Having briefly outlined the main contents of Article 8 and the disruptive interplay between data protection principles and AI; we now shift our focus to a detailed examination. Having in mind the fundamental right's checklist, as a structured framework, this section explores the specific limitations and interferences that deployers must critically assess when evaluating their compliance with this fundamental right.

---

[862] Id., in part. p. 174.

[863] As clarified by the Italian Data Protection Authority, "when video-surveillance systems are used, the data controller, in addition to providing first level information by means of warning signs in the vicinity of the area subject to video-surveillance, must also provide data subjects with 'second level information', which must 'contain all the compulsory elements pursuant to Article 13 of [the Regulation]' and 'be easily accessible to the data subject, for example by means of a comprehensive information page made available at a central junction [...] or posted in an easily accessible place", Sanction 5/2024, doc. web n. 9977020.

[864] This is in the very nature of the FRT and the purpose of collecting personal data in the context of law enforcement. Art. 8, Directive (EU) 2016/680 specifies that any processing of personal data must be based on the law and be legitimate, i.e., comply with all the data protection principles. In a narrower sense, the principle of lawfulness of processing denotes that such processing must have a legal basis or be laid down by the law in accordance with the named Article.

Instead, Article 8 para. 2 requires that Member State law regulating processing within the scope of the Law Enforcement Directive should specify "at least the objectives of processing, the personal data to be processed and the purposes of the processing". Maria Tzanou, 'Article 8 LED. Lawfulness of Processing' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enfocemente Directive (LED): a commentary* (Oxford University Press 2024).

[865] Yichun Shi and Anil K Jain, 'Uncertainty-Aware Face Recognition' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024).

[866] Genia Kostka, Léa Steinacker and Miriam Meckel, 'Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States' [2021] Public Understanding of Science 09636625211001555.

To address these challenges, this section examines three interconnected clusters of concerns: (1) whether data used in the training and modelling phases qualifies as personal data under the GDPR; (2) the legality and ethicality of utilising publicly available images for model development; and (3) compliance with data retention and erasure obligations.

These clusters are chosen not only because they are the expression of the concepts enshrined in Article 8 of the CFREU. For instance, the opacity and scale of data usage for the purpose of training FRT or use of these systems make it difficult for individuals to fully understand or control how their personal data are processed,[867] harnessing the true colours of Art. 8, being that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". Therefore, by analysing these three elements, it would be possible to move from the "checklist" to the concrete addressing of the issues to find potential solutions.

Specifically, cluster 1 addresses the foundational question of whether the data used during the training and modelling phases of FRT constitutes "personal data" as defined by Article 4 para. 1 of the GDPR. This determination is critical because it dictates whether the GDPR's protections and obligations apply from the very outset of the technology's development. Given that FRT quasi-exclusively relies on biometric data, which is considered a special category of personal data under Article 9 GDPR. Understanding this helps ensure that data protection principles are embedded throughout the lifecycle of FRT, not just during deployment.[868]

---

[867] Bart Custers and Gianclaudio Malgieri, 'Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data' (19 January 2022) <https://papers.ssrn.com/abstract=4329245> accessed 16 February 2024.

[868] This aspect was the object of the analysis of the Court of Justice of the European Union, Judgment of 7 December 2023, Schufa Holding v., C-634/21, concerning the inclusion within the umbrella of the object of data subject's rights also the *ex ante* decision, in that case, the credit-scoring evaluation, was to be considered to fall under the scope of GDPR, especially, Art. 22. This provision establishes that individuals have the right not to be subjected to decisions based solely on automated processing, including profiling when these decisions produce legal effects or significantly affect the person. In the *Schufa* case, the Court confirmed that such evaluations fall within the protective framework of the GDPR, even before any subsequent decision is made based on automated processing. This principle is especially relevant in the context of an FRT where the initial evaluation, identifying or verifying an individual, may occur before a secondary decision, such as its use for law enforcement purposes. For instance, FRT 'processed' data might form the basis for issuing an order that restricts an individual's freedom. Such scenarios raise significant questions about the interplay between automated decision-making and fundamental rights, particularly when legal or significant effects arise from automated evaluations. A parallel debate has emerged concerning whether large language models (LLMs) store personal data. The Hamburg Data Protection Authority (DPA), in a white paper, concluded that LLMs do not inherently store personal data but remain subject to data protection rules in several ways. Conversely, the Irish Data Protection Commission (DPC)

Following, cluster 2 examines the legality and ethicality of using publicly available images for model development. While such images are accessible, their use in training FRT models raises complex issues related to consent, purpose limitation, and fairness. The GDPR stipulates that personal data collected for one purpose should not be repurposed without proper legal basis, and public availability does not negate an individual's data protection rights. This cluster is essential in assessing whether the practices of collecting and processing publicly available images align with data protection laws and ethical standards, especially considering the potential for misuse and discriminatory outcomes. [869]

Finally, the third cluster focuses on compliance with data retention and erasure obligations, as well as the procedural enforcement and exercise of data subject rights. The GDPR mandates that personal data should be kept no longer than necessary, as per Article 5, para. 1, lett. e), and grants individuals rights to access, rectify, and erase their data, due to Artt. 15-17, and Art. 16 of Directive (EU) 2016/689. In the context of FRT, adherence to these principles is paramount. This cluster also emphasises the importance of procedural mechanisms that enable individuals to enforce their rights effectively. Without robust enforcement and accessible procedures, the rights enshrined in the GDPR risk being theoretical rather than practical protections.[870]

---

has highlighted the risks of "memorisation" in AI models, where personal data from training datasets may be unintentionally reproduced in outputs generated by the model. This raises additional concerns about the implications of automated processing for privacy and data protection frameworks, as well as the broader scope of GDPR's application to advanced AI systems. See Hamburg Commissioner for Data Protection and Freedom of Information, 'Discussion Paper: Large Language Models and Personal Data', 2024; Irish Data Protection Commission, 'AI, Large Language Models and Data Protection', 2024; finally, from a different perspective, Lokke Moerel and Marijn Storm, 'Do LLMs "store" Personal Data? This Is Asking the Wrong Question' <https://iapp.org/news/a/do-llms-store-personal-data-this-is-asking-the-wrong-question> accessed 3 December 2024.

[869] One of the primary concerns regarding the use of Clearview AI software in the EU is its ability to automatically collect images of individuals' faces from a wide range of online sources, including employment sites, news platforms, educational websites, and social media networks such as Facebook, YouTube, Twitter, Instagram, and even Venmo. This capability raised significant questions about the legality of such practices under GDPR, particularly in relation to the principles of lawfulness, fairness, and transparency (Article 5 GDPR) and the necessity of explicit consent for processing biometric data (Article 9 GDPR). The indiscriminate scraping of publicly available images without users' knowledge or consent has drawn scrutiny from European Data Protection Authorities, highlighting the software's profound implications for privacy and data protection rights. For an analysis of the EU reactions to Clearview AI, see Kohn (n 454); Benjamin Sobel, 'HiQ v. LinkedIn, Clearview AI, and a New Common Law of Web Scraping' [2020] LinkedIn, Clearview AI, and a New Common Law of Web Scraping (April 21, 2020).

[870] Effective exercise of these rights depends on transparent processes and responsive data controllers. Procedural enforcement involves ensuring that individuals are informed about their rights and have accessible means to exercise them. This includes clear communication channels, timely responses to requests, and remedies in case of non-compliance. For FRT systems, which often operate opaquely and

5.4.1 Cluster 1: training and modeling – are these personal data?

The classification of data used in the training and modelling phases of FRT is foundational to understanding their compliance with data protection frameworks, particularly the GDPR and the LED. The lifecycle of biometric systems begins with the collection and preparation of datasets that are then used to train the deep learning models.[871] This phase, while often less visible in discussions of data protection, is critical because it sets the stage for how the system operates, what risks it poses, and how data protection principles apply. The GDPR's applicability hinges on whether the data used qualifies as "personal data," and how this data is handled during the training phase is a determinative factor for the extent of compliance.[872]

Specifically, under Article 4 para. 1 GDPR, "personal data" includes any information relating to an identified or identifiable natural person.[873] This "law of everything"[874], as interpreted by the CJEU in cases such as *IAB Europe v. Gegevensbeschermingsautoriteit,*

involve complex data processing activities, facilitating the exercise of these rights is particularly challenging yet essential. Moreover, supervisory authorities play a critical role in enforcing data protection laws and handling complaints. Adequate enforcement mechanisms deter violations and promote accountability among organizations deploying FRT. Without effective procedural enforcement, the protections offered by the GDPR and other data protection frameworks cannot be fully realized, leaving individuals vulnerable to infringements of their privacy and autonomy. The specific issue connected with granting access to effective remedies is going to be analysed in Chapter 6.

[871] For a technical explanation of the functioning of FRT, it is recalled the analysis in Chapter 3 of this thesis.

[872] The EDPB in its opinion defines AI models as "those developed through a training process. Such training process is a part of the development phase, where models learn from data to perform their intended task. Therefore, the training process requires a dataset from which the model will identify and 'learn' patterns. In these cases, the model will use different techniques to build a representation of the knowledge extracted from the training dataset. This is notably the case with machine learning. In practice, any AI model is an algorithm, whose functioning is determined by a set of elements. For example, deep learning models are often in the form of a neural network with multiple layers consisting of nodes connected by edges that have weights, which are adjusted during training to learn the relationships between inputs and outputs. The characteristics of a simple deep learning model would be: (i) the type and size of each layer, (ii) the weight attributed to each edge (sometimes called 'parameters'), (iii) the activation functions between layers, and possibly (iv) other operations that may happen between layers. For instance, when training a simple deep learning model for image classification, inputs (the "image pixels") will be associated with outputs, and weights may be adjusted, so as to produce the right output most of the time." See EDPB, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models', 17 December 2024, p.11.

[873] Lee A Bygrave and Luca Tosoni, 'Article 4(1). Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[874] Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40.

includes any information related to an identified or identifiable individual,[875] where identifiability can be established directly or indirectly.[876]

For FRT, this means that facial images, behavioural patterns, or other biometrics used for training are likely to trigger data protection obligations, particularly when combined with auxiliary datasets that increase the likelihood of identification.[877] As recently clarified by the EDPB,

> "AI models, regardless of whether they are trained with personal data or not, are usually designed to make predictions or draw conclusions, i.e. they are designed to infer. Furthermore, AI models trained with personal data are often designed to make inferences about individuals different from those whose personal data were used to train the AI model." [878]

The authority also noted that most of such models, when trained of personal data, are taught to infer characteristics on individuals.[879] In these cases, such AI models include information relating to an identified or identifiable natural person "and so will involve the processing of personal data". Hence, saying it differently, it is not only to be considered whether the AI is trained with personal data to apply the relevant law, but also

[875] The concept is broken down by the WP29 in the famous opinion on the concept of personal data as "Personal data is: (a) information, (b) relating to (c) an identified or identifiable (d) natural person". See, WP 136, 'Opinion 4/2007 on the concept of personal data', 20 June 2007.

[876] Importantly, the Court noted that it is not necessary for a piece of information to independently identify an individual; rather, it suffices if the data, when combined with additional information accessible to the data controller, allows for identification. Recital 26 GDPR further establishes that identifiability is assessed based on "reasonable means," meaning that a controller need not possess all the necessary information for identification but must be in a position to access it without disproportionate effort. In the case at hand, the CJEU determined that a TC String, although not containing elements that directly identify a data subject, still qualifies as personal data because it includes user-specific preferences. If linked to an identifier such as an IP address, the TC String could single out and identify an individual. The Court underscored that the inability of the IAB to directly combine the TC String with other identifiers was irrelevant. The decisive factor was that IAB, as the data controller, had the authority to request such additional information from its members, satisfying the 'reasonable means' threshold for identification.

[877] Ali Akbari, 'Facial Recognition Technologies 101: Technical Insights' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

[878] EDPB, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models', id.

[879] As explained in Chapter 2, this is the very feature that distinguish AI from previous technologies, the ability to infer features and elements. See §2.2 and, in part., §2.2.1.

the fact that, by inferring, the system is able to produce or simply reveal information about natural persons, as in the case of generative AI or deep learning, like FRT.[880]

Furthermore, a significant debate exists about the classification of data models as personal data under the GDPR.[881] This refers not only to machine learning models, but more broadly, to the concept of 'computer code'.[882] This debate centres on two primary issues: whether individuals whose data were part of the training dataset are identifiable through the model and whether applying GDPR to these contexts is desirable or practical.[883]

Scholars such as Veale, Binns, and Edwards argue that model inversion and membership inference attacks – hence, techniques used to extract or infer training data – demonstrate that ML models can sometimes qualify as personal data.[884] They contend that models may constitute pseudonymised personal data because, when combined with additional information, such as auxiliary datasets, individual re-identification becomes possible. Furthermore, they cautiously support extending GDPR principles to ML models to enhance transparency and accountability. In contrast, Leiser and Dechesne take a more critical stance,[885] asserting that such an application would stretch GDPR's scope too far, particularly because any re-identification attacks on ML models would likely involve illegal activities. They also caution against overextending GDPR's applicability to algorithms, arguing that this could lead to over-inclusivity and potential regulatory

[880] "The EDPB considers that, even when an AI model has not been intentionally designed to produce information relating to an identified or identifiable natural person from the training data, information from the training dataset, including personal data, may still remain 'absorbed' in the parameters of the model, namely represented through mathematical objects. They may differ from the original training data points, but may still retain the original information of those data, which may ultimately be extractable or otherwise obtained, directly or indirectly, from the model. Whenever information relating to identified or identifiable individuals whose personal data was used to train the model may be obtained from an AI model with means reasonably likely to be used, it may be concluded that such a model is not anonymous", *ibidem,* §31.

[881] The debate is live and does not have a clear solution yet. According to Wachter and Mittelstadt, data inferred by an algorithm is not personal data and hence does not fall within the GDPR. Wachter and Mittelstadt (n 129).

[882] "The distinction between an algorithm and a computer program implementing that algorithm has disappeared, and a computer program implementing algorithms is called an algorithm", as noted by Nadezhda Purtova and Ronald Leenes, 'Code as Personal Data: Implications for Data Protection Law and Regulation of Algorithms' (2023) 13 International Data Privacy Law 245.

[883] EDPB, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models', id.

[884] Michael Veale, Reuben Binns and Lilian Edwards, 'Algorithms That Remember: Model Inversion Attacks and Data Protection Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180083.

[885] MR Leiser and Francien Dechesne, 'Governing Machine-Learning Models: Challenging the Personal Data Presumption' (2020) 10 International Data Privacy Law 187.

overreach. Expanding this discussion, Purtova and Leenes bring a broader perspective, exploring whether computer code, in general, could be classified as personal data.[886] They emphasise that code, including its outputs and design, often contains information that relates to individuals. This information may not always be semantic (directly meaningful, such as a name or identifier) but can also be syntactic, functional data that influences reality, such as behaviour, preferences, or decisions.[887]

This issue is not merely technical but has practical and regulatory implications on FRT, as these systems rely heavily on biometric data for training and modelling. Especially, as also clarified by the Spanish Data Protection Authority, it is deemed crucial to recognise AI systems as means rather than ends:[888] a shift that makes it possible to underscore the controller's accountability in designing processing activities that are compliant with the GDPR since the beginning, and not just in the delivery of the output. In this sense, controllers must ensure that the use of AI aligns with the intended purposes and complies with data protection obligations, including assessing risks to data subjects' rights and freedoms.

Therefore, if FRT models are considered personal data, this would extend GDPR protections, such as transparency, purpose limitation, and accountability, to the pre-deployment phase, addressing key concerns about dataset composition, data subjects' rights, consent, principle of minimisation. Given the risks posed by FRT, including potential re-identification and the chilling effect on fundamental rights like privacy and freedom of assembly, treating these models as personal data could reinforce safeguards, ensuring their design and deployment align with data protection principles and broader democratic values.[889] As scholars point out, training datasets derived from publicly available sources often exacerbate risks by including facial images that individuals have no knowledge are being used, nor have they consented to such use.[890]

---

[886] Purtova and Leenes (n 882).

[887] In particular, they argue that the GDPR's broad definition of personal data, encompassing "any information" relating to an identifiable person, could apply to code because it relates to individuals in its content, purpose, or effect.

[888] AEPD, 'AI: System vs Processing, Means vs Purposes', 10 April 2023, <https://www.aepd.es/en/prensa-y-comunicacion/blog/ai-system-vs-processing-means-vs-purposes>, accessed 3 December 2024.

[889] These datasets, instead, which are critical to the pre-deployment phase of FRT, often operate in a legal grey area, where the absence of enforceable safeguards allows companies to bypass GDPR obligations. By focusing regulatory scrutiny primarily on downstream processing, current frameworks risk neglecting the pre-deployment phase, where critical decisions about dataset composition and handling occur.

[890] Taner Kuru, 'Lawfulness of the Mass Processing of Publicly Accessible Online Data to Train Large Language Models' [2024] International Data Privacy Law ipae013.

Moreover, the lack of clear regulatory oversight at this stage creates loopholes that undermine core GDPR principles. Companies frequently classify publicly scraped datasets as non-personal data to avoid obligations such as informed consent or impact assessments under Article 35 GDPR.[891] Yet, the cumulative harm caused by these practices, particularly when models are deployed at scale, such as for real-time surveillance in public spaces, illustrates the inadequacy of this approach. This not only disregards the GDPR's fairness and accountability principles but also weakens individuals' control over their personal data, as they are deprived of meaningful opportunities to intervene before identifiable data is processed.[892]

Addressing these challenges requires a rethinking of how data protection principles apply across the lifecycle of FRT. This is a task of the European legislator and is of pressing pace, given the broader risks of producing loopholes without protection.

5.4.2 Cluster 2: the use of publicly available data

The second and perhaps most contentious issue revolves around the use of publicly available images to train FRT models. Clearview AI's practice of scraping[893] billions of images from social media exemplifies the scale and ethical ambiguity of such practices.[894] As also witnessed by the *Glukhin case*, the police, to identify the applicant, relied on the collection of personal biometric data obtained through Telegram. This highlights a critical legal point since under Article 9, para. 2, lett. e) the GDPR permits the processing of special categories of biometric data, such as facial images, only when the data subject has

[891] For instance, extending data protection impact assessments to include the training phase could mitigate risks by identifying and addressing potential vulnerabilities before deployment. Without these measures, the reliance on ambiguous classifications of training data risks undermining both the GDPR's efficacy and public trust in the governance of biometric technologies.

[892] "Applying the GDPR to computer code can provide digital rights advocates with ammunition to claim rights to access and control the use of algorithms where those rights do not yet exist under alternative legal regimes", Purtova and Leenes (n 882).

[893] According to the EDPB, ""Web scraping" is a commonly used technique for collecting information from publicly available online sources. Information scraped from, for example, services such as news outlets, social media, forum discussions and personal websites, may contain personal data", EDPB, 'Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models', id., p. 11, §18.

[894] Kohn (n 453); Sobel (n 868); Kashmir Hill, 'Clearview AI's Facial Recognition App Called Illegal in Canada' *The New York Times* (4 February 2021) <https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html> accessed 3 December 2024; Betsy Swan, 'Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen' *The Daily Beast* (26 February 2020) <https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen> accessed 3 December 2024.

"manifestly made them public."[895] What happens here concretely is that companies extract – hence, scrape – photos of people from the web that are shared via social media in public mode or even in a professional context, like the workplace websites that have pictures of the teams. With this extraction of photos, then the biometric system is trained. In this sense, the scraping activity is not *per se* a processing of personal data. It becomes such photos are processed through specific technical means, allowing the unique "identification or authentication of a natural person".[896]

Hence, focusing on the legal conditions for processing personal data, as explained in Chapter 3, special categories of personal data[897] can be processed only if specific exceptions apply, namely: 1) explicit consent of the data subject; 2) the processing is necessary to carry out obligations and exercise specific rights of the controller or of the data subject in the field of employment and social security and social protection law; 3) the protection of a vital interest of the data subject; 4) the processing is carried out in the context of NGOs; 5) when data are manifestly made public, etc.

In this context, 'making public' should be construed to include publishing the data in the mass media, putting them on online social network platforms or similar actions. However, this provision has been interpreted in many contradictory ways:[898] it definitely requires more than the mere availability of data in a public space; it demands an explicit and informed act by the data subject to make their data publicly accessible, coupled with an understanding of the consequences.[899] In this sense, the EDPB has clarified that being passively recorded, such as entering the range of a surveillance camera, does not meet the threshold of an affirmative act.[900] Furthermore, "the mere fact of entering into the range

[895] Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[896] Fabrizio Lala, 'Data Collection via Web Scraping: Privacy and Facial Recognition after Clearview' (2023) 16 i-lex 34.

[897] Formerly classified as "sensitive data" under Directive 95/46/EC.

[898] The lack of guidance and the scarce attention that this topic had until this moment is well documented by Edward S Dove and Jiahong Chen, 'What Does It Mean for a Data Subject to Make Their Personal Data "Manifestly Public"? An Analysis of GDPR Article 9(2)(e)' (2021) 11 International Data Privacy Law 107.

[899] Though, it is very difficult for the data controller to verify this aspect.

[900] "It is important to note here that every exemption listed in Article 9 is not likely to be usable to justify processing of special categories of data through video surveillance. More specifically, data controllers processing those data in the context of video surveillance cannot rely on Article 9 (2) (e), which allows processing that relates to personal data that are manifestly made public by the data subject". EDPB, 'Guidelines 3/2019 on processing of personal data through video devices', Version 2.0, Adopted on 29 January 2020, p. 17.

of the camera does not imply that the data subject intends to make public special categories of data relating to him or her."[901] As also reinstated by the CJEU, in *Meta Platforms Inc and Others v Bundeskartellamt*,[902] merely visiting a website or app does not meet the threshold of the 'data subject's awareness', as users typically do not intend to make their likes, hence their interactions publicly accessible.[903] A crucial example is to be found in what the Court highlighted as forms of posting: interactions features like "Like" or "Share" buttons could constitute "manifestly making public" data, but only if users are provided with clear options and knowingly choose settings that make their data visible to an unlimited audience.[904] Therefore, more practically, if privacy settings are absent or inadequate, users cannot be deemed to have made their data public, unless they have explicitly consented to such disclosure following clear and express information provided by the platform.[905]

Clearly, any data obtained unlawfully falls outside the exception's scope: it is meant data 'ripped' from the data subject. But what does it mean? Where is the line between data 'made manifestly public' and data ripped from the data subject?[906]

This limitation is also[907] critical in the context of FRT training datasets, which often scrape publicly available images from social media platforms, public forums, and websites without the knowledge or consent of the data subjects. Companies frequently claim that these images qualify as 'publicly available,' thus falling outside GDPR's strict processing requirements. However, this interpretation stretches the legal meaning of 'manifestly made public' and fails to account for the 'affirmative intent' required under

---

[901] Id.

[902] CJEU (GC), Meta Platforms Inc and Others v Bundeskartellamt, C-252/21, 4 July 2023.

[903] §77 "for the purposes of the application of the exception laid down in Article 9(2)(e) of the GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public".

[904] §80-81, "these actions mean that the user interacts with the website or app in question, and, as the case may be, the website of the online social network, whereby the extent to which that interaction is public may vary in that it may be determined by the individual settings chosen by that user. […] [I]t is for the referring court to ascertain whether it is possible for the users concerned to decide, on the basis of settings selected with full knowledge of the facts, whether to make the information entered into the websites or apps in question and the data from clicking or tapping on buttons integrated into them accessible to the general public or, rather, to a more or less limited number of selected persons".

[905] This interpretation aims to ensure that platforms respect data subjects' rights and prevents misuse of personal data under the guise of public availability.

[906] This ambiguity emerged also in the CNIL sanction against Clearview AI. The Authority ordered Clearview AI, in particular, to cease the collection and use of data of persons on French territory in the absence of a legal basis and to facilitate the exercise of individuals' rights and to comply with requests for erasure.

[907] Kuru specifies the issues in the context of GPAI, where, for instance, OpenAI claim that ChatGPT is trained with information that are publicly available in the web. Kuru (n 890).

GDPR, as clarified by the EDPB. This aspect clearly emerged already in the cases that regarded FRT, where "the DPAs scrutinising Clearview AI specifically emphasised that data subjects could not have reasonably expected their images to be processed to create a facial recognition app while determining that Clearview AI's processing activities were unlawful".[908] In practice, such reliance on publicly available images for FRT training raises significant ethical and legal concerns. First, the datasets often include 'sensitive' biometric data, which enjoys heightened protection under GDPR. Without the affirmative consent of data subjects or a lawful basis for processing, such practices directly contravene the principles of fairness, transparency, and accountability enshrined in GDPR Articles 5 and 6.

The use of these datasets highlights a broader regulatory gap in the oversight of pre-deployment stages of FRT systems, which adds to the previously analysed conundrum of whether it is possible to consider models as personal data.

Furthermore, to address these challenges, a comprehensive and multi-layered approach is necessary. First, GDPR principles must be applied more rigorously to scrutinise the composition of training datasets, ensuring compliance with requirements for informed consent and lawful processing. This includes reinforcing the necessity of opt-out mechanisms,[909] which provide individuals with a meaningful opportunity to withdraw their data from such datasets. These mechanisms are crucial for safeguarding autonomy and enabling individuals to retain control over their personal information, particularly in cases where data is scraped or collected without explicit consent. Second, clearer and more robust guidance is required to delineate the boundaries of "manifestly public" data, as outlined under Article 9, para. 2, lett. e) of the GDPR, especially in the age of AI where the use of techniques like text and data mining and scraping are the way these models are

[908] Id.

[909] In a nuanced way, also the CJEU in the Meta case mentioned this aspect, when stating that "When the users concerned actually have that choice, they can be regarded, when they voluntarily enter information into a website or app or when they click or tap on buttons integrated into them, as manifestly making public, within the meaning of Article 9(2)(e) of the GDPR, data relating to them only in the circumstance where, on the basis of individual settings selected with full knowledge of the facts, those users have clearly made the choice to have the data made accessible to an unlimited number of persons, which it is for the referring court to ascertain." On the contrary, "if no such individual settings are available, it must be held, […] that, where users voluntarily enter information into a website or app or click or tap on buttons integrated into them, they must, in order to be deemed to have manifestly made those data public, have explicitly consented".

trained.[910] Mandatory audits and transparency regarding the sources of training data should form part of this oversight process, not only to ensure compliance but also to rebuild public trust in the governance of biometric technologies.

Therefore, to align with GDPR's fairness and accountability principles, this regulatory oversight must extend beyond dataset composition to encompass the lifecycle of FRT systems, particularly in ensuring the enforcement of data subject rights. This includes robust mechanisms for addressing data retention and erasure, as explored in the third and following cluster of this analysis. Without clear procedures for data minimisation, retention limits, and verifiable erasure protocols, individuals' rights to privacy and data protection risk being severely undermined.

5.4.3 Cluster 3: data retention and erasure

How can we reconcile the concept of a "digital self,"[911] composed of the vast and fragmented array of data circulating across the digital ecosystem, with the right to erasure? How can data deletion be effectively enforced in the age of AI? These questions are central to the third cluster, which encapsulates and builds upon the considerations addressed in the preceding analysis. As a matter of fact, if an AI model is not classified as personal data, the rights of the data subject, such as the right to erasure under Art. 17 GDPR and Art. 16 LED, become inapplicable, thereby, on the one hand, leaving the data subject without safeguards and remedies, and, on the other, the data controller from obligations under GDPR. This legal loophole challenges the practical enforcement of data protection principles which fragility has been recently addressed in various forms.[912]

---

[910] As the Meta case shows, the issue was already relevant in the realm of platforms. However, AI and, more specifically, complex models like LLMs or deep learning, "further process publicly accessible online data to, among others, learn connections between words to generate their answers by predicting the words most likely to follow each other. Hence, they present their users with 'processed' information, which, as explained above, sometimes appears inaccurate. Therefore, it can be argued that LLMs go beyond being solely an intermediary between the source of information and the user since there is a (possible) alteration of the information throughout the process." Quoting Kuru (n 890).

[911] Maria Pia Rossignaud and Derrick De Kerckhove, *Oltre Orwell. Il Gemello Digitale.* (Castelvecchi 2020).

[912] Paul De Hert, 'C4Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law' in Deirdre Curtin and Mariavittoria Catanzariti (eds), *Data at the Boundaries of European Law* (Oxford University Press 2023); Paul De Hert, 'Eu Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the Gdpr in the Spirit of Cooperative Federalism', *EU Law Enforcement* (Routledge 2021).

Moreover, the sheer volume of publicly available data, often collected and retained without clear boundaries or oversight, creates significant obstacles to ensuring comprehensive and meaningful data deletion. The fragmented and often decentralised nature of data processing further complicates compliance, as it risks enabling indiscriminate and prolonged retention of data that should otherwise be erased.[913] In this context, addressing the challenges of data deletion is not merely a procedural exercise but a critical component of safeguarding fundamental rights in the AI era.

Given this premise, this third cluster, as anticipated, is focusing on the challenges in ensuring a real erasure of data and practical oversight in ensuring retention of data for no longer than necessary. A brief clarification. Retention and erasure are different, as well as two sides of the same coin. While data retention focuses on the duration and conditions under which personal data may be stored,[914] data erasure concerns the mechanisms and rights associated with permanently deleting personal data when its retention is no longer justified.[915] These dimensions are critical for safeguarding fundamental rights in the AI era, especially given the fragmented and decentralised nature of data processing. Without clear standards, the risk of indiscriminate and prolonged retention undermines the effective exercise of erasure rights,[916] thereby compromising privacy and data protection principles.

[913] Scholars note, in particular, that "such protections are particularly important in an era when sensitive data is processed in an uncontrollable data-tsunami-fashion that becomes sharable with various state entities, and given that the European Court of Human Rights has held the view (and emphasised) for more than a decade that mere retention/collection of personal data may raise serious privacy-concerns", Paul De Hert and Georgios Bouchagiar, 'European Biometric Surveillance, Concrete Rules, and Uniform Enforcement: Beyond Regulatory Abstraction and Local Enforcement' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024).

[914] Mark Leiser and Bart Custers, 'Time Limits for Storage and Review' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[915] Herke Kranenborg, 'Article 17 Right to Erasure ("Right to Be Forgotten")' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020).

[916] "In principle, general and indiscriminate retention is considered legitimate only where the aim is that of safeguarding national security; all other goals, including crime prevention or repression, do not justify a similar limitation of fundamental rights. In this second domain, therefore, retention obligations are allowed only insofar as they are targeted". Giulia Lasagni, 'Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the "Data Retention Saga"' (GBR 2024).

5.4.3.1 The right to erasure: who wants to live forever?

Under Article 17 of the GDPR,[917] the right to erasure allows data subjects to request the deletion of personal data when conditions such as unlawful processing, withdrawal of consent, or the data's irrelevance are met. [918]

This right complements the principle of data minimisation, which mandates that data is not retained longer than necessary.[919]

However, the practical application of this right is fraught with challenges, particularly in AI systems, where data becomes deeply embedded in models, making selective deletion difficult.[920] "Who wants to live forever" sings the Queen. And this is the question that we must consider in an environment such as that of AI. This complexity raises questions about how to reconcile technological realities with legal obligations.

In particular, the difficulties mainly rely on understanding what to erase, its concrete realization, and under which procedure. [921]

---

[917] Jef Ausloos, *The Right to Erasure in EU Data Protection Law* (1st edn, OUP Oxford 2020). The right to erasure is often conflated with the right to be forgotten; it plays a critical role in empowering individuals to control their personal data and mitigate the risks of 'data immortality', as explained in the following footnote.

[918] Instead, and differently from the right to erasure, the right to be forgotten, as established in the *Google Spain* case, is focused on delisting or de-indexing search engine results, targeting the control of information dissemination rather than its deletion. Both rights reflect the dual nature of European privacy law, balancing compliance-driven data protection mechanisms with individual autonomy and informational privacy. Yet, the GDPR's technical neutrality, vague procedural requirements, and broad exceptions often undermine the enforceability of these rights. Addressing these shortcomings is essential to align the legal framework with the realities of AI-driven systems, ensuring that individuals can effectively exercise their rights in the digital age. Franz Werro, 'The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1401357 <https://papers.ssrn.com/abstract=1401357> accessed 3 December 2024; Robert Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere' [2017] SSRN Electronic Journal <http://www.ssrn.com/abstract=2953468> accessed 3 December 2024.

[919] As it is known, this right was much developed in the well famous case Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Grand Chamber, 13 May 2014, C-131/12. It is not the purpose of this paper to delve into this judgment. For a more in-depth analysis, this paper refers back to Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (n 181). See also Marco Bassini and Oreste Pollicino, 'Reconciling Right to Be Forgotten and Freedom of Information in the Digital Age: Past and Future of Personal Data Protection in the European Union', [2014] Diritto Pubblico Comparato ed Europeo 641.

[920] Eduard Fosch Villaronga, Peter Kieseberg and Tiffany Li, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304; Laura Graves, Vineel Nagisetty and Vijay Ganesh, 'Does AI Remember? Neural Networks and the Right to Be Forgotten' <https://uwspace.uwaterloo.ca/handle/10012/15754> accessed 3 December 2024; Veale, Binns and Edwards (n 883).

[921] Article 17 par. 3 lists the grounds under which the processing is still considered necessary: "(a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c)

On the first aspect, ever since the *Google Spain* decision, the CJEU has attempted to curb the risk of being exposed to a perpetual digital memory through the application of the right to be forgotten. Better identified as the "right to erasure", or even "right to de-indexing", the Court recognized the right of the data subject to have search results relating to his or her name deleted. In fact, de-indexing actually means to obscure content and not delete it. The CJEU has repeatedly ruled on the link between privacy and information, attempting to dictate guidance for both the Courts and search engine operators on handling the ever-increasing number of de-indexing requests[922]. Thus, it is no surprise that a part of the literature underlines the threat of private censorship by online companies that will emerge if a right to be forgotten is generally recognised.[923] In particular, scholars highlight the risks of making service providers decide what to show and delete – and imagine it in the context of AI, without solid procedural mechanisms.[924]

On a second stance, the difficulties in actually enforcing this right have also been highlighted in the Court's recent ruling in *T.U. and R.E. v. Google LLC,* which revolves around this issue.[925] The case concerns a de-indexing request submitted by T.U., who occupies positions of responsibility and holds stakes in several companies, and R.E., who was his partner and, until May 2015, an attorney for one of those companies. The data subjects had sent a request to the search engine, Google, as the data controller, to remove links to three articles that, in the plaintiffs' opinion, contained inaccurate or untrue statements. The truly innovative element of this ruling lies not so much in the role of the search engine operator as a silencer or promoter of information nor in the guideline to be applied to the de-indexing of thumbnails. As a matter of fact, the "procedural fairness"[926], as called by Advocate General Pitruzzella, requires the search engine operator to carry out a kind of substantive judgment, the preliminary stage of which is the groundwork for

---

for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defence of legal claims".

[922] Ex multis, C-507/17, Google LLC v. CNIL.

[923] Ugo Pagallo and Massimo Durante, 'Human Rights and the Right to Be Forgotten', *Human Rights, Digital Society and the Law* (Routledge 2019); Orla Lynskey, 'The "Europeanisation" of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies 252.

[924] MR Leiser, '"Private Jurisprudence" and the Right to Be Forgotten Balancing Test' (2020) 39 Computer Law & Security Review 105458.

[925] CJEU (GC), *TU, RE v Google LLC,* C-460/20, 8 December 2022.

[926] §42 of the Opinion.

granting the de-indexing request. A phase that assumes substantive relevance since, in the Court's opinion resulting from this very case, the interested party need not necessarily accompany its request with a judicial pronouncement sanctioning the inaccuracy of the information whose de-indexing is sought by the search query. The procedural remedy described is proposed to counter the risk of imposing on the search engine operator "general obligations not to host publications containing false information or general obligations to ascertain the falsity or otherwise of information that is the subject of a de-indexing application"[927].

Since the GDPR fails to specify the procedure for such a decision and merely states the conditions under which the right to erasure can be exercised, it is left to the data controllers to create internal and different procedures for each case. Therefore, as testified by *T.U. and R.E. v. Google LLC*, it is necessary a realignment of the right to erasure to be enforceable in the context of AI and biometric systems,[928] especially since AI is a new powerful form of searching, retaining, scraping and curating contents, that might significantly impair, as mentioned the ability of the data subject to actually obtain a true erasure of their personal data,[929] even in more powerful way than 'traditional' search engines did.

This aspect has also been recently underlined by two measures issued by the Italian DPA. On the one hand, the authority sanctioned OpenAI for not, *inter alia,* having been able to create a clear procedure for their users to asking the erasure of their personal data.[930]

Secondly, in the measure issued against Clearview AI for infringing several principles of the GDPR[931], it was ordered the erasure of the data, including biometric data, processed

[927] §49 of the Opinion.
[928] Graves, Nagisetty and Ganesh (n 920).
[929] Jevan Hutson and Ben Winters, 'America's next "Stop Model!" Model Deletion Essay' (2024) 8 Georgetown Law Technology Review 124.
[930] Italian DPA, Register of Measures, No. 755 of 2 November 2024, doc. web no. 10085455. In particular, the sanction demanded the creation by the company of an "institutional communication campaign aimed at promoting awareness of the personal data protection issues at stake in the case at hand, with particular reference to the terms and conditions through which data subjects will be able to exercise, in a simple and effective manner, all their rights under the current legislation, starting with those of opposition, rectification and erasure." Text translated by the author.
[931] See *Registro dei provvedimenti,* Order n. 50, published on the 10th, February 2022, against Clearview AI. In particular, the company failed to comply with the transparency obligation, the purpose limitation, and the storage limitation. Indeed, it failed to provide the information set out by article 13-14, to provide information on an action taken on a request under Article 15 within the due timeframe, and to designate a representative in the EU.

by the company's facial recognition system with regard to persons in the Italian territory. The Italian DPA did not order the deletion of the algorithm trained with the illicitly collected pictures of unaware data subjects, nor did it outline which datasets the company should delete.

Differently, the Federal Trade Commission[932] has forced[933] a company, to destroy the algorithms built with data gathered illicitly or deceptively[934] to create a facial recognition system. The US-based company, Everalbum, provides customers with a cloud storage service, "Ever." The FTC issued an order where Everalbum violated Section 5 of the FTC Act for misrepresenting its privacy practices. The most important aspect of this decision is the remedy chosen by the Commissioners. It was ordered the deletion of the illicitly collected biometric data.[935] Moreover, "algorithmic disgorgement" (or algorithmic destruction) was mandated. By this name, the Authority meant an order that tackled the illicitly collected data by demanding the organisation destroy the models and the algorithms the company developed by using the photos and videos uploaded by its users who were not aware of the further processing.[936] The FTC decision is not just meaningful regarding consumer protection but is shedding light on the problem analysed by the present cluster. Particularly, in light of the criticalities pointed out above on ensuring deletion, this remedy might seem appealing.

Can algorithmic destruction represent a natural remedy, or is it just a threat to companies collecting illicit data? Can the individuals activate this remedy horizontally as per enforcing Article 17 of the GDPR? Can this remedy be effective in tackling both

[932] As known, the Federal Trade Commission is a bipartisan federal agency that champions the interests of American consumers. Hereafter, FTC.

[933] Federal Trade Commission, Everalbum, Inc., also d/b/a Ever and Paravision, decision and order docket no. c-4743/2021.

[934] Randi Singer and Michael Goodyear, 'FTC Orders Destruction of Algorithms Created from Unlawfully Acquired Data', 4(6) 2021 The Journal of Robotics, Artificial Intelligence & Law 11. The FTC issued an Order where Everalbum was found to violate Section 5 of the FTC Act for misrepresenting its privacy practices. Section 5(a) of the FTC Act provides that «unfair or deceptive acts or practices in or affecting commerce […] are […] declared unlawful», 15 U.S.C. Sec. 45(a)(1).

[935] It was not indeed the first time that the FTC issued such an order. It happened also in its final decision against Cambridge Analytica, where the company was required to delete or destroy the data itself as well as "any information or work product, including any algorithms or equations, that originated, in whole or in part, from this Covered Information", see Section IV – 'Required deletion of data', p. 5 of Docket no. 9383/2019.

[936] See Paper "III – Deletion" of the Order, p. 4-5, "to delete or destroy all Face Embeddings derived from Biometric Information Respondent collected from Users who have not, by that date, provided express affirmative consent for the creation of the Face Embeddings".

personal and non-personal data? Algorithmic disgorgement (or algorithmic destruction) is a remedy FTC has been using for a while, tackling illegal data collection. The idea is not to let companies profit from either the data or any algorithm developed using the illicitly collected data. However, even this remedy – which seems to be more of a threat and a remedy or a general deterrence solution[937] – does not seem a real alternative answer to the critical claim explained above, ultimately resulting in an aggressive act that does no good both to companies and data subjects.[938]

Nonetheless, it remains the problem: it is difficult to ensure erasure, especially in the context of FRT.[939] In transitioning to the question of retention, it is critical to examine how inadequate oversight of retention policies not only undermines the right to erasure but also creates a framework where personal data can be indefinitely stored, leading to systemic risks of misuse, overreach, and the erosion of individual freedoms.

5.4.3.2 Data retention: it's now or never?

Data retention represents a critical challenge in aligning the regulation of AI systems, particularly biometric technologies such as FRT, with fundamental rights and constitutional law.[940] Central to this issue is the principle under Art. 4 para. 1 lett. e) LED, and Art. 5, which mandates that "Member States shall provide for appropriate time limits

---

[937] In the words of Rebecca Kelly Slaughter, one of the Commissioners: «the authority to seek this type of remedy comes from the Commission's power to order relief reasonably tailored to the violation of the law.115 This innovative enforcement approach should send a clear message to companies engaging in illicit data collection to train AI models: Not worth it», Rebecca Kelly Slaughter, Janice Kopec and Mohamad Batal, 'Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission', (2021) Yale Journal of Law and Technology, 39. See also: Dissenting Statement of Commissioner Regarding the Matter of FTC vs. Facebook, (F.T.C. July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf.

[938] As highlighted by Li: "if deletion of machine learning training models becomes an established and routine legal consequence for the deployment of a bad model or a bad artificial intelligence system in general, this might harm small startups and discourage new market entrants in technology industries". Li (n 600).

[939] Monika Zalnieriute, 'From Data Retention to Facial Recognition Technologies: Counter-Terrorism Implications for Human Rights and the Rule of Law' (Social Science Research Network 2021) SSRN Scholarly Paper ID 3876833.

[940] Marco Bassini, 'Data Retention as a Matter of Constitutional Law' in Eleni Kosta and Irene Kamara (eds), *Data retention in Europe and beyond* (2024); Barbara Grabowska-Moroz, 'Data Retention in the European Union' in Marek Zubik, Jan Podkowik and Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer International Publishing 2021); Marek Zubik, Jan Podkowik and Robert Rybski, 'Judicial Dialogue on Data Retention Laws in Europe in the Digital Age: Concluding Remarks' in Marek Zubik, Jan Podkowik and Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer International Publishing 2021).

to be established for the erasure of personal data or a periodic review of the need for the storage of personal data". A similar provision is contained in Art. 5 para. 1 lett. e) GDPR, in which personal data must only be retained for as long as necessary to fulfil its original purposes.[941] In a nutshell, both texts require procedural measures to be adopted to ensure that those time limits are observed, and such an obligation is placed on the controllers that must also create all the technical and organisational measures "for ensuring notably that, by default, the legitimate period of storage of personal data be respected".[942]

However, retention practices frequently fall short of this requirement, particularly in high-risk applications like mass surveillance and law enforcement. A key lies in the inadequacy of safeguards to ensure compliance with proportionality and necessity requirements. This issue was at the centre of a notable 'judicial saga' which involved the European data retention regime, which has faced significant legal and regulatory upheavals since the annulment of the 2006 Data Retention Directive[943] by the CJEU in *Digital Rights Ireland*.[944] The Directive was invalidated for its incompatibility with EU fundamental rights, particularly under Articles 7 and 8 of the CFREU. Its repeal created a regulatory vacuum, with no subsequent legislative initiative by the EU to harmonise national retention laws,[945] that still lacks a subsequent act that builds on the ashes of the Data Retention Directive. Therefore, following the 'legislative inertia', the CJEU has to – once again[946] – the player of an outsized role[947] in shaping the legal boundaries of data retention. Post-*Digital Rights Ireland*, the Court's jurisprudence, including

[941] Mark Leiser and Bart Custers, 'Time Limits for Storage and Review' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[942] Cécile de Terwangne, 'Article 5 Principles Relating to Processing of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020). It is to be noted that the storage limitation principle permits the storage of personal data for longer periods if it is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is subject to the implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

[943] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, no longer in force.

[944] Joined C-293/12 and C- 594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.

[945] As well noted by Bassini, in Bassini, 'Data Retention as a Matter of Constitutional Law' (n 940). As a matter of fact, this 'legislative inertia' is indeed emblematic of the political challenges in achieving consensus among Member States on a unified framework for data retention, particularly when balancing privacy rights with national security and public safety concerns.

[946] Pollicino, 'Potere Digitale' (n 3); Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (n 181).

[947] Maria Tzanou and Spyridoula Karyda, '*Privacy International and Quadrature Du Net:* One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28 European Public Law.

Tele2/Watson,[948] *Privacy International*,[949] and *La Quadrature du Net*,[950] has progressively delineated the conditions under which data retention may comply with fundamental rights.[951] The Court has repeatedly struck down indiscriminate or blanket data retention schemes, emphasising that such measures represent a disproportionate interference with privacy and data protection rights. However, its judgments have also allowed narrowly tailored retention measures for specific purposes, such as national security or serious crime prevention, provided they are subject to strict procedural safeguards and time limitations.[952] Furthermore, this imbalance is particularly pronounced in public surveillance contexts, where individuals are often unaware of how long their data is being retained or for what purposes.

Leaving the retention regulation to the judicial interpretation of the CJEU, it clearly created changes in precedents and a lack of clear harmonization. This is testified by the judgment in *La Quadrature du Net II*[953] where the Court evolved its previous precedent on the retention of IP addresses. While reaffirming the general prohibition of bulk

[948] CJEU (Grand Chamber), Joined C-203/15 and C-698/15, Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016.

[949] CJEU (Grand Chamber), Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, C-623/17, 6 October 2020.

[950] Joined C-511/18, C-512/18, and C-520/18, *La Quadrature du Net*, cit.

[951] Arianna Vedaschi and Valerio Lubello, 'Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective' (2015) 20 Tilburg Law Review.

[952] Vague justifications for retaining data shift the burden of safeguarding rights from data controllers to individuals, leaving them with limited capacity to challenge or enforce retention limits. This imbalance is particularly acute in public surveillance scenarios, where individuals are rarely informed about how long their data will be retained or for what purposes. See, also, Lukas Martin Landerer, 'Data Retention' [2024] Verfassungsblog <https://verfassungsblog.de/data-retention/> accessed 29 November 2024.

[953] CJEU (GC), *La Quadrature du Net (et al.) v. Premier ministre et Ministre de la Culture,* C-470/21, 30 April 2024. In *La Quadrature du Net II* (LQdN II), the CJEU clarified the standards for data retention and access, distinguishing between serious and non-serious interferences with fundamental rights. The Court held that serious interferences, such as those enabling precise and invasive conclusions about an individual's private life, can only be justified for combating serious crime. Non-serious interferences, such as retaining IP addresses that cannot lead to detailed inferences, may be used to combat ordinary crime, provided safeguards are in place to ensure the separation and oversight of retained data categories (paras. 77–89). The judgment further addressed the necessity of access to retained data, ruling that *Hadopi* could access IP addresses for investigating copyright infringement as long as the interference was non-serious and necessary in individual cases (paras. 99–121). Finally, the Court reiterated the principle established in *Tele2 Sverige* that prior judicial or administrative review is generally required for serious interferences but not for non-serious ones, unless atypical cases involve merging data in a way that reveals sensitive personal information (paras. 124–139). For a more in-depth analysis of the case, refer to Marco Mauer, 'The Unbearable Lightness of Interfering with the Right to Privacy' [2024] Verfassungsblog <https://verfassungsblog.de/the-unbearable-lightness-of-interfering-with-the-right-to-privacy/> accessed 28 November 2024; Marcin Rojszczak, 'Data Retention in the Light of Copyright Infringements: Protecting the Status Quo or Seeking a Third Way? (Case C-470/21 La Quadrature Du Net II)' [2024] Maastricht Journal of European and Comparative Law 1023263X241287402.

retention,[954] it opened the door for certain permissible practices under narrowly defined conditions, such as limited retention of IP addresses and targeted data retention in situations of genuine and foreseeable threats posed by "serious crimes".[955] As a matter of fact, the Court affirmed that "the general and indiscriminate retention of a set – even a vast set – of static and dynamic IP addresses used by a person in a given period does not necessarily constitute, in every case, a serious interference with the fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter". It follows that such an interference might be "justified by the objective of combating criminal offences in general".[956]

This interpretation is reopening again the window for allowing the retention frameworks, engaging a "one step forward, two steps back"[957] dance that is particularly worrying given the lack of a hard law base. Thus, indiscriminate retention practices often lead to function creep,[958] where data collected for one purpose is repurposed for another, potentially infringing not only data protection and privacy but also freedom of expression and assembly. The chilling effect of such practices is particularly pronounced in public surveillance contexts, where individuals may alter their behavior due to the awareness of being monitored. These concerns are further exacerbated in the case of biometric technologies like FRT. The retention of biometric data, by its immutable and sensitive nature, poses unique risks, including the potential for re-identification and the erosion of individual autonomy. Unlike traditional data categories, biometrics cannot be 'reissued' or 'reset,' for the technical reasons examined in Chapter 3, heightening the consequences of prolonged or unnecessary retention.

The fragmented legal landscape adds to these challenges. Data retention policies vary widely among Member States, with many lacking harmonised procedural safeguards or clear temporal limitations.[959] This regulatory patchwork creates significant risks of under-enforcement and systemic gaps in ensuring the timely deletion of data. Moreover, the absence of robust oversight mechanisms means that retention practices often escape

[954] §69.
[955] §79-81.
[956] Id.
[957] Tzanou and Karyda (n 947).
[958] Maria Tzanou, 'The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection'.
[959] Bassini, 'Data Retention as a Matter of Constitutional Law' (n 940).

scrutiny, particularly when vague justifications are employed.[960] The practical difficulties of enforcing deletion rights, combined with the technical challenges of AI systems that embed biometric data into models, underscore the urgent need for a nuanced and enforceable framework.

The failure to replace the Data Retention Directive reflects the EU's ongoing struggle to reconcile the competing priorities of safeguarding fundamental rights and equipping Member States with the tools to address security threats. This regulatory inertia has created a vacuum, placing undue reliance on the judiciary to define the legal boundaries of data retention. While the CJEU has stepped in to provide critical guidance, emphasising proportionality, necessity, and procedural safeguards, its rulings also reveal the limitations of judicial activism in achieving harmonisation across the EU. By leaving significant discretion to Member States and data controllers, this approach risks posing a burden on the actors themselves, potentially reproducing loopholes of under-safeguard. Without clear, uniform legislative standards, the fragmented implementation of data retention frameworks exacerbates the risk of non-compliance and undermines the fundamental rights the GDPR, and other legal instruments seek to protect.

This regulatory gap becomes particularly pronounced when viewed through the lens of the FRIA.

Specifically, one of the FRIA's key roles is to provide transparency and oversight regarding how these systems operate and the duration for which data is stored. Combined with the DPIA, the FRIA imposes on the deployer a clear obligation to demonstrate compliance with both storage limitations and data erasure requirements. This dual-layered mechanism compels deployers to justify not only the proportionality and necessity of data processing but also the specific storage periods for the data collected.

However, this poses significant challenges for deployers, as they must navigate the tension between ensuring the right to erasure and avoiding the risks of unlimited data storage. Indiscriminate or prolonged retention contradicts fundamental rights and exacerbates the challenges of enforcing the GDPR's principles. Moreover, retention practices involving biometric data demand heightened scrutiny under FRIA's criteria. The deployers of FRT systems must not only specify clear retention periods but also provide

[960] As noted by Mauer, this "lightness" in regulatory oversight places the burden on individuals to safeguard their rights, often without the technical or legal means to do so, Mauer (n 953).

robust justifications for these timelines, particularly in light of the proportionality and necessity principles.[961]

Crucially, the FRIA framework reveals how retention practices, particularly in the context of biometric data, present unique risks to individual autonomy and fundamental rights. Biometric data's immutable nature amplifies the consequences of over-retention, making compliance with proportionality and erasure obligations not just a legal requirement but a moral imperative. Without robust safeguards, the risk of function creep and chilling effects on fundamental freedoms, such as freedom of expression and assembly, becomes a tangible threat. As such, the analysis of these three clusters demonstrates that addressing data protection in the context of FRT requires a combination of regulatory clarity, methodological rigor, and enforceable safeguards. FRIA provides a pathway to make such tensions visible and to reconcile the competing priorities of technological advancement and fundamental rights, ensuring that data protection is adapted to the complexities of AI-driven systems.

5.4.4 Chilling effects

Adopting the FRIA model here proposed, as anticipated, is possible to draw the attention not only to what we called "the higher risk rights" – such as data protection, *supra*, and the right to effective remedy, *infra* –, but also to the chilling effects, being those a phenomenon where the fear of sanctions or other negative consequences suppresses or alters individual behaviour.[962] They have gained significant attention in legal and human rights discourse, particularly in the context of FRT. For instance, in 2020, the UN Human Rights High Commissioner explicitly condemned the use of FRT in peaceful protests, highlighting its role in creating a potential chilling effect.[963]

[961] Bart van der Sloot, 'Principles Relating to Processing of Personal Data' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024); Leiser and Custers, 'Time Limits for Storage and Review' (n 184); Els J Kindt, 'The Need for a Consistent Legal Regulation of Biometric Data' in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013); Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars- Can the Lisbon Treaty Be Expected to Help' (2009) 46 Common Market Law Review; Serge Gutwirth and others, *Reinventing Data Protection?* (Springer Science & Business Media 2009).

[962] Büchi and others (n 840).

[963] United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', 24 June 2020, UN Doc. A/HRC/44/24. In part., §34, "Assemblies traditionally have allowed participants a certain level of protection against being singled out or identified. This protection was already considerably weakened by

Henceforth, the ability of governments to use these technologies to identify, monitor, and potentially harass protesters might result in an interference with the right to protest, [964] potentially stifling "freedom of expression through the chilling effect of perceived omnipresent monitoring".[965]

Therefore, the term 'chilling effect' is defined in both jurisprudence and legal scholarship and refers to the deterrence or modification of speech due to fear of sanctions or negative repercussions.[966] While it is not the sole explanation for behavioural reactions, nor does it always result in self-censorship, the chilling effect represents a significant risk in contexts where individuals perceive potential consequences for expressing opinions or participating in public assemblies. Courts have increasingly recognised the chilling effect as a legal doctrine designed to address this behavioural phenomenon.[967] It manifests as either suppression of speech, where individuals choose not to speak at all, or modification of speech, where they adopt more cautious or subdued forms of expression to avoid potential sanctions.

The concept of the chilling effect has also been examined by the CJEU, particularly in cases concerning the independence of the judiciary.[968] For example, the Court has underscored that even indirect interferences, such as mechanisms that might discourage judges from exercising their functions independently, are sufficient to raise concerns under fundamental rights frameworks. Similarly, in the context of FRT, the mere presence

---

many States that routinely made audiovisual recordings of assembly participants. The rise of facial recognition technology has led to a paradigm shift in comparison with practices of audiovisual recordings, as it dramatically increases the capacity to identify all or many participants in an assembly in an automated fashion. This is particularly problematic if live facial recognition technology is deployed, permitting real-time identification as well as targeted surveillance and tracking of participants. Faulty live identification may also lead to undue interventions in peaceful assemblies by security forces. The negative effects of the use of facial recognition technology on the right of peaceful assembly can be far-reaching, as United Nations human rights experts have pointed out. Many people feel discouraged from demonstrating in public places and freely expressing their views when they fear that they could be identified and suffer negative consequences".

[964] In particular, Warthon (n 763).

[965] Ünver (n 768). See also the EDPB, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement,' updated 26 April 2023.

[966] Mohor Fajdiga and Saša Zagorc, 'Freedom or Feardom of Expression of Judges? Exploring the "Chilling Effect" on Judicial Speech' (2023) 19 European Constitutional Law Review 249.

[967] *Inter alia,* ECtHR, *Biliński v. Poland*, Application No. 13278/20, 30 April 2022; ECtHR, *Synakiewicz and others v. Poland,* Application Nos. 46453/21, 8076/22, 9988/22, 15928/22, 23 May 2022. In the context of the CJEU, instead, CJEU (GC), Pál Aranyosi and Robert Căldăraru v Generalstaatsanwaltschaft Bremen, Joined Cases C-404/15 and C-659/15 PPU, 5 April 2016. See the comment Mohor Fajdiga, 'Chilling Effect: Turning the Poison into an Antidote for Fundamental Rights in Europe' [2024] Maastricht Journal of European and Comparative Law.

[968] CJEU (GC), Joined Cases C-558/18 and C-563/18 *Miasto Łowicz and Prokurator Generalny*, para. 58–59; Case C-791/19 *Commission v. Poland (Disciplinary regime for judges)*, EU:C:2021:596, para. 227.

of pervasive surveillance can deter individuals from engaging in lawful protests or expressing dissent, even when no direct sanction is immediately evident. This underscores the importance of addressing not only direct interferences with rights but also the broader, systemic impacts that technologies like FRT can have on fundamental freedoms.

Therefore, in this context, the FRIA must go beyond evaluating solely the direct interferences with rights such as privacy and data protection, which are more readily identifiable. It must also assess the broader societal implications, including potential chilling effects on freedom of expression, assembly, and other rights that may only be indirectly or potentially impacted. By doing so, also in the absence of any specifications on the scope of application of the FRIA by the European legislator, this tool is intended to ensure that all fundamental rights – whether directly or tangentially affected – are taken into account, providing a comprehensive framework for evaluating the deployment of FRT and similar technologies.

Exactly, with respect to the use of FRT, the chilling effects have been highlighted in *Glukhin v. Russia*, where the ECtHR underscored how the awareness of being surveilled through sophisticated tools like FRT might significantly discourage public participation in protests and other forms of civic engagement.[969] The Court's judgment stressed that this undermines the societal and democratic fabric, as individuals self-censor to avoid potential repercussions, even when participating in lawful activities.[970]

This aspect becomes even more pronounced in countries where the rule of law is perceived to be weak or lacking, as the use of advanced surveillance technologies, such as FRT, risks exacerbating existing vulnerabilities, enabling unchecked state overreach and undermining fundamental rights. In this regard, concerns were highlighted by civil society in some countries of Latin America.[971] For instance, reports from Venezuela and Bolivia indicate that FRT has been deployed to identify and track individuals, especially in the context of protests.[972] This not only erodes the right to freedom of assembly but also exacerbates fears of retaliation among activists, journalists, and ordinary citizens,

[969] "[The ECtHR] considers that the use of highly intrusive facial recognition technology to identify and arrest participants in peaceful protest actions could have a chilling effect in relation to the rights to freedom of expression and assembly", as in §88, *Glukhin v. Russia.*

[970] Warthon (n 763).

[971] Katrak and Chakrabarty (n 411).

[972] Al Sur, 'Facial Recognition in Latin America: Trends in the Implementation of a Perverse Technology' (2021) 7; Derechos Digitales, 'Gender Impacts and other Inequalities. Identity systems and social protection in Venezuela and Bolivia', (2024) 1-46.

leading to widespread self-censorship. The lack of transparency and clear legal frameworks governing these deployments compounds the problem, leaving significant room for misuse. These practices mirror the challenges identified in *Zakharov v. Russia*,[973] where the ECtHR emphasized the need for robust procedural safeguards to prevent indiscriminate and disproportionate interference with privacy and democratic rights.

The chilling effects of FRT are not confined to authoritarian regimes. Even in democratic contexts, the integration of biometric surveillance into public safety frameworks raises concerns about proportionality and necessity. For instance, in the United States and parts of Europe, protests against racial injustice and climate change have been monitored using advanced surveillance technologies, including FRT.[974] Such practices underscore the global relevance of addressing the societal risks posed by these technologies. The potential for abuse becomes particularly pronounced when oversight mechanisms are weak or absent, as demonstrated by examples in Latin America, where public safety objectives often mask political control.[975]

Ultimately, the chilling effects of FRT highlight the need for a paradigm shift in how societies approach biometric surveillance. By prioritising human rights and democratic values in the design and deployment of these technologies, it is possible to mitigate their risks while harnessing their potential benefits. This requires a commitment to transparency, accountability, and inclusive policymaking, ensuring that the voices of affected communities are central to the conversation.[976]

Finally, the analysis of the chilling effect underscores the urgent need for mechanisms that do not merely recognise potential rights violations but actively address them through accessible and effective remedies. This chilling effect, while subtle, can have profound implications for democratic participation, transparency, and public trust.

Accordingly, the next chapter will critically examine how Article 47 of the CFREU can operationalise these remedies, focusing on the procedural safeguards and judicial

[973] ECtHR (GC), *Roman Zakharov v. Russia*, Application no. 47143/06, 4 December 2015.

[974] US Government Accountability Office (GAO), 'Facial Recognition Technology:Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks', GAO-21-518, 29 June 2021.

[975] For example, activists in Colombia and Argentina have reported feeling less inclined to participate in public protests due to the fear of being identified and targeted, illustrating the need for policy responses that address both the psychological and practical barriers created by FRT, as highlighted by Katrak and Chakrabarty (n 411).

[976] Which is precisely the scope of Art. 27, para. 1, lett. d) AI Act when it specifies that "the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons", and, consequently, encourage deployers to consult stakeholders while performing the FRIA.

guarantees necessary to protect individuals against the misuse of biometric technologies. By emphasising the role of effective legal recourse, the chapter aims to bridge the gap between the identified rights interferences and ensure meaningful accountability.

5.5 Conclusion

This chapter has tested the FRIA methodology by applying it to the analysis of Article 8 CFREU, a cornerstone of data protection law, in the context of facial recognition technology (FRT). FRT has been shown to create unique and pressing challenges, particularly in balancing public safety objectives with the fundamental rights to privacy and data protection. By dissecting the application of FRIA, the chapter has interrogated how this framework can systematically identify and address the interferences posed by FRT on data protection rights.

Three critical clusters were identified as key obstacles to the meaningful realisation of Article 8's principles: training and modeling with personal data, the use of publicly available images, and compliance with retention and erasure obligations. These clusters represent concrete areas where FRT practices often fail to adhere to the principles of minimization, purpose limitation, proportionality, and fairness. Rather than providing merely a theoretical lens, FRIA enables deployers to navigate these challenges by focusing on targeted risk assessments and mitigation strategies tailored to each context.

This analysis also underscores the broader implications of unchecked retention and processing practices. Practices such as indiscriminate retention, repurposing publicly available data, and weak enforcement of erasure rights do not only infringe upon data protection but also create a chilling effect on other fundamental freedoms, such as freedom of expression and assembly. Cases like *Glukhin v. Russia* exemplify how pervasive surveillance, enabled by FRT, alters public behaviour and undermines democratic engagement, highlighting the critical importance of effective safeguards.

By employing the FRIA methodology, the chapter has shown how a structured and systematic approach can bridge the gap between legal principles and operational realities. The methodology emphasises context-driven assessments, transparency, accountability, and enforceable safeguards to address systemic vulnerabilities, starting from the legal framework itself, and having repercussions on the concrete deployment of the technology. Crucially, FRIA compels deployers to evaluate not only the technical aspects of FRT

systems but also the broader regulatory frameworks and their alignment with fundamental rights.

Yet, this chapter is not only diagnostic but also preparatory. The findings herein lay the groundwork for the next chapter, which will pivot to the critical issue of remedies under Article 47 of the EU Charter of Fundamental Rights. If FRIA provides a framework for identifying and mitigating risks, the focus on remedies addresses the crucial question of accountability and redress when rights are violated. In particular, the right to an effective remedy becomes indispensable in ensuring that the safeguards discussed in this chapter are not only theoretical but enforceable. By exploring the intersections between biometric technologies, procedural fairness, and the right to effective remedies, the next chapter will build upon the insights gained here to advance a comprehensive understanding of how fundamental rights can be meaningfully protected in an era of pervasive surveillance.

6. EFFECTIVE REMEDIES: "WHATEVER IT TAKES" FOR THE PROTECTION OF FUNDAMENTAL RIGHTS

SUMMARY: 6.1 Introduction. – 6.2 Legal framework: the right to an effective remedy; 6.2.1 The European legal framework; 6.2.1.1 Applicability of the right; 6.2.1.2 Limitations; 6.2.1.3 The role of MS in ensuring effective judicial protection. – 6.3 The right to an effective remedy in the digital age. 6.4 The remedies under the AI Act; 6.4.1 Another one bites the dust?. – 6.5 Agency: *ubi societas, ibi ius*?. – 6.6 (Judicial) Authority: *quid iuris*?; 6.6.1 Diverging standards of scrutiny; 6.6.2 'In subordine': at least quasi-judicial oversight; 6.6.3 "It's a though call: they are so different": the Italian case"- 6.7 Conclusion.

6.1 Introduction

The analyses in Chapters 4 and 5 laid the foundation for understanding how biometric technologies, particularly facial recognition systems, challenge fundamental rights and necessitate robust governance mechanisms. Chapter 4 introduced the Fundamental Rights Impact Assessment (FRIA) as a vital tool for mitigating risks posed by high-risk AI systems. Building on this, Chapter 5 applied the FRIA framework specifically to biometric systems, demonstrating its capacity to make visible and, consequently, addressable the tensions between innovation and fundamental rights protections.

This chapter now extends that analysis by focusing on the right to an effective remedy, enshrined in Article 47 of the Charter of Fundamental Rights of the European Union (CFREU).[977] Remedies are not only procedural safeguards but also the backbone of accountability and justice in democratic systems.[978] This right ensures that individuals can seek meaningful recourse when their rights are violated, yet the complexity and opacity of FRTs, coupled with their pervasive societal impact,[979] often create structural barriers to justice. These barriers include difficulties in identifying violations, holding deployers accountable, and accessing redress mechanisms, raising fundamental questions

[977] Steve Peers and others, 'Article 47', *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2021); Tobias Lock and Denis Martin, 'Article 47 CFR' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019).

[978] Simona Demková, *Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023).

[979] Giovanni Ziccardi, 'Global Surveillance Activities and Digital Mining of Citizens' Data Balancing Security Issues and Civil Rights' [2018] Ragion pratica.

about the adequacy of existing legal frameworks, as crucially underlined by the European Agency for Fundamental Rights report on the use of FRT by law enforcement authorities.[980]

This raises critical questions: Are current legal frameworks adequate to address the systemic risks of FRT? And how can FRIA be leveraged to ensure remedies that are accessible, enforceable, and aligned with the principles of transparency and accountability?

To address these questions, this chapter revisits the theoretical and practical insights from Chapters 4 and 5, examining how FRIA can bridge the gap between legal principles and the unique challenges posed by FRT. Hence, using also in this case the fundamental right's checklist, the Chapter aims to dissect the interferences to the enjoyment of this right both substantially and procedurally.[981] Therefore, the study of Article 47 in this chapter is twofold. First, it evaluates whether existing remedies under the current legal framework align with the standards of accessibility, accountability, and independence required by Article 47.[982] Second, it reflects on how these remedies can be adapted to address the invasive nature of FRTs, which are often deployed in public spaces, target large groups, and operate in ways that are inherently opaque. Substantive rights must ensure individuals can redress violations effectively, while procedural safeguards must guarantee transparency, oversight, and accountability. This dual perspective provides a comprehensive framework for assessing how the principles of Article 47 can respond to the governance challenges of biometric technologies. [983]

The chapter is structured as follows. It begins by evaluating the procedural and substantive dimensions of Article 47 in the context of AI systems, focusing on the need for remedies that are not only theoretically sound but also practically viable. Next, it highlights how FRIA can be operationalised to address the dual challenges of agency – who can claim remedies – and procedure – how those remedies are enforceable in a system that is transitioning towards forms of "digital justice".[984] Finally, the chapter

[980] European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019.
[981] Bonelli (n 50).
[982] Sarah de Heer, 'Artificial Intelligence and the Right to an Effective Remedy' in Alberto Quintavalla and Jeroen Temperman (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023).
[983] De Hert and Bouchagiar (n 774).
[984] Erik Longo, 'La ricerca di un'antropologia costituzionale della società digitale' (2023) 5 Rivista italiana di informatica e diritto 147.

contextualises these issues within the Italian legal framework, drawing parallels between wiretapping jurisprudence and facial recognition technologies. This brief comparative lens offers valuable insights into how national legal systems can adapt to the demands of digital justice without compromising the protection of fundamental rights. By bridging theoretical principles with practical applications, this chapter seeks to understand hoe remedies can be strengthen in access to them, as well as tuning the utmost guaranteeing procedures. Only through the combination of substance and procedure it is possible to ensure effective and efficient remedies.

6.2 Legal framework: the right to an effective remedy

The right to an effective remedy has roots in international human rights law. It is explicitly recognised in Article 8 of the Universal Declaration of Human Rights (UDHR)[985] and codified in binding instruments such as Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR).[986] This right also features prominently in regional frameworks, including Article 25 of the American Convention on Human Rights (ACHR),[987] Article 13 of the European Convention on Human Rights (ECHR),[988] and Article 47 of the CFREU.[989] For its part, the ECtHR has clarified that an effective remedy must be "as effective as can be,"[990] considering the inherent limitations of any

[985] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).
[986] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
[987] American Convention on Human Rights (22 November 1969), B-32 (ACHR).
[988] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
[989] "1. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. 2. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. 3. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice."
[990] ECtHR, *Klass v Germany,* App. no. 5029/ 71, 6 September 1978, §69.

legal system.[991] The ECtHR further mandates that remedies be both adequate and accessible, effective not only in theory but also in practice.[992]

6.2.1 The European legal framework

Codified in Article 47 CFREU,[993] the right has evolved into an independent guarantee for the enforcement of EU law, shaping the remedial obligations of both the EU and its Member States.[994] Therefore, Art. 47 encapsulates more than one meaning as per the multifaceted interpretation of the CJEU,[995] which developed a jurisprudence that strengthens the contours of this right through the principles of effectiveness and sincere cooperation, as in Article 19 para. 1 TEU, demonstrating its pivotal role in ensuring accountability and upholding fundamental rights within the Union.[996] As a matter of fact,

[991] The remedy must be capable of preventing or halting the alleged violation or offering appropriate redress. It is insufficient for remedies to exist merely in theory; they must be practically accessible and free from obstructions caused by state actions or inactions. Moreover, the efficiency of complaint procedures should not take precedence over the effectiveness of the remedy. FRA, 'European standards on legal remedies, complaints mechanisms and effective investigations at borders', 2021.

[992] *Inter alia,* ECtHR, El-Masri v. "the former Yugoslav Republic of Macedonia", App. no. 39630/09, 13 December 2012, in part., §255.

[993] Article 47 CFREU has a complex relationship with Articles 6 and 13 of ECHR as it draws inspiration from these provisions but also extends beyond their scope in significant ways. Whilst incorporating element from the Convention – where Art. 6 ECHR guarantees the right to a fair trial in disputes concerning civil rights and obligations or criminal charges, and Art. 13 ECHR secures the right to an effective remedy for individuals whose rights under the Convention have been violated – actually, Article 47 CFREU expands their application in two key respects. First, it applies to all areas of EU law, including administrative law, and is not limited to civil and criminal proceedings as Article 6 ECHR is. Secondly, differently than Art. 13 ECHR, adding emphasis on tribunals, underscores a higher standard of procedural rigour and judicial oversight. See, Kathleen Gutman, 'The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?' (2019) 20 German Law Journal 884.

[994] Takis Tridimas, 'The Rights of Defence' in Takis Tridimas (ed), *The General Principles of EU Law* (Oxford University Press 2006).

[995] The principle of effective judicial protection, reaffirmed by the CJEU in cases such as *Alassini*, stems from these constitutional traditions and aligns with the ECHR's guarantees of fair trial and effective remedies. However, Article 47 CFREU extends these rights by explicitly linking them to EU law and requiring judicial remedies rather than merely national authority oversight. This nuanced evolution reflects the EU's commitment to a robust framework for fundamental rights, which highlights the dual procedural and substantive guarantees enshrined in Article 47. Moreover, in *Francovich,* the CJEU ruled that EU law requires national courts to provide specific remedies, ensuring "the full effectiveness of that rule of Community law requires that there should be a right to reparation provided that three conditions are fulfilled", §39. See, CJEU (4th Sec.), *Rosalba Alassini v Telecom Italia SpA, Filomena Califano v Wind SpA, Lucia Anna Giorgia Iacono v Telecom Italia SpA, and Multiservice Srl v Telecom Italia SpA,* Joined cases C-317/08, C-318/08, C-319/08 and C-320/08, 18 March 2010; CJEU, *Andrea Francovich and Danila Bonifaci and others v Italian Republic,* Joined cases C-6/90 and C-9/90, 19 November 1991. See, also, Paul Craig and Gráinne de Búrca, '9. The Application of EU Law: Remedies in National Courts', *EU Law* (Oxford University Press).

[996] Damian Chalmers, Gareth Davies and Giorgio Monti (eds), 'Rights and Remedies in Domestic Courts', *European Union Law: Text and Materials* (4th edn, Cambridge University Press 2019); Bonelli (n 50).

since the Treaty of Lisbon entered into force, the right to an effective remedy has become central to the EU's constitutional framework.[997] Article 19 para. 1 TEU,[998] read with Article 4(3) TEU,[999] imposes an obligation on Member States to ensure effective judicial protection and maintain structural guarantees of judicial independence and separation of powers.[1000] The CJEU has emphasised that effective judicial protection is integral to the EU's rule of law, constituting the "essence" of the EU legal order.[1001]

The formulation adopted by the CFREU includes both the right to an effective remedy and a fair trial, establishing a foundational pillar for the enforcement of fundamental rights within the EU legal order. Its dual focus, described effectively by the literature with the expression "two strings on one bow",[1002] on procedural and substantive guarantee underscores its role as both a mechanism for individual redress and a structural safeguard for the rule of law.

The double-edged nature of this right is indeed exemplified by the wording and the structure of Art. 47 itself. Specifically, para. 1 guarantees the right to an effective remedy before a tribunal[1003] for anyone whose rights and freedoms under EU law are violated. This broad guarantee requires remedies to be accessible in practice and capable of addressing the alleged violations comprehensively, ensuring substantive and procedural

[997] Since the enter into force of the Lisbon Treaty, there has been an increasing attention on grantin this right, as demonstrated quantitively and qualitatively by Simona Demková and Herwig CH Hofmann, 'Chapter 12: General Principles of Procedural Justice' in Katja Ziegler, Paivi J Neuvonen and Violeta Moreno-Lax (eds), *Research Handbook on General Principles in EU Law* (2022).

[998] TEU, Art. 19, para. 1, "The Court of Justice of the European Union shall include the Court of Justice, the General Court and specialised courts. It shall ensure that in the interpretation and application of the Treaties the law is observed. Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law".

[999] This provision establishes the principle of 'sincere cooperation', and has been used by the CJEU so far to articulate stronger requirements of adequacy and effectiveness in the domestic enforcement of EU Law. Paul Craig and Gráinne de Búrca, '9. The Application of EU Law: Remedies in National Courts', *EU Law* (Oxford University Press).

[1000] Therefore, "in line with the obligations under Article 19 TEU, effective judicial protection must be offered not only by the CJEU but, first and foremost, by national courts and tribunals recognised as such by EU law", as in Demková and Hofmann (n 997).

[1001] *Inter alia,* CJEU (GC), *Rosneft EU*, C-72/15, §73, or CJEU (GC), *Minister for Justice and Equality v LM*, C-216/18, in part., § 51.

[1002] Giulia Gentile, 'Two Strings to One Bow? Article 47 of the EU Charter of Fundamental Rights in the EU Competition Case Law: Between Procedural and Substantive Fairness' (2020) 4 Market and Competition Law Review 169.

[1003] The concept of tribunal and court is defined by the CJEU, as, *inter alia,* in CJEU (GC), *Graham J. Wilson v Ordre des avocats du barreau de Luxembourg,* C-506/04, 19 September 2006, where it is stated that "whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law" (§48), then it can suffice the definition.

justice.[1004] Then, the second paragraph focuses on granting the right to a fair and public hearing within a reasonable timeframe by an independent and impartial tribunal.[1005] It also provides individuals with the right to legal representation, underlining the procedural safeguards necessary for fair judicial processes. Finally, paragraph three mandates the provision of legal aid to individuals lacking sufficient resources, but only to the extent necessary for effective access to justice.[1006] This ensures that economic barriers do not impede individuals from asserting their rights under EU law.

Ultimately, an effective remedy is a substantive right that ensures an adequate means of redress, whilst the right to fair trial encapsulates more the procedural dimension, as the effective access to a fair hearing vis-à-vis a judicial authority.[1007] In this respect, recent case law underscored the procedural safeguards that are indispensable to the effective application of Article 47 as in contexts shaped by technologies and automated decision-making systems.[1008] For instance, the *Ligue des droits humains*[1009] decision by the CJEU emphasised the necessity of individual review in situations involving automated decision-making, where decisions are often opaque and lack clear accountability. The judgment highlights the importance of procedural elements such as transparency and reasoning, which enable individuals to understand and challenge decisions that impact their fundamental rights.[1010] In this context, procedural safeguards are not merely technical

[1004] Within the concept of "effective remedies", the CJEU includes several elements: i. the right to bring an action; ii. the right of access to a tribunal; iii. the right to be heard; iv. the rights of the defence; v. the principle of equality of arms; vi. the principle of *audi altera partem.* For an overview of each elements, Gutman (n 993).

[1005] Romolo Donzelli, 'Sul «giusto processo» civile «regolato dalla legge»' [2015] Rivista di Diritto Processuale 942.

[1006] For the European perspective of the principle, Daniele Domenicucci and Fabio Filpo, 'La Tutela Giurisdizionale Effettiva Nel Diritto Dell'Unione Europea' in Oreste Pollicino and others (eds), *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè Editore 2017); whilst, for a national perspective, Marcello Stella, 'La tutela giurisdizionale effettiva nel diritto processuale civile' id. (Giuffré 2017).

[1007] For a general discussion, see Pekka Aalto et al., 'Right to an Effective Remedy and to a Fair Trial', in Steve Peers et al. (eds.), *The EU Charter of Fundamental Rights: A Commentary*, (Hart, 2014) in part., 1197–276.

[1008] On the power of exercising a real review of ADM decisions, see Simona Demková, 'Exercising Effective Review: Tust but Care?', in Simona Demková, *Automated Decision-making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023).

[1009] CJEU (GC), Ligue des droits humains ASBL v Conseil des ministres, C-817/19, 21 June 2022.

[1010] Id., §195, "given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained".

requirements but essential tools for preserving fairness and accountability in technologically complex scenarios.[1011]

Nonetheless, without any claim to exhaustiveness, we proceed from these premises to examine in the next paragraphs the scope of the rule's application, aiming to clarify its essential facets for the analysis of the present case related to ensuring access to effective remedies within the application biometric identification systems, such as FRT.

6.2.1.1 Applicability of the right

Article 47 CFREU applies broadly in both vertical and horizontal contexts, reflecting its expansive reach within the EU legal system. In its vertical application, Article 47 binds Member States and EU institutions, mandating them to uphold effective remedies whenever they act within the scope of EU law.[1012] Moreover, Art 47 CFREU must be interpreted "under the conditions and within the limits defined by relevant Treaty provisions which make provision for it", according to Art 52 para. 2 CFREU. Moreover, recent jurisprudence has expanded the applicability of Art. 47 beyond traditional vertical relationships, where it binds Member States and EU institutions, to horizontal disputes between private parties. The Court's ruling in cases such as *K.L. v X*[1013] illustrates this transformation. In *K.L. v X*, the Court affirmed that Article 47 could be invoked independently in a horizontal context, without requiring an intrinsic link to a specific directive or an underlying subjective right under EU law.[1014] This marked a shift in the Court's jurisprudence, emphasising that Article 47 is "sufficient in itself" to confer rights that individuals may invoke in disputes, thereby enabling the disapplication of conflicting national laws.

[1011] On a more general level, Francesca Palmiotto, 'Preserving Procedural Fairness in The AI Era: The Role of Courts Before and After the AI Act' [2023] Verfassungsblog <https://verfassungsblog.de/procedural-fairness-ai/> accessed 12 February 2024.
[1012] CFREU, Art. 51.
[1013] CJEU (GC), *K.L. v X sp. z o.o.,* C-715/2020, 20 February 2024.
[1014] Fien Van Reempts, 'The Court of Justice of the EU and the Philosopher's Stone: The Independent Horizontal Direct Effect of Article 47 of the Charter in K.L. v X: ECJ 22 March 2024, Case C-715/20, X (Absence de Motifs de Résiliation)' (2024) 20 European Constitutional Law Review 482.

6.2.1.2 Limitations

Despite its broad scope, Article 47 is not without limitations. Article 52 para. 1, CFREU permits restrictions on the right to an effective remedy, provided they respect the essence of the right, pursue legitimate general interest objectives, and satisfy proportionality requirements. For example, administrative exhaustion requirements, which require individuals to first seek resolution through administrative bodies, are permissible as long as they do not create unreasonable delays or excessive burdens.[1015] These limitations underscore the ongoing tension between procedural efficiency and the fundamental rights guaranteed by Article 47, highlighting the need for a nuanced approach that preserves the core essence of the right while accommodating practical constraints.[1016]

6.2.1.3 The role of MS in ensuring effective judicial protection

Furthermore, moving on to the analysis of the MS perspectives,[1017] the application of Article 47 within the EU legal framework, as briefly anticipated, is governed by the principles of equivalence and effectiveness.[1018] These principles allow Member States to retain procedural autonomy in designing remedies, provided such remedies are equivalent to those available for similar domestic claims (equivalence) and do not render the exercise of EU rights practically impossible or excessively difficult (effectiveness).[1019] This

[1015] Simona Demkova, 'The Decisional Value of Information in European Semi-Automated Decision-Making' (2021) 2 Review of European Administrative Law 38.

[1016] Domenicucci and Filpo (n 1006).

[1017] Koen Lenaerts, Kathleen Gutman and Janek Tomasz Nowak, 'Union Law and National Procedures and Remedies' in Koen Lenaerts, Kathleen Gutman and Janek Tomasz Nowak (eds), *EU Procedural Law* (Oxford University Press 2023).

[1018] Andreas Hofmann, 'The Role of National Courts in Redressing Fundamental Rights Violations by the EU' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024).

[1019] This relationship between EU and MS is regulated by the so-called Rewe test, articulated by the CJEU *Rewe-Zentralfinanz eG* and *Comet BV*, which clarified that Member States have the discretion to designate the competent courts and establish procedural rules in the absence of specific EU provisions. However, this discretion is contingent on meeting the conditions of equivalence and effectiveness. As the CJEU has emphasised, procedural conditions must provide not only theoretical access to remedies but also practical and enforceable avenues for redress. For instance, the effectiveness requirement entails ensuring both legal and practical possibilities for claims to be heard and decided on their merits. Subsequent case law has refined the Rewe principles, underlining the need for a balanced approach to procedural rules. For instance, in *Puškár*, the Court upheld Slovakian procedural rules requiring data subjects to first bring complaints before the data protection authority, viewing this as an efficient mechanism that complemented judicial remedies rather than undermining them. Such rulings highlight how national procedural rules can coexist

system of de-centralised enforcement is the 'procedural autonomy principle', which, even though it provides the MS with the power to design the national remedies and procedures, is not without caveat.[1020] Especially, as observed by scholars, a canon or a trend that emerged in the CJEU jurisprudence in so far as "a continuing reduction of the 'autonomy' of the Member States in the procedural field, and of stricter demands placed on the Member States by EU law".[1021]

In this respect, Italian jurisprudence provides an illustrative example of how Article 47 has been progressively integrated into domestic legal systems, particularly through its alignment with the standards of EU law. A foundational step in this alignment was the Constitutional Court's "twin judgments" (nos. 348 and 349 of 2007), which established EU law and the European Convention on Human Rights (ECHR) as essential benchmarks for evaluating the constitutionality of domestic legislation under Article 117, para. 1 of the Italian Constitution. These rulings underscored that remedies provided under Italian law must meet the procedural and substantive guarantees articulated in Article 47 CFREU, ensuring robust protection of fundamental rights.[1022]

These considerations become particularly critical in the context of emerging technologies such as facial recognition systems and AI-driven processes. The technical complexity and potential for rights violations in these contexts demand enhanced procedural safeguards to ensure fairness and accountability. As we move into the next section on due process, these issues underscore the need to examine how procedural guarantees and oversight mechanisms can address the unique challenges posed by these technologies and safeguard individuals' access to justice in the face of increasing automation in decisions.

with EU law requirements, provided they respect the principles of fairness, proportionality, and accountability. ECJ, *Rewe*, C-33/76, 1978, para 5; *Comet*, C- 45/76, 1979; ECJ, *Puškár*, C-73/16, 2017. See also Demková and Hofmann (n 997).

[1020] Matteo Bonelli, 'Article 47 of the Charter, Effective Judicial Protection and the (Procedural) Autonomy of the Member States' in Matteo Bonelli, Mariolina Eliantonio and Giulia Gentile (eds), *Article 47 of the EU Charter and Effective Judicial Protection* (Hart Publishing 2022).

[1021] Id.

[1022] Francesco Viganò, 'La Tutela Dei Diritti Fondamentali Della Persona Tra Corti Europee e Giudici Nazionali' [2019] Quad. cost.; Mart Cartabia, 'The Italian Constitutional Court and the Relationship Between the Italian Legal System and the European Community' (1990) 12 Michigan Journal of International Law 173.

6.3 The right to an effective remedy in the digital age

The right to an effective remedy, enshrined in Article 47 CFREU, is increasingly central to digital regulation as it provides a crucial legal foundation for protecting individuals in a rapidly evolving technological environment.[1023] This right serves as a benchmark for designing systems that not only address rights violations but also adapt to the unique challenges posed by algorithmic technologies that are reshaping contemporary society. In this context, the EU has increasingly expanded its regulatory intervention in the digital age, particularly with respect to remedies. Scholars have noted the proliferation of procedural safeguards across various regulatory frameworks.[1024] However, this expansion has been accompanied by significant fragmentation, which risks undermining the constitutional right to an effective remedy enshrined in Article 47 CFREU. The lack of harmonisation in procedural mechanisms not only jeopardises the consistency of rights protection across Member States but also challenges the enforceability and accessibility of remedies in practice.

In the landmark *Schrems judgments*, Article 47 CFREU emerged as a pivotal safeguard for the enforcement of fundamental rights, even in contexts extending beyond the EU's territorial jurisdiction. In *Schrems I*,[1025] the CJEU identified a violation of the essence of Article 47[1026] because the Safe Harbour framework failed to provide individuals with meaningful avenues to access, rectify, or erase their personal data when transferred to the United States. This lack of effective remedies was a key factor in the Court's ruling that the Safe Harbour decision was incompatible with EU law. Building on this precedent, the *Schrems II* judgment further underscored deficiencies in remedy mechanisms under the GDPR.[1027] The Court criticised the absence of redress mechanisms against certain forms of unlawful electronic surveillance conducted for national security purposes, finding this

[1023] Giovanni De Gregorio and Simona Demkova, 'The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe' (Social Science Research Network, 31 January 2024) <https://papers.ssrn.com/abstract=4712096> accessed 3 December 2024; Gentile, 'Between Online and Offline Due Process' (n 555); de Heer (n 981).

[1024] De Gregorio and Demkova (n 1023).

[1025] CJEU, Case C-362/14 *Schrems I,* cit.

[1026] Gloria Gonzalez Fuster, *The Essence of the Fundamental Right to Data Protection: Background Paper Commissioned by the European Data Protection Supervisor (EDPS)* (European Data Protection Supervisor (EDPS) 2023); Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779; Takis Tridimas and Giulia Gentile, 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794.

[1027] CJEU, Data Protection Commissioner v Facebook Ireland Ltd, Case C-311/18, cit.

incompatible with Article 47. Both these judgments highlighted the indispensable role of effective remedies in ensuring that fundamental rights are upheld in the digital age, particularly in the context of cross-border data transfers and surveillance frameworks.[1028]

Specifically, this concept has been translated by the EU to the field of data protection, e.g. in Art. 22 of the GDPR, where a right to contest the processing of personal data is solely based on automated systems.[1029] The reason why 'due process'[1030] mechanisms are so important both in the context of public law and of personal data is that they are "a sort of shield against arbitrariness".[1031] Therefore, they can facilitate the exercise of supervisory functions by any interested party. On the other hand, they impose specific obligations on the other party – be it a public or a private actor.

European data protection law has provided substantive obligations and procedural safeguards to regulate all aspects of data processing, from risk analysis to safeguards for data subjects. As emphasized in the literature, procedural rights also play a central role in ensuring a more complete enjoyment of substantive rights that can be enforced vis-à-vis private actors, even in the context predictive privacy violations[1032]. Thus, in the context of the Internet, 'due process' has gained increasing importance in enforcing the law and, in particular, fundamental rights. The GDPR is proof of this attitude which- as pointed out in the literature[1033] - was at least *de facto* recognized by the CJEU even before the GDPR entered into force, as shown by the saga regarding the right to erasure.

[1028] Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (n 181).

[1029] Henrik Palmer Olsen and others, 'What's in the Box? The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration' (Social Science Research Network 2019) SSRN Scholarly Paper ID 3402974; Francesca Palmiotto, 'When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis' (2024) 25 German Law Journal 210; S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243.

[1030] 'Due process' is a cornerstone of the US and UK legal systems, and, around the globe, is used in particular within the sphere of public and administrative law. As described in the literature, the 'due process' mechanism is the way the law is "both facilitating and constraining exercises of power by public authorities and in thus promoting public goals and protecting individual interests", Giacinto della Cananea and Giacinto della Cananea, *Due Process of Law Beyond the State: Requirements of Administrative Procedure* (Oxford University Press 2016).

[1031] Id.

[1032] Oreste Pollicino, 'The Quadrangular Shape of the Geometry of Digital Power(s) and the Move towards a Procedural Digital Constitutionalism' (2023) 29 European Law Journal 3.

[1033] Id. Pollicino (n 49); Giovanni De Gregorio (ed), 'Digital Constitutionalism, Privacy and Data Protection', *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022).

With respect to digital platforms and to strengthen the position of individuals vis-à-vis private actors,[1034] the approach of the EU, especially in recent regulatory developments such as the DSA[1035] and the Copyright Directive (Directive (EU) 2019/790),[1036] aimed to create and strengthen the procedural safeguards to rebalance and address the power asymmetries between individuals and large-scale private actors. As noted by scholars, "fundamental rights lend themselves to interpretative evolutions […] Due to their wide-ranging applications, the EU standards of due process have also been employed in the digital world",[1037] by imposing specific obligations on platforms to ensure transparency, accountability, and access to remedies.

Namely, the DSA requires platforms to notify users when content is removed, providing them with reasons for the decision and the opportunity to contest it.[1038] This includes the establishment of internal complaint mechanisms and access to independent out-of-court dispute resolution bodies.[1039] These procedural safeguards ensure that users are not left powerless in the face of opaque and unilateral decisions, reinforcing transparency and fairness in content moderation processes. Whereas the Copyright Directive mandates platforms to create mechanisms enabling content creators to contest decisions related to the takedown of their contents. Article 17 para. 9 requires Member States to ensure that disputes between users and platforms are subject to an impartial and efficient complaint-handling system.[1040] These safeguards illustrate the aim of the EU to use due process-like mechanisms to balance the rights of users and the responsibilities of private actors, fostering accountability while preserving fundamental rights.[1041]

[1034] Erik Longo, 'The Risks of Social Media Platforms for Democracy: A Call for a New Regulation' in Bart Custers and Eduard Fosch-Villaronga (eds), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice* (TMC Asser Press 2022).

[1035] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/ OJ L 277, 27.10.2022.

[1036] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, [2019] OJ L 130.

[1037] Gentile, 'Between Online and Offline Due Process' (n 556).

[1038] DSA, Art. 16.

[1039] DSA, Art. 20-21.

[1040] Alina Trapova, 'From Public to Private Enforcement – Inclusivity and Copyright Law' (Social Science Research Network, 2 August 2023) <https://papers.ssrn.com/abstract=4589884> accessed 2 December 2024.

[1041] De Gregorio and Demkova (n 1023).

Ultimately, all digital regulations, including the AI Act and GDPR, affirm the availability of judicial remedies as the ultimate recourse for individuals when administrative or internal complaints do not suffice.[1042] As a matter of fact, both under the GDPR and the DSA, a crucial role is served by supervisory authorities, such as Data Protection Authorities (DPAs) or Digital Services Coordinators, in handling complaints. These authorities can address violations, enforce regulations, and ensure compliance with EU law.[1043]

The analysis of remedies in digital regulation reveals a gradual evolution in the EU's approach to ensuring individuals have access to justice and meaningful redress. Frameworks such as the GDPR, DSA, and Copyright Directive showcase an increasing focus on procedural safeguards to address the asymmetries between individuals and powerful private actors, such as platforms and AI system deployers. These mechanisms, ranging from internal complaint systems to judicial remedies, highlight the EU's effort to operationalise Article 47 CFREU in the digital space. However, despite these advancements, significant fragmentation persists, and the question remains whether the AI Act, designed to govern high-risk AI applications, adequately addresses these gaps.

[1042] "The requirement of ensuring effective access to remedies is not an 'unfettered prerogative" […] EU law guarantees judicial remedy only as the final or ultimate remedy", id.

[1043] It is out of the scope of this thesis to address the role of SA. It suffices to highlight that, even though traditionally tasked with overseeing compliance with privacy and data protection laws, DPAs now face expanded responsibilities in addressing systemic risks posed by AI systems, such as biometric surveillance. Their role has shifted from merely enforcing compliance to also ensuring that individuals have access to remedies for rights violations, whether through administrative oversight or judicial redress. For example, under the GDPR, DPAs are empowered to investigate complaints, impose sanctions, and mandate corrective measures. These functions reflect the procedural guarantees of Article 47, ensuring that individuals can seek redress without facing insurmountable barriers. However, in the context of AI systems, the role of DPAs becomes more complex. Technologies like facial recognition are often deployed at scale, impacting large groups rather than identifiable individuals, and their systemic nature raises broader societal concerns. Supervisory authorities must therefore adapt their approaches to include not only traditional complaint-handling mechanisms but also proactive measures to address systemic risks. For a more in depth analysis, refer to Filippo Bagni and others, *Sistema Delle Fonti e Nuove Tecnologie: Il Ruolo Delle Autorità Indipendenti* (Giappichelli 2023); Koen Bovend'Eerdt, Argyro Karagianni and Miroslava Scholten, 'EU Law Enforcement Authorities and Access to Justice' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024); David E Shipley, 'Due Process Rights before EU Agencies: The Rights of Defense' (2008) 37 Georgia Journal of International and Comparative Law 1; Jeanne Pia Mifsud Bonnici and Ritumbra Manuvie, 'Supervisory Authority' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024); Herke Kranenborg, 'Right to an Effective Judicial Remedy against a Supervisory Authority' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024) < 4; Paul De Hert, 'Eu Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the Gdpr in the Spirit of Cooperative Federalism', *EU Law Enforcement* (Routledge 2021).

Unlike earlier regulations, the original proposal of the AI Act lacked robust mechanisms for individual redress.[1044] Its focus was on fostering compliance among developers and deployers of AI systems through ex-ante obligations, leaving individuals with limited recourse in cases of rights violations. This omission starkly contrasts with other frameworks, such as the DSA, which explicitly imposes obligations on platforms to provide internal and external mechanisms for contesting decisions. Scholars have criticized this approach, noting that without concrete procedural rights for individuals, the AI Act risks undermining the constitutional principle of effective remedies.[1045]

Subsequent amendments to the AI Act introduced provisions for individuals to lodge complaints regarding the misuse of AI systems.[1046] While this is a step forward, these rights remain narrow and lack detailed procedural safeguards akin to those in the DSA or GDPR. For example, the AI Act does not establish clear pathways for individuals to challenge decisions made by AI systems or demand transparency regarding the reasoning behind those decisions.[1047] Therefore, the AI Act's limited focus on remedies raises critical questions about how to operationalise the principles of accessibility, adequacy, and enforceability required under Article 47 CFREU. The absence of detailed provisions for complaint mechanisms and oversight bodies places an undue burden on individuals to navigate complex and fragmented legal systems.

As the chapter moves forward, the discussion will examine the AI Act's approach to remedies in greater detail, focusing on the rights it recognizes, its *lex specialis* nature, and its interaction with broader digital regulations. The analysis will highlight the need to strengthen both procedural and substantive safeguards to ensure that remedies under the AI Act are not only available but also effective in addressing the specific challenges posed by AI systems, particularly in the realm of biometrics. This examination will set the stage for a deeper exploration of two critical dimensions of remedies: agency, which addresses

[1044] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, Com/2021/206 Fin. On the evolution of the AI Act, *inter alia,* Francesca Palmiotto, 'The AI Act Roller Coaster: How Fundamental Rights Protection Evolved in the EU Legislative Process' (4 June 2024) <https://papers.ssrn.com/abstract=4904179> accessed 3 December 2024.

[1045] Margot E Kaminski and Jennifer M Urban, 'The Right to Contest Ai' (2021) 121 Columbia Law Review 1957.

[1046] This happened, especially, with the publication of the EP position, 14 June 2023. Palmiotto, 'The AI Act Roller Coaster' (n 303).

[1047] Fink and Finck (n 158).

who can claim rights under the Act, and procedure, which examines how those rights are operationalized to ensure meaningful access to justice.

6.4 The remedies under the AI Act

The regulation of FRT deployed by law enforcement authorities imposes the analysis of at least two regulatory frameworks, as explained in Chapter 3 of this thesis. It is worth underlining, however, that fundamental rights concerns when FRT is deployed stem not only from the risks to the freedom of the individuals whose facial images are captured and processed, who might be wrongfully identified, but also from their weak position, that a right such as Art. 47 should be able to re-balance.[1048]

In this respect, the rules established by the AI Act, as mentioned *supra,* are true *lex specialis* concerning data protection and law enforcement frameworks. This means that they take precedence over general data protection laws in situations where specific risky AI applications, such as biometric identification, are concerned.[1049] Specifically, Recital 38 of the AI Act makes it clear that the regulation's provisions, which prohibit certain uses of AI technologies like real-time biometric identification systems in publicly accessible spaces, should be understood as a more specialised set of rules derived from Article 16 TFEU.[1050] These rules are meant to apply as *lex specialis* in relation to the data protection standards established in the GDPR and in Article 10 of Directive (EU) 2016/680.[1051] This regulatory framework underscores the unique risks posed by AI-driven biometric systems and reflects the need for specific safeguards tailored to address these concerns.

[1048] European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019.

[1049] This classification ensures that the AI Act comprehensively governs both the use and processing of biometric data for law enforcement purposes, addressing the specific risks associated with these technologies in an exhaustive manner. By applying the principle of *lex specialis*, the Act ensures that the stricter rules it sets forth override more general provisions found in broader data protection laws. Consequently, when conflicts arise between the AI Act and other legal instruments on data protection, the AI Act's rules prevail, ensuring a more targeted regulatory approach to biometric surveillance and its potential impacts on privacy and civil liberties.

[1050] AI Act, Rec. 3.

[1051] 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.

Nonetheless, remedies peeped into the AI Act only at a later stage, as also an answer to the pressures of civil society and other institutions, such as the EDPS.[1052] It is to be said that such an answer was not as strong as it was hoped for.[1053] Particularly, Regulation (EU) 2024/1689 only suffices with three very general articles that reveal significant gaps in enforceability and coherence, especially in ensuring compliance with the principles of accessibility, adequacy, and enforceability required under Article 47 CFREU.

6.4.1 Another one bites the dust?

The AI Act introduces a framework for addressing high-risk AI systems through Articles 85, 86, and 87. However, these provisions largely prioritise systemic compliance over individual empowerment. With limited pathways for personal redress, the framework fails to fully operationalize the principles of effective remedies under Article 47 CFREU. This misalignment underscores the Act's inability to provide robust safeguards for individuals impacted by AI misuse. As a matter of fact, the Regulation includes only, in Chapter IX on 'post-market monitoring', the following: 1) Art. 85, the right to lodge a complaint vis-à-vis the Market Surveillance Authority; 2) Art. 86, the right to explanation; 3) Art. 87, reporting of infringements.

More specifically, Article 85 provides the right to lodge a complaint with national market surveillance authorities for violations of the AI Act. While this allows for administrative oversight, it lacks the robust procedural safeguards and judicial enforceability present in the GDPR[1054] and LED.[1055] Complaints remain limited to systemic violations, offering little recourse for individuals seeking redress for personal harm. Therefore, this Article and consequent Recital just refer to the other remedies present in the Union and national law,[1056] which would not be a problem if the remedies were sufficient in themselves, a question which will be examined in the following

[1052] EDPS, 'Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments', 23 October 2023.

[1053] Allow the reference to an earlier writing noting the lack of substantive remedies in the AI Act,
Federica Paolucci, 'Due Process of Artificial Intelligence: A Challenge for the Protection of Fundamental Rights', *Digital Single Market and Artificial Intelligence* (Aracne 2024).

[1054] GDPR, Art. 79.

[1055] LED, Art. 53-54.

[1056] As also specified by Rec. 170, AI Act, "without prejudice to those remedies, any natural or legal person that has grounds to consider that there has been an infringement of this Regulation should be entitled to lodge a complaint to the relevant market surveillance authority".

paragraphs and which we expect to be answered in the negative, at least for FRTs, as the legislator's intention to create a *lex specialis* on the same in the AI Act seems to be feared.

Following, Article 86 guarantees the right to an explanation for individuals impacted by decisions made using high-risk AI systems. However, this right is narrowly defined, focusing on providing clarity about the role of the AI system in decision-making but lacking the operational depth to challenge the outcomes effectively.[1057] This provision grants individuals affected by decisions made using high-risk AI systems the right to a "clear and meaningful explanation" of two factors: the role of the AI system in the decision-making process; and the main elements of the decision itself. This right is particularly relevant in contexts where decisions have significant legal or societal impacts, such as biometric identification used in public spaces. By providing individuals with insights into how decisions are made, the provision aims to enhance transparency and facilitate accountability. However, Article 86 suffers from critical limitations.[1058]

First and foremost, the right to explanation applies only to high-risk systems as defined in Annex III of the AI Act, excluding many AI-driven technologies that may still significantly impact individuals' rights. For example, systems used for real-time biometric identification are excluded since they are regulated by Art. 5, AI Act, and fall under the 'prohibited use' risk categorisation, and no specific extension of this right being made by the Regulation, despite their critical potential to influence decisions on fundamental rights, as largely documented in this thesis.

Secondly, the system for review is, once again – as also noted for the risk assessment –[1059] self-serving for the deployer, who, on the one hand, has no supervision in this respect, and, on the other, not being responsible for the training of the system, might lack the technical knowledge, or, even, might rely solely on the documentation shared by the provider. This accountability gap undermines the meaningfulness of the explanations

[1057] Simona Demková, 'The AI Act's Right to Explanation: A Plea for an Integrated Remedy' (*MediaLaws*, 31 October 2024) <https://www.medialaws.eu/the-ai-acts-right-to-explanation-a-plea-for-an-integrated-remedy/> accessed 3 December 2024; Ljubisa Metikos, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188.

[1058] The importance of this right is acknowledged, but with a view to delimiting the scope of this thesis, we refer to more appropriate analyses of Demková, 'The AI Act's Right to Explanation' (n 1056); Metikoš and Ausloos (n 122); Richard Mackenzie-Gray Scott and Elena Abrusci, 'Automated Decision-Making and the Challenge of Implementing Existing Laws' [2023] Verfassungsblog <https://verfassungsblog.de/automated-decision-making-and-the-challenge-of-implementing-existing-laws/> accessed 3 December 2024.

[1059] Wachter (n 244).

provided,[1060] leaving individuals without substantive recourse.[1061] Thirdly, unlike the GDPR, which outlines clear procedures for individuals to contest automated decisions (Article 22) and escalate complaints to supervisory authorities, the AI Act provides no direct procedural mechanisms to challenge insufficient explanations or enforce compliance with Article 86. Lastly, to conclude this brief overview, Article 87 addresses the protection of whistleblowers, aligning with Directive 2019/1937. While this safeguards systemic accountability, it does not directly empower individuals to contest violations stemming from AI system misuse.

Although the AI Act introduces mechanisms to address some procedural gaps, its reliance on compliance oversight and market surveillance authorities demonstrates a systemic bias toward ex-ante governance rather than ex-post remedies. This approach is deemed insufficient, as anticipated, for technologies like facial recognition systems, where rights violations often occur in real time and require immediate, enforceable solutions.[1062] In particular, it is crucial to underline two main critics: i) the absence of remedies or mechanisms that enable individuals to contest the deployment of high-risk AI systems before they are put into operation; ii) and, as a consequence, the limited role of the Authority under Art. 77.

On the first aspect, while Article 27 mandates that deployers of high-risk AI systems disclose FRIA as part of the assessment process, this disclosure is limited to internal compliance and reporting requirements just to the Market Surveillance Authority. It does not provide an avenue for external scrutiny or individual participation, leaving affected persons unable to raise objections or challenge the system's deployment proactively, with no mandatory public disclosure. This means that affected individuals have no formal mechanism to access the FRIA or contest its findings before the system is operational.

[1060] As specified by Metikos, explanations should be personalised, and, *inter alia*, "this provision misses any mention of the need to disclose the weight of different input variables. While the parameters and input data might be accurate, a litigant might also wish to contest the relative importance of certain data points. In addition, there is also no mention of disclosing the relationship between different parameters. Moreover, the pattern and correlation that an algorithm finds between different parameters can be contested as well by a litigant". Quoting Metikos (n 1057).

[1061] As suggested by Demková, it is crucial to design a system of accountability that interest the whole AI life cycle, namely "a collaborative responsibility between AI deployers and providers is essential for effective explanation and oversight", id.

[1062] See, also, the analysis of Demková referred to migration and border control in Simona Demková, 'The EU's Artificial Intelligence Laboratory and Fundamental Rights' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024).

The absence of pre-deployment remedies also undermines the principles enshrined in Article 47 CFREU, which guarantees individuals the right to an effective remedy. This internalised approach shifts the burden of oversight entirely to deployers and regulatory authorities, making it nearly impossible for individuals or civil society to voice concerns or protest against a system's use before harm occurs. Had the AI Act mandated public disclosure of FRIA findings or created mechanisms for independent review before deployment, it could have strengthened its framework for rights protection. Such provisions would align with the preventative approach envisioned in the GDPR, where DPIAs must be conducted and documented, and supervisory authorities can intervene to prevent harm before it occurs.

The second critical aspect regards the role of the Authority under Art. 77, AI Act. This provision introduces a unique mechanism for integrating fundamental rights oversight into the governance of high-risk AI systems. This provision ensures that national public authorities, tasked with supervising or enforcing Union law protecting fundamental rights, play a direct role in scrutinising the use of high-risk AI systems, including those in Annex III. Therefore, the article aims at bridging the gap between fundamental rights protection and AI-specific compliance by empowering these authorities to request documentation and even trigger testing of AI systems, when necessary, as per Art. 77 para. 1. However, this Authority is not tasked with the power to address direct complaints from individuals impacted by high-risk AI systems. The focus remains on enabling authorities to investigate compliance with fundamental rights protections, leaving individuals reliant on these authorities to act on their behalf. This approach introduces several limitations: individuals cannot directly invoke Article 77 to request documentation or trigger testing of AI systems, even when their rights are directly impacted.[1063].

This complex framework, when biometrics are deployed in the context of law enforcement is complemented by the LED:[1064] as specified by articles 53 and 54 of the Directive, individuals whose personal data is processed unlawfully have the right to an effective judicial remedy under the LED, ensuring access to justice even in contexts

[1063] AI Act, Art. 77, para. 4, any information or documentation obtained by the national public authorities or bodies referred to in paragraph 1 of this Article pursuant to this Article shall be treated in accordance with the confidentiality obligations set out in Article 78.

[1064] For the comparison and the integration of the disciplines, see Chapter 3.

involving sensitive law enforcement activities.[1065] Similar to the AI Act, the LED provides for complaints to supervisory authorities, enabling individuals to raise concerns about data processing violations. Finally, the LED guarantees the right to compensation for damages caused by violations of its provisions, creating a substantive pathway for redress that is often absent in the AI Act.[1066]

While these provisions provide a more structured framework for addressing rights violations, their effectiveness hinges on transparency: indeed, without meaningful disclosure of data processing activities or the deployment of systems like facial recognition technologies, affected individuals are left in the dark, unable to identify violations or seek timely remedies.[1067] This connection between transparency and accountability has been underscored by recent CJEU jurisprudence,[1068] on the interpretation of Articles 13 and 54 of Directive 2016/680.[1069] In this case, the CJEU addressed the interplay between the right to be informed and the right to an effective remedy. The Court clarified that transparency is not merely a procedural formality but a foundational element that enables individuals to exercise their rights under Article 47 CFREU effectively, especially in the context of law enforcement. The Court held that data subjects must be informed when authorities access their personal data unless doing so would jeopardise ongoing investigations. This obligation ensures that individuals are aware of potential violations and can seek judicial recourse when their rights are infringed. By linking the right to information with the right to a remedy, the Court emphasised the interconnectedness of transparency and accountability.[1070]

[1065] Kranenborg (n 64); Evelien Brouwer, 'Right to an Effective Judicial Remedy against a Controller or Processor' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[1066] Herke Kranenborg, 'Right to Lodge a Complaint with a Supervisory Authority' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

[1067] Kosta, 'Algorithmic State Surveillance' (n 144).

[1068] CJEU (Grand Chamber), *C.G. v Bezirkshauptmannschaft Landeck,* 4 October 2024, §111-123.

This case involved access to the applicant's, CG, mobile phone data, the Court found that the authorities should have informed the individual once disclosure no longer risked prejudicing the investigation. This failure undermined CG's ability to exercise his right to a judicial remedy under Article 54, reinforcing the critical role of transparency in upholding procedural fairness.

[1069] While Article 13 para. 3 of the LED permits Member States to limit the obligation to inform data subjects to protect investigative objectives, such limitations must comply with Article 52 para. 1 CFREU. Restrictions must be lawful, respect the essence of the right, and be proportionate. Blanket exclusions from transparency, the Court ruled, are incompatible with EU law, as they prevent individuals from exercising their fundamental rights.

[1070] Note, in particular, §118, "it is apparent from the case-law that the right to an effective judicial remedy, guaranteed in Article 47 of the Charter, requires, in principle, that the person concerned must be able to

The interplay between transparency and remedies is particularly significant in the context of biometric systems, such as facial recognition technologies. These systems often operate covertly, collecting and processing data without individuals' knowledge, thereby exacerbating the barriers to seeking redress. Without meaningful information sharing, such as notifying individuals when their data is collected or systems are deployed, it becomes nearly impossible to ensure effective remedies as guaranteed under Article 47 CFREU. Essentially, as also underlined by the FRA,

> "a precondition to exercise the right to an effective remedy is that a person must be aware that his or her facial image is processed. As the CJEU has noted, in the context of security measures affecting the right to private life and the right to the protection of personal data, national law enforcement authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer capable of jeopardising the investigations undertaken by those authorities. Such a situation occurs, for example, when law enforcement authorities populate a 'watchlist' used for facial recognition with a great number of facial images. The CJEU has found that notification is, in fact, necessary to enable the persons affected by these measures to exercise, inter alia, their right to an effective legal remedy guaranteed in Article 47 of the Charter."[1071]

Therefore, the LED's provisions, as interpreted by the CJEU,[1072] emphasise that remedies are not limited to judicial actions post-violation. They encompass procedural safeguards, including the right to be informed, which is essential for enabling individuals to hold authorities accountable. However, the lack of proactive transparency mechanisms

ascertain the reasons on which the decision taken in relation to him or her is based, so as to make it possible for him or her to defend his or her rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his or her applying to the court with jurisdiction, and in order to put the latter fully in a position in which it may carry out the review of the lawfulness of that decision".

[1071] European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019.

[1072] See also CJEU, joined cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, 21 December 2016, para. 12. See also, *mutatis mutandis*, C-555/07, Seda Kücükdeveci v. Swedex GmbH & Co. KG, 19 January 2010, para. 52; C-362/14, Maximillian Schrems v. Data Protection Commissioner, 6 October 2015, para. 95. 171 CJEU, joined cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others, 21 December 2016, para. 12.

in both the LED and the AI Act raises critical questions about the adequacy of the current framework for protecting fundamental rights in the age of AI.

At the centre of such critical aspects, we can find facial recognition: their invasive nature, use in public spaces, and potential for mass surveillance demand a harmonised legal response that goes beyond the fragmented remedies offered by the AI Act and LED. These systems raise critical questions about two main aspects: agency and authorisation: who is entitled to seek redress, and how are rights distributed in contexts where systemic risks, such as mass surveillance, affect entire populations rather than specific individuals? Who grants the 'legal green light' for deploying biometric systems, and what safeguards ensure that such authorisations respect fundamental rights and democratic principles?

The AI Act offers preliminary guidance on these issues. Article 5 para. 3 mandates prior judicial or independent administrative authorization for the use of real-time biometric systems in public spaces, while Article 26 para. 10 extends similar requirements to post-remote biometric identification systems. However, the effectiveness of these provisions hinges on their enforcement and the safeguards in place to monitor compliance, which remain limited. Moreover, the provisions address procedural elements without fully grappling with the broader implications for human rights and democratic accountability.

The FRIA framework, when properly integrated, offers a pathway to bridge this gap. By requiring deployers to evaluate not just the legality but also the societal impacts of biometric systems, FRIA demands transparency and accountability at every stage of the AI lifecycle. It shifts the focus from procedural compliance to the substantive protection of rights, emphasizing proportionality, necessity, and public oversight. For instance, FRIA could compel deployers to clearly outline who is impacted by these systems, how systemic risks are mitigated, and the mechanisms for redress, ensuring that the safeguards are not only theoretical but operational.

As we move forward, the interplay between agency and authorisation under the current legal framework will be critically examined to assess whether it can meaningfully respond to the complexities of biometric technologies. These questions go beyond technicalities or procedural safeguards; they challenge the very mechanisms by which fundamental rights are safeguarded in an era of pervasive AI. By embedding FRIA principles into these

considerations, the legal framework can be strengthened to ensure both individual and collective protections against the risks posed by FRT.

6.5 Agency: *ubi societas, ibi ius?*

Ubi societas, ibi ius, where there is society, there is law, is one of the most renowned legal maxims, emphasising the inseparable connection between human interactions and the regulatory frameworks governing them.[1073] This concept inherently recognises that law does not operate in isolation; it arises from and adapts to the complexities of societal structures.[1074]

In the context of agency under Article 47 CFREU, this brocardo acquires new dimensions. Agency, which determines who can assert their rights and seek remedies,[1075] becomes particularly intricate in the realm of algorithmic surveillance and biometric technologies. The concept of agency, determining who qualifies to assert their rights and seek remedies, is a pivotal dimension of Article 47 CFREU, particularly in the context of algorithmic surveillance and biometric technologies.[1076] Unlike traditional rights violations, these technologies challenge conventional understandings of victimhood by affecting not only individuals but also broader societal groups. As underlined by scholars, "the current legal regime is based to a large extent on the individual, such as by granting natural persons subjective rights to defend their individual interests, while data-driven projects often affect large groups or society as a whole".[1077] This broader scope raises profound legal and practical questions about who can claim victimhood and how current legal frameworks address the complexities of systemic technological impacts.

Moreover, biometric systems such as facial recognition operate both in real-time and remotely and captures data indiscriminately from all individuals within their operational range.[1078] This real-time nature means that individuals may be subjected to profiling,

[1073] Bin and Pitruzzella (n 21).
[1074] Pinelli (n 21).
[1075] Simona Demková,'Accessing Remedies', in Simona Demková, *Automated Decision-Making and Effective Remedies : The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023).
[1076] Melanie Fink, Clara Rauchegger and Joyce De Coninck, 'The Action for Damages as a Fundamental Rights Remedy' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024); Kosta (n 91).
[1077] van der Sloot and van Schendel (n 798).
[1078] Jasserand, 'The Future AI Act and Facial Recognition Technologies in Public Spaces' (n 404).

monitoring, or data processing without their knowledge or consent, creating a category of potential victims who are unaware of their rights being infringed.[1079] Moreover, the systemic nature of these technologies complicates the identification of specific harm or causality. For example, an individual subjected to real-time facial recognition in a public space may not know if their biometric data was processed, how it was used, or whether it led to adverse consequences such as misidentification or discriminatory profiling. Without meaningful transparency or notification requirements, these individuals are left in legal limbo, unable to assert their rights or claim victimhood effectively. This indiscriminate data collection creates a diffuse class of victims who may never know their data has been processed, let alone the potential uses or consequences.

Thus, as Kosta notes, "algorithmic surveillance creates new categories of individuals whose rights are at stake –those classified into groups based on opaque, data-driven profiling that they cannot contest."[1080]

These systemic impacts blur the boundaries between individual and collective harm, presenting unique challenges for accountability and redress. Moreover, the relevance of the group (which exists alongside the individual context, not as a replacement) is in some way evidenced by the FRIA itself.[1081] Article 27 of the AI Act, in its formulation, does not mandate a personalized assessment tailored to each individual, hence, *ad personam*; rather, it requires an evaluation of the impact that the use of a particular technology may have on identified categories of individuals. These categories are grouped together based on characteristics that may potentially trigger risks associated with the AI system. This approach reflects the systemic nature of technological impacts and underscores the importance of considering collective dimensions of harm when assessing the implications of AI-driven technologies.[1082]

[1079] van Schendel (n 148).

[1080] Kosta, 'Algorithmic State Surveillance' (n 144).

[1081] van der Sloot and van Schendel (n 798); Anuj Puri, 'The Group Right to Mutual Privacy' (2023) 2 Digital Society 22; Malou Beck and Sofia Ranchordás, 'Vulnerability' in Mareile Kaufmann and Heidi Mork Lomell (eds), *Handbook of digital criminology* (De Gruyter 2024).

[1082] The issue has been analysed at scholarly level also with respect to the right to privacy. *Inter alia,* Anuj Puri, 'The Group Right to Mutual Privacy' (2023) 2 Digital Society 22; Bart van der Sloot, 'Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected under Article 8 ECHR' [2017] Group privacy: new challenges of data technologies 197; Jennifer Jiyoung Suh and Miriam J Metzger, 'Privacy Beyond the Individual Level' in Bart P Knijnenburg and others (eds), *Modern Socio-Technical Perspectives on Privacy* (Springer International Publishing 2022).

Current legal mechanisms, including the AI Act, fail to provide proactive safeguards or clear pathways for individuals to challenge the deployment of such systems before harm occurs. This gap underscores the need for a rethinking of victimhood in the context of systemic technologies, ensuring that legal frameworks address not only post-violation remedies but also preventive and anticipatory measures to protect individuals in real-time. The challenges extend beyond mere infringements of the AI Act. These issues involve multiple layers of complexity, including the inherent opacity of AI systems and the difficulty of proving harm in FRT applications.

Nonetheless, the AI Act introduces significant regulatory mechanisms for AI systems, but it notably fails to address the issue of agency: who can claim remedies for harm caused by high-risk AI systems. Articles 85, 86, and 87 of the Act focus on procedural mechanisms, such as the right to lodge complaints with market surveillance authorities and the provision of whistleblower protections. However, these provisions do not establish clear standards for determining 'victimhood', nor do they provide meaningful pathways for individuals to challenge violations proactively.[1083] The omission is particularly problematic in the context of biometric surveillance, where individuals may be unaware that they have been subjected to monitoring or profiling. Without explicit mechanisms to notify individuals of their inclusion in biometric databases or their exposure to high-risk AI systems, the AI Act leaves significant gaps in the protection of fundamental rights.

Differently, the GDPR and the LED provide a structured framework for categorising individuals affected by data processing, ensuring their rights are protected in contexts involving surveillance and data use. Under Article 6 LED, competent authorities are required to distinguish between categories of data subjects, including suspects, convicted persons, victims, and other parties such as witnesses or informants.[1084] However, while this categorisation offers significant clarity, it inadvertently leaves out individuals who

[1083] The AI Act is quite vague in defining the contour of whom can actuate the remedies under Arts. 85-87, using just general wording like "any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation" (Art. 85), or, a bit more specific, "any affected person subject to a decision" (Art. 86). It is to be noted also that lack from the Regulation any specific definition to identify the "natural or legal person", differently from the GDPR, which refers to the concept of "data subject".

[1084] Teresa Quintel and Valsamis Mitsilegas, 'Distinction between Different Categories of Data Subject' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024).

may not fall into these defined groups but are nonetheless affected by the system, such as bystanders caught in surveillance[1085] or those whose data is incidentally processed without their awareness or explicit involvement.[1086]

This gap highlights a critical issue in the applicability of existing categorisations to modern surveillance contexts, particularly when advanced technologies like facial recognition systems are employed. For instance, individuals who pass by a camera in a public space and whose images are collected and potentially analysed, may not fit neatly into the defined categories of suspects, victims, or witnesses but are still subject to the implications of the system's operation, as also underlined by the FRA report on face recognition, *supra.* Their exclusion from structured protections under these categories underscores the inadequacy of current frameworks in addressing the broader societal impact of systemic data collection and use.

Moreover, this omission poses practical challenges for ensuring accountability and remedy. The lack of a category for incidental or unintentional subjects of data collection prevents these individuals from accessing the rights and safeguards afforded to formally recognized data subjects. This is particularly concerning in the context of widespread AI-driven surveillance, where the potential for "non-targeted" data collection is high, and the consequences for privacy and autonomy can be significant.[1087]

[1085] For example, *mutatis mutandis* a similar case is that of so-called 'indirect' interceptions, which are those interceptions, which, although placed on third parties' users, involved in the conversations involving Members of Parliament, as in the Decision n. 170/2023 of the Italian Constitutional Court. Pietro Villaschi, 'La Sentenza n. 170 Del 2023: La Corte Costituzionale Chiarisce Il Perimetro Della Nozione Di Corrispondenza e Torna Sull'interpretazione Della Legge n. 140 Del 2003' [2023] Rivista di Diritto dei Media - MediaLaws.

[1086] Please refer to the analysis of how these systems are trained with allegedly 'public available data', in Chapter 5.

[1087] The Europol case provides a critical illustration of this issue. Europol was found to have retained vast amounts of data,

including information on individuals who had no proven connection to criminal activities. The EDPS criticised Europol for its failure to adequately categorise the data subjects, leaving incidental individuals caught in data sweeps without meaningful protection or avenues for redress. This case underscores the risks of non-targeted data collection in undermining privacy and accountability, especially in systems reliant on broad data gathering from AI-driven tools. For further analysis, see the document examining Europol's data retention practices and the EDPS decision, Teresa Quintel, 'The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation: The Question of Legitimizing Unlawful Practices Reports: European Union' (2022) 8 European Data Protection Law Review (EDPL) 90; 'EDPS Takes Legal Action as New Europol Regulation Puts Rule of Law and EDPS Independence under Threat | European Data Protection Supervisor' (2022) <https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/edps-takes-legal-action-new-europol-regulation-puts-rule-law-and-edps-independence-under-threat> accessed 2 December 2024.

In this sense, the ECtHR has extensively addressed the concept of victimhood in the context of state surveillance, offering valuable insights that can inform also the regulation of AI-driven technologies. Key cases such as *Zakharov v. Russia*[1088] and *Big Brother Watch and Others v. UK*[1089] provide critical benchmarks for evaluating the scope of victimization and the availability of remedies.

In *Zakharov v. Russia*, the ECtHR recognized that the mere existence of broad and indiscriminate surveillance legislation could constitute a violation of individual rights, even in the absence of demonstrable harm. The Court emphasized that surveillance laws must be narrowly tailored and include robust safeguards to prevent overreach.[1090] This decision highlights the importance of scrutinizing not only the deployment of surveillance technologies but also the legislative frameworks that authorize them.[1091] Similarly, in *Big Brother Watch and Others v. UK*, the Court reiterated that the scope of surveillance legislation must be proportionate to its stated objectives. It further emphasized the need for stringent justifications and procedural safeguards to prevent the misuse of personal data. These rulings underscore that even individuals who cannot prove direct harm may be considered victims if surveillance measures disproportionately impact their rights or fail to provide adequate protections.[1092]

More specifically, the *Zakharov* decision addressed the difficulty of proving direct harm in secret surveillance contexts. The Court recognised that individuals could claim victimhood if they belonged to a group potentially subject to surveillance under an overly broad legislative framework.[1093] Similarly, in *Big Brother Watch*, the ECtHR highlighted

[1088] ECtHR (GC), *Zakharov v. Russia,* App. no. 47143/06, 4 December 2015.
[1089] ECtHR (GC), *Big Brother Watch v. U.K.*, App. no. 58170/13, 62322/14, 24960/15, 25 May 2021.
[1090] Lorna Woods, 'Zakharov v. Russia (Eur. Ct. H.R.)' (2016) 55 International Legal Materials 207.
[1091] Kosta, 'Algorithmic State Surveillance' (n 144).
[1092] Bart Van der Sloot and Eleni Kosta, 'Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance' (2019) 5 Eur. Data Prot. L. Rev. 252; Giulia Gentile, 'Does Big Brother Exist?: Facial Recognition Technology in the United Kingdom' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024); Paolucci Federica, 'Verso una normalizzazione della sorveglianza di massa? Big Brothers Watch c. Regno Unito, ultimo atto' [2021] Quaderni Costituzionali 981.
[1093] ECtHR, *Zakharov,* "The term "reasonable likelihood" implies that there are negative consequences for an applicant who is potentially subject to secret surveillance, on account of certain information that is made available to the authorities through interception, and excluding the possibility that this information could be uncovered by other means. The Court made this approach dangerously simple in order to examine the merits of these cases, presuming that persons who are subject to secret supervision by the authorities are not always subsequently informed of such measures against them, and thus it is impossible for the applicants to show that any of their rights have been interfered with. In these circumstances the Court concluded that applicants must be considered to be entitled to lodge an application even if they cannot show that they are victims", Concurring Opinion of Judge Dedov.

the societal harm caused by mass surveillance, emphasizing that effective remedies must account for the broader democratic implications of unchecked data collection.[1094] Henceforth, these cases demonstrate the importance of framing victimhood broadly to include individuals potentially affected by overreaching surveillance frameworks and recognising societal harms caused by systemic data collection.

In this regard, as argued, the AI Act falls short in providing a coherent and inclusive definition of agency that aligns with these principles. While it introduces essential regulatory mechanisms, it fails to ensure meaningful agency for individuals who are unaware of their victimisation or unable to trace the systemic impacts of AI technologies. The absence of mechanisms for proactive notification, transparency, and group-based remedies underscores the need for a paradigm shift in how agency and victimhood are conceived in the era of AI-driven technologies. A rethinking of legal frameworks to prioritise preventive and anticipatory measures is essential, ensuring that individuals and groups are equipped with the tools to assert their rights and secure meaningful remedies in real time. Only then can the systemic challenges posed by AI technologies be effectively addressed within the broader context of fundamental rights protection.[1095]

6.6 (Judicial) Authority: *quid iuris?*

The deployment of advanced surveillance technologies like facial recognition systems in law enforcement requires not only robust judicial authorisation mechanisms but also a re-evaluation of the broader context in which these systems operate: due to the systemic and pervasive nature of AI-driven technologies, it is necessary to assess the safety and appropriateness of the context in which FRT is deployed, particularly in public spaces where its use can result in widespread and often invisible impacts on fundamental rights.

[1094] ECtHR, *Big Brother Watch,* "While technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, global terrorism, drug trafficking, human trafficking and the sexual exploitation of children. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected. [..]. Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate" (§323).

[1095] Raffaele Bifulco, *Diritto e generazioni future: problemi giuridici della responsabilità intergenerazionale / Raffaele Bifulco* (FrancoAngeli 2008).

Consequently, the FRIA framework, as discussed in earlier chapters, offers a pivotal tool for embedding these broader considerations into the authorisation process. In law enforcement, FRIA's emphasis on evaluating not only the specific use of a technology but also the risks posed by its deployment in particular contexts ensures that decision-making moves beyond narrow justifications.[1096] For instance, authorising the use of FRT requires not only an examination of whether it is proportional in an individual case but also an analysis of its potential to create systemic risks.

In this sense, the European legislator's approach to the regulation of biometrics under the AI Act presents several critical points for discussion. This section, however, focuses specifically on the choice of authorisation methodology. As stipulated in Article 5, paragraph 5 of the AI Act, Member States are granted the discretion to determine whether the authorization for the use of certain AI technologies,[1097] such as real-time biometric identification systems, should be granted by a judicial authority or an independent administrative authority. As a matter of fact, the crucial aspect of this regulation is that both real-time and ex-post biometric systems can only be used with prior authorisation from a judicial or independent administrative authority, and even then, their use must be limited to "targeted" cases.[1098] This means that widespread, indiscriminate use of biometric identification technology is not permitted unless it is directly tied to a specific criminal threat, ongoing criminal proceedings, or the search for a missing person. These provisions are designed to mitigate the risks associated with biometric surveillance and protect individuals from disproportionate intrusions into their privacy and civil liberties, without banning all the use of biometrics.[1099]

This decision has significant implications, as it directly affects the level of oversight, scrutiny, and protection of fundamental rights associated with the deployment of these AI systems. Before delving into the analysis of these standards, it is crucial to underline that granting a certain degree of protection to the oversight of such privacy – *inter alia* – interferences are indeed an element of Art. 47. These frameworks ensure that the deployment and use of such technologies operate under continuous scrutiny, providing a

[1096] See, in part., Chapter 5.
[1097] AI Act, Art. 5 para. 3-5, Rec. 37.
[1098] See, in part., Chapter 2 and 3.
[1099] Civil society advocated in this direction, especially with the "Reclaim Your Face" Campaign promoted by EDRi, 'Facial Recognition Is Racist, Sexist & Creepy' (*Reclaim Your Face*) <https://reclaimyourface.eu/> accessed 3 December 2024 2024.

layer of protection that extends beyond initial approval. They align with Article 47 by guaranteeing that individuals have access to independent and impartial bodies, especially of a judicial nature, both oversee the deployment of these technologies and remain available to address any rights violations or disputes arising from their use.

Therefore, the choice between judicial and administrative authorisation is not merely procedural but reflects deeper concerns about how to balance security needs with the protection of civil liberties.[1100] The differences in accountability, transparency, and the degree to which fundamental rights are safeguarded vary greatly depending on the type of authority overseeing these decisions, and this divergence raises important legal and ethical considerations that will be explored in the following discussion.

6.6.1 Diverging standards of scrutiny

The choice between judicial authority and administrative authority is not neutral because the standards of authorization and oversight vary significantly between these two types of bodies, and the decision ultimately influences the balance between security needs and the protection of fundamental rights.[1101]

First and foremost, judicial authorities are inherently bound by constitutional safeguards and operate under a strict mandate to protect fundamental rights.[1102] Their decisions are typically subjected to higher levels of legal scrutiny, ensuring compliance with the principles of necessity, proportionality,[1103] and due process.[1104] This level of scrutiny is particularly important for AI-driven surveillance technologies,[1105] like

[1100] Rolando Tarchi and Andrea Gatti, 'Intelligenza Artificiale e Protezione Dei Dati Personali: Problemi Di Metodo e Di Procedura' (2024) 64 DPCE Online.

[1101] Casaburo and Marsh, "Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: the ALIGNER Fundamental Rights Impact Assessment", *AI and Ethics* (2024); Gutman, "The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?", 20 *German Law Journal* (2019), 884–903.

[1102] Cartabia, *I diritti in azione* (n 29).

[1103] Peers and others (n 977); Koen Lenaerts, 'Upholding the Rule of Law through Judicial Dialogue' (2019) 38 Yearbook of European Law 3.

[1104] Paolucci, 'Due Process of Artificial Intelligence: A Challenge for the Protection of Fundamental Rights' (n 1052); Frank Pasquale, 'Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication' in Amnon Reichman and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021).

[1105] The use of biometrics should not be treated differently than wiretapping and other surveillance measures, which is granted, at least in some Member States, such as in Italy, a high-level of protection with judicial oversight. See, in particular, Zecca (n 405).

biometrics, which have far-reaching implications for privacy, freedom of expression, and freedom of movement.

According to Article 47 of the EU Charter of Fundamental Rights, individuals must have access to effective judicial protection, which includes the right to an effective remedy before an independent and impartial tribunal.[1106] This standard of protection is integral to maintaining the rule of law within the EU and ensures that the deployment of risky AI technologies like biometric identification systems does not infringe upon individual rights.[1107] Hence, Art. 47's broad application requires national courts to play a key role in upholding EU law. In the context of AI and biometric technologies, individuals must have access to national courts to challenge both the legality of AI deployments and any resulting violations of their rights.

While procedural autonomy allows member states to determine how EU law is enforced within their jurisdictions, Article 47 creates a binding obligation to ensure that remedies are effective and equivalent to those provided under national law for similar violations. This is a critical point, as procedural autonomy should not become an excuse for insufficient access to justice in cases involving AI and fundamental rights. Furthermore, the CJEU has repeatedly ruled that member states must ensure that their legal systems provide for effective judicial protection, particularly in contexts where Union law guarantees specific rights. This is particularly important for AI enforcement, as gaps in national procedural frameworks could hinder the ability of individuals to access justice. For instance, if a member state's legal framework does not offer adequate remedies for violations of the AI Act, it could be seen as failing to meet its obligations under Article 47.[1108]

In contrast, independent administrative authorities, though often more specialised and efficient, may operate under less stringent requirements.[1109] Their decisions may be

[1106] de Heer (n 982); Gutman (n 50).
[1107] Kosta, 'Algorithmic State Surveillance' (n 144).
[1108] CJEU (Grand Chamber), *Associação Sindical dos Juízes Portugueses v Tribunal de Contas,* Case C-64/16, 27 February 2018. In this case, the Court reiterated that the right to effective judicial protection is essential to the rule of law in the EU, particularly where individual rights under Union law are at stake. This ruling reinforces the idea that judicial oversight is indispensable for ensuring that AI systems, especially those that affect fundamental rights, are deployed ethically and lawfully.
[1109] This is a problem already emerged in the data protection framework. A recent report by the Fundamental Rights Agency underscored that Data Protection Authorities should be strengthened in their independence, also from a human, financial, and technical point of view. European Agency for Fundamental Rights, 'GDPR in practice – Experiences of data protection authorities' <https://fra.europa.eu/es/publication/2024/gdpr-experiences-data-protection-authorities> accessed 8

driven by regulatory or policy considerations rather than a thorough analysis of the legal rights at stake.[1110] While administrative bodies can act more swiftly and may have technical expertise in AI, they are not constitutionally bound to the holy respect of the rule of law, which is a prerogative of the courts, instead.[1111]

Looking at the case study of this analysis, facial recognition technology, especially when used in public spaces, represents a severe intrusion into personal privacy. For this reason, the AI Act attempts to safeguard against these risks by requiring prior authorisation for such technologies, but the effectiveness of these safeguards depends on the nature of the authorising body.

As sustained in both literature and case law, judicial authorities can grant independence and transparency of a decision that has a high impact on the individual's rights, as the CJEU has clarified in *Corbiau*, C-24/92 (i.*e.* par. 15).[1112] In this decision, the Court placed significant importance on the idea of independence in defining whether a body constitutes a court or tribunal. This emphasis is not surprising given that the core principle of the rule of law hinges on the reviewability of decisions made by public authorities through independent courts. Moreover, in *Kadi and Al Barakaat*,[1113] the Court held that effective judicial review is essential for ensuring compliance with fundamental rights, particularly when administrative decisions have far-reaching consequences for individuals. This case underscores the need for courts to remain independent and impartial: a topical aspect especially when reviewing AI-related decisions, in high-risk contexts like biometric surveillance and law enforcement.

This choice is not without consequences since it might provoke a clash also with respect to the jurisprudence of the ECtHR, once again, to which the MS should refer. In this respect, the ECtHR elaborated a three-tiered 'quality of law' requirement to ascertain

October 2024. See also Philip Schütz, 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective' in Jan Camenisch and others (eds), *Privacy and Identity Management for Life* (Springer 2012).

[1110] Independence entails that these authorities should not receive instructions from any other entity concerning the performance of their duties. The CJEU ruled that a supervisory authority must be free from any external influence, whether that be from public or private sectors, ensuring that their decis*ion-making is solely based on the law.* CJEU (Grand Chamber), European Commission v Federal Republic of Germany.Case, C-518/07.

[1111] ECJ, *Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen***,** Case 14/83.

[1112] ECJ, Pierre Corbiau v Administration des Contributions, C-24/92.

[1113] CJEU (Grand Chamber), Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, Joined cases C-402/05 P and C-415/05.

the justification for the interference of law enforcement on individuals' privacy.[1114] Thus, according to established jurisprudence, any interference must adhere to stringent standards of legal quality, necessitating that domestic legislation be clear, foreseeable, and readily accessible. Specifically, the Court emphasised that domestic law must provide robust measures to prevent any misuse of personal data that could violate these guarantees. This need for safeguards is particularly pronounced when it comes to using personal data for police purposes, especially given the increasingly sophisticated technology available, as in the case of AI and biometric technologies. For this very purpose, the application of such systems should happen with adequate care of individuals' rights, striking a careful balance between the benefits of technology and the protection of fundamental rights,[1115] which is to be ensured via stringent justifications.[1116] Moreover, the Court, in the case of *Big Brother Watch and Others v. UK,* established that, especially in cases of criminal investigation, without individual knowledge, "in a field where abuse in individual cases is potentially so easy and could have such harmful consequences for a democratic society as a whole, it is desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure".[1117] The message here is very clear: the "best" option is the judge. And, such a best option is toward granting protection of fundamental rights when biometric systems are deployed. These principles underscore the critical role of judicial bodies in upholding the 'quality of law' requirements, which demand clear limitations and safeguards against arbitrary state action.[1118]

Thus, any infringement upon individuals' right to privacy, and thus any utilisation of biometric technology, must adhere to the principle of 'quality of law', guaranteeing thorough oversight by the judicial authority over the reasoned implementation of such

[1114] Jacob Livingston Slosser, 'Interpreting the "Quality of Law" at the European Court of Human Rights: Metaphorical Framing and Evaluative Judgment' (18 September 2018) <https://papers.ssrn.com/abstract=3251277> accessed 29 March 2024.

[1115] ECtHR (GC), *S and Marper v. the United Kingdom* nos. 30562/04 and 30566/04, § 67, 2006.

[1116] ECtHR (III Sec.), *Podchasov v. Russia,* no.33696/19, §60-65, 2021.

[1117] ECtHR (GC), Big Brother Watch and Others v. the United Kingdom, nos. 58170/13 and 2 others, 2021.

[1118] Further supporting this position, the United Nations High Commissioner for Human Rights has emphasized the necessity of judicial involvement in oversight of facial recognition technologies. In the report titled *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests* (UN Doc. A/HRC/44/24, 24 June 2020), it is recommended that States involve an independent body, preferably judicial in nature, to authorize the use of facial recognition technology in the context of assemblies. The report stresses that any use of facial recognition systems should be open to judicial challenge and urges authorities to ensure transparency, notifying the public whenever such technologies are deployed.

tools. Furthermore, legislation should clearly define the scope of discretion granted to competent authorities and specify how it should be exercised with precision to ensure individuals are adequately shielded from arbitrary encroachments.[1119]

Otherwise, the choice of the authorising entity could lead to significant risks, as evidenced by certain problematic examples. A particularly concerning case is that of Italy, where the National Cybersecurity Agency, a government-controlled body, has been appointed to oversee some aspects of AI authorisation.[1120] This raises serious questions about the independence and impartiality of the regulatory process, especially in the context of sensitive technologies like real-time biometric surveillance. Unlike judicial bodies or independent administrative authorities, which are designed to operate free from political or governmental influence, the National Cybersecurity Agency is inherently tied to the executive branch.[1121] The involvement of a governmental authority in this role introduces the risk of political interference in the regulatory process, impairing impartiality and separation of powers. Therefore, when applying this analysis to the case at hand, it becomes evident that a law in a Member State lacking a proper authorisation procedure evaluated by a judicial authority fails to uphold the aforementioned quality standards and safeguards.[1122] This example highlights the importance of ensuring that the entities responsible for overseeing AI technologies, especially those involving biometric surveillance, are truly independent of political influence.

6.6.2 'In subordine': at least a quasi-judicial oversight

When implementing the options offered by Article 5, paragraph 3, and Article 26, para. 10 of the AI Act, Member States should carefully evaluate the opportunity of entrusting judicial bodies with the responsibility for authorising the use of biometric systems. While judicial oversight ensures the highest level of independence, impartiality, and adherence to fundamental rights principles, as this thesis aimed to demonstrate,[1123] particularly in cases where these technologies pose significant risks to privacy and other rights, it is equally important to acknowledge the potential challenges associated with judicial

[1119] ECHR (III Sec.), *Glukhin v. Russia,* no. 11519/20, 2023.
[1120] Draft Law, Senate Act no. 1146, 'Disposizioni e delega al Governo in materia di intelligenza artificiale', 2024.
[1121] D.L. 14 June 2021, n. 82.
[1122] van der Sloot, 'The Quality of Law' (n 834).
[1123] §82-87 of the case.

authorisation, particularly the risk of procedural delays that could impede the timely deployment of AI systems in urgent or operationally sensitive contexts.

In light of these concerns, in this section is built, an argument '*in subordine',* in a subordinate position to the main one, *supra,* Member States should consider mixed oversight systems where judicial authorities work alongside independent administrative bodies. [1124]

In this sense, the ECtHR has also recognised, in cases like *Kennedy v. UK*,[1125] the validity of mixed or quasi-judicial oversight mechanisms as "good enough";[1126] thus, as an alternative, provided these systems maintain robust guarantees of independence, impartiality, and adherence to the principles of legality, necessity, and proportionality.[1127] This flexibility has, however, encountered a crucial threshold: targeted surveillance practices – such one of the uses that a deployer can make of the biometric identification systems authorised under the AI Act – present heightened risks of rights infringements and thus demand stricter judicial oversight.[1128]

Whereas, in landmark decisions such as *Szabó and Vissy v. Hungary*[1129] and *Zakharov v. Russia*,[1130] the ECtHR affirmed that, even though judicial review remains the preferable safeguard, the Court, recognising non-judicial oversight systems as effective when judicial components, independence, and broad oversight powers are integrated, adopted a flexible approach. Instead, the Court has repeatedly stressed the need for oversight mechanisms that combine independence, transparency, and sufficient enforcement powers, tailored to the specific risks posed by surveillance systems, hence tailored on how invasive the system is assessed to be.[1131]

[1124] Gianclaudio Malgieri and Paul De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017).

[1125] ECtHR (4th Section), *Kennedy v. UK,* App. no. 26839/05, 18 May 2010.

[1126] In *Kennedy*, for example, the ECtHR evaluated the role of the UK's Investigatory Powers Tribunal and the Interception of Communications Commissioner, acknowledging their effectiveness as hybrid oversight mechanisms that incorporate elements of judicial review while leveraging administrative and technical expertise.

[1127] See, also, ECtHR, *Huvig v. France*, No. 11105/84, 24 April 1990. Paul De Hert and Angela Aguinaldo, 'A Leading Role for the EU in Drafting Criminal Law Powers? Use of the Council of Europe for Policy Laundering' (2019) 10 New Journal of European Criminal Law 99.

[1128] Malgieri and De Hert, id. See, for instance, the case of *Glukhin v. Russia, supra.*

[1129] ECtHR, *Szabò and Vissy v. Hungary*, no. 37138/ 14 (2016).

[1130] Supra.

[1131] Malgieri and De Hert, id.

This is particularly true in the context of law enforcement, where the real-time application of FRT and other biometric systems carries a significant potential for abuse. The principles of necessity and proportionality, enshrined in both EU law and ECtHR jurisprudence, require that such intrusive measures be rigorously evaluated before deployment, with specific attention to the risks they pose to privacy, equality, and freedom of expression.[1132]

In this scenario, the FRIA proves to be, once again, a crucial guideline: as outlined in Chapter 4, offers an essential tool for embedding these considerations into authorisation processes. By integrating FRIA into judicial or hybrid oversight mechanisms, decision-makers can assess not only the immediate legality of deploying FRT but also the broader systemic risks associated with its use and then react accordingly to encompass the wider societal and contextual impacts of deploying surveillance technologies, including the chilling effects on public spaces and the potential for discriminatory profiling.

Before concluding the analysis of this chapter, the Italian experience with judicial authorisation for wiretapping offers further insights into the role of oversight in ensuring procedural safeguards for surveillance measures. As discussed earlier in this chapter, the Italian Constitutional Court has emphasised the need for judicial authorisation to include clear reasoning and justification, particularly in cases involving the use of wiretapping instruments. In conclusion, while hybrid mechanisms may suffice in certain scenarios, the use of highly intrusive biometric technologies such as FRT in law enforcement requires heightened judicial scrutiny. By embedding the FRIA framework into the oversight process, judicial and hybrid mechanisms can better address the complex interplay between technological capabilities and the protection of fundamental rights, ensuring that surveillance practices are both legally justified and ethically sound.

6.7 "It's a though call: they are so different": the Italian case

Since the Member States are soon tasked with the difficult responsibility of enforcing the AI Act, it is essential to examine how national legal frameworks align, or potentially conflict, with the regulation's provisions.[1133]

[1132] See, also, ECtHR, *Huvig v. France*, No. 11105/84, 1990. De Hert and Aguinaldo (n 1127).
[1133] In particular, the provisions on prohibited AI practices – therefore, also real time biometric systems – are going to be applicable starting from February 2025, according to AI Act, Art. 113(a), Rec. 179.

In this respect, the Italian legal framework governing the use of surveillance measures, such as wiretapping, offers significant insights into the balance between law enforcement needs and the protection of fundamental rights. This aspect has long been a subject of robust debate, with its constitutional safeguards under Article 15 of the Italian Constitution providing a pivotal anchor.[1134] The article ensures the inviolability of the freedom and secrecy of correspondence and communication, while allowing for limitations "only by a reasoned act of the judiciary and under conditions established by law."

Under current Italian law,[1135] telephone or digital communications interceptions are not permitted for contraventions (*contravvenzioni*); they are strictly reserved for the investigation of more serious crimes (*delitti*).[1136] These include offenses punishable by imprisonment, life sentences, or substantial fines.[1137] This distinction between *delitti* and *contravvenzioni* reflects a substantive and procedural differentiation that extends to the use of surveillance systems. Interceptions are therefore limited to cases involving significant criminal activity, ensuring that such intrusive measures are not employed for minor offenses.[1138]

[1134] Fabio Alonzi, Renzo Orlandi and Glauco Giostra, *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, vol 22 (G Giappichelli 2018); Cecilia Pannacciulli, 'Profili costituzionali delle intercettazioni di comunicazioni tra inadeguatezza del legislatore e discrezionalità del giudice' [2012] Rivista AIC; Alfredo Gaito, 'Riservatezza ed intercettazioni tra norma e prassi' (Aracne Editrice 2011); Francesco De Leo, 'Vecchio e nuovo in materia di intercettazioni telefoniche riguardanti reati non previsti nel decreto di autorizzazione ("Nota" a Cass. 23 giugno 1986, Frisina)' (1989) 112 Il foro italiano II; Paola Chiarella, 'Tra diritto di cronaca e privacy (sul filo delle intercettazioni telefoniche e degli internet blog)' [2010] Sociologia del diritto 1; Paolo Caponi, 'Pronto Chi Parla. Cesare e Le Intercettazioni Telefoniche' [2010] Altre Modernità 221; Davide Zecca, 'L'evoluzione Delle Comunicazioni e Dei Mezzi Di Ricerca Della Prova: Le Garanzie Nelle Costituzioni Democratico-Sociali', in Davide Zecca, *La tutela costituzionale della segretezza delle comunicazioni e della corrispondenza alla prova delle tecnologie emergenti: profili comparati* (Editoriale Scientifica 2023).

[1135] The Law No. 137 of 9 October 2023, which converted into law, with amendments, the Decree-Law No. 105 of 10 August 2023. For a comment, see Silvia Renzetti, 'Qualcosa è Cambiato : Vecchio e Nuovo in Tema Di Intercettazioni' [2024] Jus : rivista di scienze giuridiche : LXXI, 1, 2024 141; Daniele Scarpino, 'Intercettazioni e Delitti Di "Criminalità Organizzata" Tra Vecchi Problemi e Nuove Soluzioni' (2024) 64 Cassazione penale 1657.

[1136] Giorgio Marinucci and Emilio Dolcini, *Manuale Di Diritto Penale: Parte Generale* (Giuffrè editore 2012).

[1137] Article 17 para. 1, Italian criminal code. See, also, Article 266 and 266*bis* of the criminal procedure code.

[1138] This includes the deployment of trojans represents a paradigm shift in surveillance capabilities. Unlike traditional wiretapping, which focuses on specific communication channels, state trojans allow for pervasive monitoring, including the activation of microphones and cameras, the capture of encrypted data, and the tracking of user activity. Also, this type of instruments is subject to judicial authorisation, Fabio Alonzi, Renzo Orlandi and Glauco Giostra, *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, vol 22 (G Giappichelli 2018).

This differentiation has direct implications for the governance of facial recognition technologies within law enforcement.

The title of this paragraph, drawn from a famous movie, highlights the irony of describing two nearly identical items as vastly different. In the same vein, this section challenges the perception that FRT and interception are fundamentally distinct, arguing that FRT's greater intrusiveness necessitates even stronger safeguards for fundamental rights. As a matter of fact, according to Annex II of the AI Act, live facial recognition systems may be deployed by police authorities only for the prevention, detection, or prosecution of 'serious crimes.' However, this threshold does not extend to the use of remote facial recognition, which is not subject to the same stringent restrictions, due to Art. 6 and Annex II of the AI Act.

This discrepancy creates a potential conflict with the Italian approach, which is more protective of fundamental rights by restricting the use of surveillance systems, including FRT, to cases of crimes and explicitly excluding minor offenses.

A second area of potential conflict lies in the authorisation procedure, analysed, for the European part *supra*. The Italian Constitutional Court has consistently emphasised the necessity of judicial authorisation to include clear reasoning and justification, particularly in cases involving intrusive surveillance technologies.[1139] This requirement reflects the principles of proportionality, necessity, and legality, ensuring that intrusive measures like interceptions remain exceptional and narrowly tailored.[1140]

Furthermore, the Italian Constitutional Court jurisprudence has consistently reinforced this high standard of protection. For instance, judgments such as Nos. 34/1973 and 173/2009 highlight the judiciary's role in authorising such measures, emphasising detailed reasoning that assesses necessity and proportionality relative to the investigation's objectives.[1141] These must explicitly assess the proportionality and necessity of surveillance measures relative to the investigation. Such mandates are complemented by procedural safeguards like the obligation to deposit all collected

[1139] Davide Zecca 'La Tutela Costituzionale Della Segretezza Delle Comunicazioni Fra Avvento Dell'era Digitale e Crisi Del Paradigma Tradizionale Nella Ricerca Della Prova' (n 389).

[1140] See, also, for a referral of *ex post* authorization requests Cass., SS. UU. pen., sent. n. 2737/2006, 29 novembre 2005 (Campenni); Cass., SS. UU. pen., sent. n. 30347/2007, 12 luglio 2007 (Aguneche).

[1141] Corrado Caruso, 'La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale' (2013) Quaderni Costituzionali 10.

materials with judicial authorities, ensuring accountability and transparency.[1142] Furthermore, the Constitutional Court, in judgment No. 172/2019, mandated continuous judicial monitoring to oversee the relevance of collected data and its eventual destruction when no longer needed. These safeguards illustrate a robust system designed to prevent misuse and protect privacy rights.[1143]

By contrast, the AI Act introduces a procedural framework that, while robust, does not uniformly require judicial authorisation, especially for remote or indirect uses of FRT. Yet the draft Italian AI Bill (*Disegno di legge per la disciplina dell'intelligenza artificiale*), introduced in 2024, fails to seize this opportunity to establish a protective legal architecture.[1144] Notably, the draft law contains no provisions governing the use of biometric technologies or FRT, nor does it provide conditions for authorisation, independent oversight, or redress mechanisms.

What is more concerning is that the bill assigns significant competences in AI governance to two existing public authorities,[1145] the *Agenzia per l'Italia Digitale* (AgID) and the *National Cybersecurity Agency,* which are administrative bodies under direct governmental control and lack institutional guarantees of independence.[1146] In the context of technologies that pose high risks to fundamental rights, such as FRT, the absence of both dedicated safeguards and independent supervisory mechanisms undermines the effectiveness of any rights-based governance. This legislative silence and institutional design gap stand in stark contrast with the safeguards already established in Italian law for similarly intrusive technologies, such as wiretapping, and leave a deep normative and regulatory vacuum in an area of heightened constitutional sensitivity.

Meanwhile, the AI Act, specifically Article 5(5), requires that Member States lay down national legislation in order to authorise the use of real-time remote biometric identification in publicly accessible spaces by law enforcement authorities. This legislation must specify the legal basis, scope of application, authorisation procedures, and applicable criminal offences in line with Article 5(1)(h) AI Act. The Commission's

[1142] Alfredo Gaito, *Riservatezza ed intercettazioni tra norma e prassi* (Aracne Editrice 2011). On this respect, Italian Cost. Court, dec. 336/2008, as widely commented by Zecca (n 118), p. 63-64.
[1143] Pannacciulli (n 1134).
[1144] Provisions and powers delegated to the Government regarding artificial intelligence, approved by the Senate 20 March 2025.
[1145] Art. 19 of said DDL.
[1146] *Supra.*

implementation guidelines reaffirm that Member States are not obligated to permit such uses, but where they do, they must adopt detailed and rights-compatible national laws and notify them to the Commission.[1147] To date, Italy has not done so.

This raises a normative concern: if Italy demands strong judicial authorisation for wiretaps, how can it permit the deployment of FRT, an even more powerful surveillance tool, without any equivalent safeguards?

Given this framework, the Italian system, *a fortiori*, should not compromise on the use of FRT, which, while not significantly different in "formal" terms from the use of telephone or digital interceptors, carries a far greater potential for intrusiveness into fundamental rights.[1148] Recalling the title of this paragraph, this comparison highlights another critical issue: if the regulatory framework for interception in Italy is so robust, there is no justification for FRT to be subject to a less rigorous regime.

The argument that FRT should receive "easier" treatment falls apart when the fundamental similarity in their potential for rights intrusions is acknowledged. Instead, the principles underpinning interception regulations should serve as the baseline, or even the foundation, for the regulation of FRT, ensuring that the latter is governed with at least the same level of scrutiny and rights protection.

As demonstrated throughout this thesis, the deployment of FRT poses amplified risks to individual privacy and freedoms, surpassing those associated with traditional surveillance tools. Its ability to operate in real-time, indiscriminately collect biometric data, and impact individuals on a systemic level necessitates a stricter approach. The principles guiding the Italian framework for interceptors – such as judicial oversight, proportionality, and necessity – must therefore be equally, if not more, rigorously applied to FRT to ensure the continued protection of fundamental rights.

6.8 Conclusion

As the final chapter of the second part of this thesis, this analysis has explored the legal and procedural challenges surrounding the deployment of biometric technologies,

[1147] §412-413 of the European Commission Guidance on Art. 5, AI Act (Feb. 2025).

[1148] Giuseppe Mobilio, 'Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies' (2023) 12 Internet Policy Review; Neil M Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934; Julie E Cohen, 'Surveillance versus Privacy: Effects and Implications' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017).

particularly facial recognition systems, within the frameworks of the AI Act, GDPR and LED, and the European 'multi-level' protection of fundamental rights. These discussions underline the pressing need to adapt legal and governance mechanisms to address the unprecedented risks posed by high-risk AI systems, especially when deployed in sensitive contexts like law enforcement.

This chapter has not only examined the regulatory shortcomings of the AI Act – its fragmented approach to authorization, its limited safeguards for individual agency, and its insufficient transparency measures – but also positioned these gaps in relation to broader systemic concerns. Biometric technologies like FRT amplify these gaps through their capacity to operate indiscriminately, their opacity, and their potential to affect entire societal groups. The systemic and often diffuse nature of these impacts demands a fundamental rethinking of regulatory principles, moving beyond individual harm to account for collective and societal dimensions of rights protection.

The Italian system, with its robust judicial safeguards for surveillance, serves as a critical point of comparison. It highlights the importance of clear thresholds, such as restricting the use of surveillance technologies to the investigation of serious crimes, and the necessity of judicial authorisation as a substantive check against overreach. Yet, the analysis also demonstrates how FRT introduces risks that far exceed those posed by traditional surveillance tools, due to its capacity to target immutable personal characteristics, such as biometric data, and its scalability for mass surveillance. These distinctions emphasise the need for judicial oversight to play a central role in any regulatory framework for biometric technologies.

The chapter has also reiterated the potential of the Fundamental Rights Impact Assessment as a vital normative tool for embedding transparency, accountability, and proportionality into the governance of AI systems: it is sustained that the FRIA must evolve into a mechanism that not only assesses risk but also serves as a procedural safeguard for ensuring compliance with fundamental rights.

As this chapter concludes the second part of the thesis, it also marks a transition to the broader reflections and synthesis offered in the final conclusions. The second part has demonstrated that while significant strides have been made to regulate AI systems, the frameworks currently in place remain fragmented and, at times, insufficient to address the unique challenges posed by biometric identification systems, like facial recognition.

In conclusion, the findings of this chapter underscore a critical theme of this thesis: that the regulation of AI systems, and particularly biometric surveillance, must be grounded in a robust legal architecture that prioritises transparency, accountability, and enforceability. As the EU moves toward implementation of the AI Act, the lessons from this analysis – drawn from both European and national frameworks – highlight the urgent need for Member States to harmonise their approaches to ensure that fundamental rights remain at the core of governance structures.

In setting the stage for the final conclusions, this chapter serves as a call for action to bridge the gaps identified in existing regulatory frameworks and to move toward a more unified and rights-respecting governance model. Only by addressing these gaps can the EU ensure that its regulatory approach to AI not only aligns with technological advancements but also reaffirms its commitment to the principles of justice, equality, and human dignity. The protection of fundamental rights in the age of AI is not merely an option; it is indeed an existential challenge.

7.

CONCLUDING REMARKS

SUMMARY: 7.1 Main findings of the thesis. – 7.2 *De iure condendo:* a blueprint for the future.

7.1 Introduction

This thesis has delved deeply into the complexities of regulating Artificial Intelligence (AI), with particular attention to the role of Facial Recognition Technology (FRT) in shaping constitutional governance and impacting fundamental rights.[1149] FRT serves as a specialised observatory for examining the broader challenges posed by AI systems to constitutional governance and fundamental rights.

Through the exploration of the legal and social challenges, this work addresses the challenges posed by AI: while it offers immense potential for societal progress, it simultaneously disrupts traditional legal paradigms, posing unique threats to privacy, accountability, and the principles of democratic governance. The analysis throughout this thesis has been driven by the need to establish regulatory frameworks that prioritise human dignity and democratic principles while fostering innovation.

The foundational sections of this thesis traced the theoretical underpinnings of AI regulation, emphasising the evolving role of constitutional law in addressing the power dynamics introduced by AI.

Specifically, Chapter 1 analysed how AI reshapes governance structures, displacing traditional mechanisms of oversight and requiring a recalibration of constitutional principles.

Furthermore, Chapter 2 contextualised FRT within the broader trajectory of AI innovation, identifying the European Union's Artificial Intelligence Act (AI Act)[1150] as a

[1149] European Agency for Fundamental Rights (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement', 2019.

[1150] 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) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

pioneering yet incomplete framework. However, the chapter also described the AI Act's risk-based approach. Furthermore, the fragmented enforcement mechanisms and the absence of cohesive integration with complementary legal instruments, such as the GDPR[1151] and the LED,[1152] further complicate the Act's ability to provide robust safeguards.

In this respect, Chapter 3 extended this analysis by delving into the ethical, technical, and procedural dimensions of biometric identification systems, with a particular focus on FRT. It examined the deployment of such systems in public spaces and their implications for fundamental rights, stressing the tensions between their efficiency in enhancing security and their capacity to infringe upon privacy, data protection, and freedom of assembly.[1153] This chapter also evaluated how existing European legal instruments attempt to balance these concerns, identifying key gaps and areas for improvement, particularly in the context of real-time biometric surveillance technologies.

In the second part of the thesis, the focus shifted to the practical implications of AI governance. Chapter 4 introduced the Fundamental Rights Impact Assessment (FRIA)[1154] as a crucial tool for evaluating and mitigating the risks associated with high-risk AI systems. In this context, it is elaborated on a proposed model for FRIA that emphasises a structured, multi-phase process: identifying rights at risk, assessing the scope and nature of potential harms, and devising targeted mitigation strategies. However, this chapter also underscored the challenges of operationalising the FRIA, particularly the lack of a standardised methodology and practical implementation guidelines, which impedes its consistent application across diverse contexts.

Building on these findings, Chapter 5 applied this theoretical framework to biometric systems, offering an in-depth analysis of FRT's deployment in public spaces. The chapter, in particular, tested the FRIA model with respect to Article 8 of the CFREU, which regulates data protection. These analyses revealed critical shortcomings in existing

[1151] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L/119.

[1152] 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.

[1153] ECtHR [III Sec.,] *Glukhin v. Russia,* no. 11519/20, 2023.

[1154] AI Act, Art. 27.

safeguards, such as gaps in transparency, enforcement, and accountability, and highlighted the urgent need for robust procedural tools that can effectively address these vulnerabilities.

Finally, the FRIA has been further applied to another critical study: Chapter 6 extended this discussion by focusing on the right to an effective remedy under Article 47 of the Charter of Fundamental Rights of the European Union (CFREU). Despite existing procedural safeguards, this chapter revealed critical gaps in the ability of individuals to access meaningful remedies, particularly in the face of the systemic and opaque harms caused by AI technologies. The fragmented nature of the current regulatory landscape leaves individuals vulnerable, especially in contexts where FRT exacerbates societal inequalities or suppresses democratic trust. [1155]

At the heart of this thesis lies an exploration of the delicate interplay between technological innovation and constitutional safeguards designed to protect fundamental rights.[1156] In this sense, constitutional law provides the foundation for ensuring that advancements in AI remain aligned with democratic values and the protection of human dignity. However, the opacity of AI systems presents significant challenges to accountability and oversight. This lack of transparency undermines established legal principles of due process and exacerbates power asymmetries between individuals, and the state.[1157] To address this, regulatory frameworks must enforce stringent requirements for explainability, transparency, and traceability, ensuring that AI systems respect the rule of law.

Finally, the analysis concentrates on the Fundamental Rights Impact Assessment emerges as a pivotal tool in this context, offering a structured framework to evaluate and mitigate the societal and legal risks of deploying high-risk AI systems. Moreover, the intersection of AI governance and constitutional law necessitates a renewed focus on judicial oversight. Courts must play a central role in interpreting and enforcing AI-related regulations, ensuring that the principles of proportionality and accountability are upheld. Judicial interventions, grounded in the constitutional mandate to protect fundamental

[1155] Antonio Estella, 'Trust in Artificial Intelligence: Analysis of the European Commission Proposal for a Regulation of Artificial Intelligence Digital Transformations of Government: Towards a Digital Leviathan?' (2023) 30 Indiana Journal of Global Legal Studies 39.
[1156] Pollicino, '"Getting the Future Right – Artificial Intelligence and Fundamental Rights". A view from the European Union Agency for Fundamental Rights' (n 79).
[1157] Pollicino, 'Potere Digitale' (n 3).

rights, are essential to bridge the accountability gaps left by administrative oversight mechanisms.

In conclusion, the transformative potential of AI technologies like FRT underscores the urgency of reimagining constitutional principles in light of technological change. By embedding robust safeguards into the governance of AI systems, policymakers can ensure that innovation enhances – rather than undermines – democratic institutions and the dignity of individuals. The challenges outlined in this thesis highlight the imperative of harmonising technological progress with constitutional values, ensuring that advancements serve as instruments of human flourishing rather than tools of oppression.[1158]

7.2 *De iure condendo*: a blueprint for the future

To address the challenges identified in this thesis, a recalibrated governance framework must be developed that reflects both the immediate risks and the long-term societal implications of AI technologies. The following considerations are pivotal to this endeavour.

First, the AI Act's risk-based approach must be complemented by judicial oversight mechanisms that go beyond the limitations of administrative safeguards. Courts must be empowered to play a central role in interpreting and enforcing AI-related norms, ensuring that procedural protections are not only robust but also accessible. Independent judicial review is essential to counterbalance potential overreach by administrative bodies and to uphold the principles of transparency, legality, and accountability. This is particularly true for high-risk AI systems used in law enforcement, where remedies under Article 47 of the Charter of Fundamental Rights must be both practical and enforceable, addressing systemic harms while ensuring that individuals can effectively assert their rights.

Second, the operationalisation of the Fundamental Rights Impact Assessment (FRIA) must evolve from a compliance-oriented instrument into a normative constitutional safeguard. This thesis has argued that FRIA must not only assess the use of a given system, but also interrogate the broader legal and institutional context in which that system is embedded. The methodology must thus include criteria capable of evaluating

[1158] Safiya Umoja Noble, 'Algorithms of Oppression', *Algorithms of Oppression* (New York University Press 2018).

whether the legal basis, oversight architecture, and democratic accountability mechanisms meet constitutional standards. In this sense, FRIA becomes a vehicle for preventing structural harm before it materialises—ensuring that high-risk systems, such as real-time biometric identification, are only deployed within governance frameworks that are substantively rights-compliant.

Thirdly, future regulatory frameworks must address the systemic nature of AI-related harms. Traditional concepts of individual victimhood and redress are insufficient in the face of diffuse, collective, and often opaque harms produced by technologies such as FRT. Legal frameworks must anticipate these harms ex ante, embedding accountability mechanisms at every stage of system design, deployment, and review. This requires a paradigm shift in how regulators conceptualise responsibility: from individual fault to structural duty. Measures such as enhanced auditability, multi-stakeholder consultation, and legally binding impact assessments are essential components of this shift.

Fourthly, the harmonisation among existing regulatory instruments is imperative. The GDPR, LED, and AI Act must function as integrated components of a cohesive governance framework that prioritizes proportionality, transparency, and accountability. By reducing inconsistencies and fostering synergy among these instruments, regulators can provide clear and effective protections for individuals while promoting the responsible deployment of AI technologies. A unified approach to enforcement will ensure that overlapping responsibilities do not create gaps in oversight, particularly in cross-border applications of AI.

Finally, the Italian case analysed in this thesis illustrates the centrality of Member States in shaping the real impact of the AI Act. As the Commission's guidance makes clear, the use of real-time remote biometric identification systems in public spaces for law enforcement purposes requires a dedicated national legal basis. The AI Act leaves it to Member States to decide whether and how to adopt such laws. This delegation of normative responsibility is significant: it gives Member States not just the discretion to regulate, but the duty to define the legal, procedural, and oversight conditions under which AI systems may lawfully operate. Italy, at the time of writing, has yet to adopt such legislation. The 2024 draft AI Bill does not address biometric systems at all and entrusts governance competences to two administrative bodies that lack guarantees of

independence. Whether Italy will take this opportunity to embed the FRIA into a robust, constitutionally anchored legal framework remains to be seen, but the urgency is clear.

If judicial safeguards are deemed indispensable for traditional interception, measures already justified by compelling public interest, then *a fortiori*, FRT's systemic capacity to alter the public-private divide demands even stricter scrutiny. Italian constitutional jurisprudence offers a valuable lens here: judgments from the Constitutional Court have consistently upheld the primacy of personal freedoms against invasive state practices, affirming the central role of judicial oversight and legal proportionality. This legacy provides both a normative benchmark and an interpretative compass for the governance of AI-powered surveillance.

As President Sergio Mattarella has aptly warned, "We must ensure that the revolution we are experiencing remains human […] inscribed within the tradition of civilisation that sees the person, and their dignity, as the irreplaceable pillar."[1159] Ensuring that the transformative power of AI remains anchored in the values of human dignity, democracy, and the rule of law is the defining challenge of this technological age.

The findings of this thesis underscore the urgency of regulatory frameworks that are not only adaptive and forward-looking, but deeply rooted in constitutional principles. By advancing a normative model of the FRIA and demonstrating its application in the context of biometric surveillance, this research aims to contribute to a governance paradigm that respects fundamental rights at every stage of technological evolution. As the EU moves toward the full application of the AI Act, the question is no longer whether regulation is needed, but whether it will be designed to protect the constitutional core of our democracies. The answer will depend on the choices made today, by EU institutions, national legislatures, and judicial actors alike.

Mattarella's words serve as a reminder that the 'great leap' we are witnessing must not compromise the human-centric foundations of our civilisation, but rather reinforce them, ensuring that AI remains a tool for justice, not control.

[1159] 'Speech by the President of the Republic Sergio Mattarella at the opening ceremony of the 3rd Festival of Regions and Autonomous Provinces entitled "The Region of the Future between Digital and Green: what skills are needed to bridge the gap?"', 20 October 2024.

REFERENCES

Bibliography and online resources

Abbass H and others, 'Editorial: From Explainable Artificial Intelligence (xAI) to Understandable Artificial Intelligence (uAI)' (2024) 5 IEEE Transactions on Artificial Intelligence 4310

Akbari A, 'Facial Recognition Technologies 101: Technical Insights' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Akhtar M and Jørgensen RF, 'Chapter 4: A Rights-Based Approach to Automated Decision-Making in the Public Sector' (2024)

Almada M, 'Regulation by Design and the Governance of Technological Futures' (2023) 14 European Journal of Risk Regulation 697

Almada M and Petit N, 'The EU AI Act: A Medley of Product Safety and Fundamental Rights?' (18 October 2023) <https://papers.ssrn.com/abstract=4308072> accessed 3 December 2024

Alonzi F, Orlandi R and Giostra G, *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, vol 22 (G Giappichelli 2018)

——, *Nuove norme in tema di intercettazioni: tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, vol 22 (G Giappichelli 2018)

Alpaydın E, *Machine Learning* (MIT Press Essential Knowledge series 2016)

Amalfitano C, *General Principles of EU Law and the Protection of Fundamental Rights* (Edward Elgar Publishing 2018)

Amatuzzo A, ‘Wherever We Go, We Leave a Trail: Surveillance and Sousveillance in the United States and United Kingdom’ (2019) 7 Penn St. JL & Int’l Aff. 489

Andrew AM, ‘Reinforcement Learning: An Introduction by Richard S. Sutton and Andrew G. Barto, Adaptive Computation and Machine Learning Series, MIT Press (Bradford Book), Cambridge, Mass., 1998, Xviii + 322 Pp.’ (1999) 17 Robotica 229

Araszkiewicz M, Nalepa GJ and Pałosz R, ‘The Artificial Intelligence Act. Taking Normative Imbalances Seriously’ (*Internet Policy Review*) <https://policyreview.info/articles/news/artificial-intelligence-act-taking-normative-imbalances-seriously/1817> accessed 3 December 2024

Ausloos J, *The Right to Erasure in EU Data Protection Law* (1st edn, OUP Oxford 2020)

Aza A, ‘Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context’ [2024] Industrial Law Journal dwae035

Badri I and Sayyouri M, ‘Face Recognition: A Mini-Review’ in Saad Motahhir and Badre Bossoufi (eds), *Digital Technologies and Applications* (Springer Nature Switzerland 2023)

Balkin JM, ‘Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation’ (2017) 51 UCDL rev. 1149

Ballell TR de las H, ‘Legal Challenges of Artificial Intelligence: Modelling the Disruptive Features of Emerging Technologies and Assessing Their Possible Legal Impact’ (2019) 24 Uniform Law Review 302

Barabási A-L and PÃ3sfai M, *Network Science* (Cambridge University Press 2016)

Barak A (ed), ‘The Components of Proportionality’, *Proportionality: Constitutional*

Rights and their Limitations (Cambridge University Press 2012)

——, *Human Dignity: The Constitutional Value and the Constitutional Right* (Cambridge University Press 2015)

Barbera A, 'Ordinamento Costituzionale e Carte Costituzionali' [2010] Quaderni costituzionali

Barsotti V and others, 'Italian Constitutional Justice in Global Context', *Italian Constitutional Justice in Global Context* (Oxford University Press, Incorporated 2015)

Bartels M, 'A Balancing Act: Data Protection Compliance of Artificial Intelligence' (2024) 73 GRUR International 526

Bassini M, 'Fundamental Rights and Private Enforcement in the Digital Age' (2019) 25 European Law Journal 182

——, 'Data Retention as a Matter of Constitutional Law' in Eleni Kosta and Irene Kamara (eds), *Data retention in Europe and beyond* (2024)

Bassini M and Pollicino O, 'Reconciling Right to Be Forgotten and Freedom of Information in the Digital Age: Past and Future of Personal Data Protection in the European Union', [2014] Diritto Pubblico Comparato ed Europeo 641

Beck M and Ranchordás S, 'Vulnerability' in Mareile Kaufmann and Heidi Mork Lomell (eds), *Handbook of digital criminology* (De Gruyter 2024)

Beha C, 'Opinion | A.I. Isn't Genius. We Are.' *The New York Times* (26 December 2024) <https://www.nytimes.com/2024/12/26/opinion/ai-genius-art.html> accessed 3 December 2024

Beitz CR, 'International Concern' in Charles R Beitz (ed), *The Idea of Human Rights* (Oxford University Press 2009) <

——, 'Normativity' in Charles R Beitz (ed), *The Idea of Human Rights* (Oxford University Press 2009)

Bentham J, *Panopticon o La Casa d'ispezione* (Marsilio 1997)

Bertaina S and others, 'Fundamental Rights and Artificial Intelligence Impact Assessment: A New Quantitative Methodology in the Upcoming Era of Ai Act' (Social Science Research Network, 18 January 2024) <https://papers.ssrn.com/abstract=4698609> accessed 3 December 2024

Bifulco R, *Diritto e generazioni future: problemi giuridici della responsabilità intergenerazionale / Raffaele Bifulco* (FrancoAngeli 2008)

Bin R and Pitruzzella G, *Diritto Costituzionale* (Giappichelli 2015)

Black J and Murray AD, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10 European journal of law and technology

Bobbio N, *L'età Dei Diritti* (Einaudi 1990)

Bonelli M, 'Effective Judicial Protection in EU Law: An Evolving Principle of a Constitutional Nature' (2019) 12 Review of European Administrative Law 35

——, 'Article 47 of the Charter, Effective Judicial Protection and the (Procedural) Autonomy of the Member States' in Matteo Bonelli, Mariolina Eliantonio and Giulia Gentile (eds), *Article 47 of the EU Charter and Effective Judicial Protection* (Hart Publishing 2022)

Bonnici JPM and Manuvie R, 'Supervisory Authority' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

Boonstra M and others, 'Lessons Learned in Performing a Trustworthy AI and Fundamental Rights Assessment' (arXiv, 22 April 2024)

Bouchagiar G, 'A Fundamental Rights Impact Assessment for Dlt-Programmes

Targeted at the Public Sphere' (12 January 2024) <https://papers.ssrn.com/abstract=4693577> accessed 3 December 2024

Bovend'Eerdt K, Karagianni A and Scholten M, 'EU Law Enforcement Authorities and Access to Justice' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024)

Bradford A, 'Europe's Digital Constitution' [2023] Verfassungsblog <https://verfassungsblog.de/europes-digital-constitution/> accessed 3 December 2024

Brggemeier G, '6 Constitutionalisation of Private Law-the German Perspective', *Constitutionalisation of private law* (Brill Nijhoff 2006)

Brkan M, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864

Brouwer E, 'Right to an Effective Judicial Remedy against a Controller or Processor' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

Bryson JJ, 'The Artificial Intelligence of the Ethics of Artificial Intelligence: An Introductory Overview for Law and Regulation' in Markus D Dubber, Frank Pasquale and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (Oxford University Press 2020)

Büchi M and others, 'Chilling Effects of Profiling Activities: Mapping the Issues' [2019] Available at SSRN 3379275

Búrca G de, 'The Road Not Taken: The European Union as a Global Human Rights Actor' (2011) 105 American Journal of International Law 649

Busch F and others, ‘Navigating the European Union Artificial Intelligence Act for Healthcare’ (2024) 7 npj Digital Medicine 1

Busuioc M, ‘Accountable Artificial Intelligence: Holding Algorithms to Account’ (2020) 81 Public Administration Review

Butler I, ‘A Fundamental Rights Strategy for the European Union’ (Open Society Foundations 2014) <https://www.jstor.org/stable/resrep43002> accessed 3 December 2024

Bygrave LA, ‘Article 25 Data Protection by Design and by Default’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Bygrave LA and Tosoni L, ‘Article 4(1). Personal Data’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Article 4(11). Consent’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Caggiano G, ‘Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione’ 18

Calliess C and van der Schyff G (eds), ‘Comparative Constitutional Identity and Multilevel Constitutionalism’, *Constitutional Identity in a Europe of Multilevel Constitutionalism* (Cambridge University Press 2019)

Cananea G della and Cananea G della, *Due Process of Law Beyond the State: Requirements of Administrative Procedure* (Oxford University Press 2016)

Cantero Gamito M and Marsden CT, ‘Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act’ (2024) 32 International Journal of Law and Information Technology eaae011

Caponi P, ‘Pronto Chi Parla. Cesare e Le Intercettazioni Telefoniche’ [2010] Altre Modernità 221

Cardona-Pineda DS and others, ‘Face Recognition—Eigenfaces’ in Julian Andres Zapata-Cortes and others (eds), *Handbook on Decision Making: Volume 3: Trends and Challenges in Intelligent Decision Support Systems* (Springer International Publishing 2023)

Carena A, ‘Le Nuove Tendenze Del Diritto Costituzionale’ [1931] Annali di scienze politiche 248

Cartabia M, ‘The Italian Constitutional Court and the Relationship Between the Italian Legal System and the European Community’ (1990) 12 Michigan Journal of International Law 173

Cartabia M, ‘La tutela multilivello dei diritti fondamentali. Il cammino della giurisprudenza costituzionale italiana dopo l’entrata in vigore del Trattato di Lisbona’, Incontro trilaterale tra le Corti costituzionali italiana, portoghese e spagnola, Santiago del Compostela 16-18 ottobre 2014

Cartabia M, *L’ora Dei Diritti Fondamentali Nell’Unione Europea* (Il Mulino 2007)

——, *I diritti in azione: Universalità e pluralismo dei diritti fondamentali nelle Corti europee* (Società editrice il Mulino 2009)

——, ‘Prefazione’, *I diritti in azione* (Società editrice il Mulino, Spa 2009)

——, ‘Universality of Rights in the Era of “New Rights”’ [2009] Quaderni costituzionali

Cartabia M and Lupo N, ‘The Constitutional Court’, *The Constitution of Italy* (Bloomsbury Publishing Plc 2022)

Caruso C, ‘La libertà e la segretezza delle comunicazioni nell’ordinamento costituzionale’

Casaburo D and Marsh I, ‘Ensuring Fundamental Rights Compliance and Trustworthiness of Law Enforcement AI Systems: The ALIGNER Fundamental Rights Impact Assessment’ [2024] AI and Ethics

Cascini F and others, ‘Personalized Medicine Through Artificial Intelligence: A Public Health Perspective’ in Alfredo Cesario and others (eds), *Personalized Medicine Meets Artificial Intelligence: Beyond “Hype”, Towards the Metaverse* (Springer International Publishing 2023)

Castets-Renard C, ‘Human Rights and Algorithmic Impact Assessment for Predictive Policing’ in Amnon Reichman and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021)

Cavazos JG and others, ‘Accuracy Comparison across Face Recognition Algorithms: Where Are We on Measuring Race Bias?’ [2020] arXiv:1912.07398 [cs]

Cecchetti L, ‘Unravelling Horizontal Direct Effect in EU Law: The Case of the Fundamental Right to Paid Annual Leave between “Myth” and “Practice”’ (2023) 42 Yearbook of European Law 42

Celeste E, *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2022)

Celeste E and Gregorio GD, ‘Digital Humanism: The Constitutional Message of the GDPR’ (2022) 3 Global Privacy Law Review

Ćemalović U, ‘Prohibited Artificial Intelligence Practices According to Article 5 of the European Union’s Regulation on AI—between the “Too Late” and the “Not Enough”’ (2024) 32 International Journal of Law and Information Technology eaae023

Chalmers D, Davies G and Monti G (eds), ‘Rights and Remedies in Domestic Courts’,

European Union Law: Text and Materials (4th edn, Cambridge University Press 2019)

Chamon M, 'The Legal Framework for Delegated and Implementing Powers Ten Years after the Entry into Force of the Lisbon Treaty' (2021) 22 ERA Forum 21

Chiara P and Galli F, 'Normative Considerations on Impact Assessments in EU Digital Policy' [2024] MediaLaws

Chiarella P, 'Tra diritto di cronaca e privacy (sul filo delle intercettazioni telefoniche e degli internet blog)' [2010] Sociologia del diritto 1

Christakis T and others, 'Mapping the Use of Facial Recognition in Public Spaces in Europe – Part 1: A Quest for Clarity: Unpicking the "Catch-All" Term' (15 May 2022)

Christensen TK, 'Pre-Installed Cameras in Vehicles—New Technology from a Data Protection Law Perspective' (2024) 53 Computer Law & Security Review 105980

Ciacchi AC, 'The Direct Horizontal Effect of EU Fundamental Rights: ECJ 17 April 2018, Case C-414/16, Vera Egenberger v Evangelisches Werk Für Diakonie Und Entwicklung e.V. and ECJ 11 September 2018, Case C-68/17, IR v JQ' (2019) 15 European Constitutional Law Review 294

Cohen JE, 'Surveillance versus Privacy: Effects and Implications' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017)

Cohen JE and Cohen JE, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019)

Craig P and Búrca G de, '9. The Application of EU Law: Remedies in National Courts', *EU Law* (Oxford University Press)

——, '12. Human Rights in the EU', *EU Law* (Oxford University Press)

Craig PP, ‘The Charter, the ECJ and National Courts’ in Diamond Ashiagbor, Ioannis Lianos and Nicola Countouris (eds), *The European Union after the Treaty of Lisbon* (Cambridge University Press 2012)

Custers B and Malgieri G, ‘Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data’ (19 January 2022) <https://papers.ssrn.com/abstract=4329245> accessed 3 December 2024

Cynthia O’Murchu, ‘Facial Recognition Cameras Arrive in UK School Canteens’ *Financial Times* (17 October 2021) <https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9> accessed 3 December 2024

Dalla Corte L and van Brakel R, *Data Protection Impact Assessment Methods for the Urban Environment: A Report for the Commissie Persoonsgegevens Amsterdam (CPA)* (2022)

Danaher J, ‘The Threat of Algocracy: Reality, Resistance and Accommodation’ (2016) 29 Philosophy & Technology 245

Data D, ‘Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice’(Vol’ 94 New York University Law Review 2019

de Abreu Duarte F, De Gregorio G and Golia A, ‘Perspectives on Digital Constitutionalism’ (2023) <https://papers.ssrn.com/abstract=4508600> accessed 3 December 2024

de Beco G, ‘Human Rights Impact Assessments’ (2009) 27 Netherlands Quarterly of Human Rights 139

de Búrca G, ‘After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?’ (2013) 20 Maastricht Journal of European and Comparative

Law 168

De Felice D, ‘Business and Human Rights Indicators to Measure the Corporate Responsibility to Respect: Challenges and Opportunities’ (2015) 37 Human Rights Quarterly 511

De Gregorio G, ‘The Rise of Digital Constitutionalism in the European Union’ [2021] International Journal of Constitutional Law <https://doi.org/10.1093/icon/moab001> accessed 23 May 2021

——, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022) <

—— (ed), ‘Digital Constitutionalism, Privacy and Data Protection’, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge University Press 2022)

——, ‘The Normative Power of Artificial Intelligence’ (2023) 30 Indiana Law Journal

De Gregorio G and Demková S, ‘The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe’ in Charlotte van Oirsouw and others (eds), *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era* (TMC Asser Press 2024)

De Gregorio G and Demkova S, ‘The Constitutional Right to an Effective Remedy in the Digital Age: A Perspective from Europe’ (Social Science Research Network, 31 January 2024) <https://papers.ssrn.com/abstract=4712096> accessed 3 December 2024

de Heer S, ‘Artificial Intelligence and the Right to an Effective Remedy’ in Alberto Quintavalla and Jeroen Temperman (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023)

De Hert P, ‘A Human Rights Perspective on Privacy and Data Protection Impact Assessments’ in David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, vol 6 (Springer Netherlands 2012)

De Hert P and Aguinaldo A, ‘A Leading Role for the EU in Drafting Criminal Law Powers? Use of the Council of Europe for Policy Laundering’ (2019) 10 New Journal of European Criminal Law 99

De Hert P and Bouchagiar G, ‘European Biometric Surveillance, Concrete Rules and Uniform Enforcement: Beyond Regulatory Abstraction and Local Enforcement’, *Cambridge Handbook on Facial Recognition in the Modern State* (Cambridge Univ Press 2024)

de Hert P and Sajfert J, ‘Regulating Big Data in and out of the Data Protection Policy Field: Two Scenarios of Post-GDPR Law-Making and the Actor Perspective’ (2019) 5 European data protection law review (Internet) 338

de Terwangne C, ‘Article 5 Principles Relating to Processing of Personal Data’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Demkova S, ‘The Decisional Value of Information in European Semi-Automated Decision-Making’ (2021) 2 Review of European Administrative Law

Demková S, *Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023)

——,‘Accessing Remedies’, in Simona Demková, *Automated Decision-Making and Effective Remedies : The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023)

Demkova S, ‘The EU’s Artificial Intelligence Laboratory and Fundamental Rights’ (Social Science Research Network, 31 August 2023)

Demková S, ‘The EU’s Artificial Intelligence Laboratory and Fundamental Rights’ in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the ‘Complete System of Remedies’* (Cambridge University Press 2024)

——, ‘The AI Act’s Right to Explanation: A Plea for an Integrated Remedy’ (*MediaLaws*, 31 October 2024) <https://www.medialaws.eu/the-ai-acts-right-to-explanation-a-plea-for-an-integrated-remedy/> accessed 3 December 2024

‘Exercising Effective Review: Tust but Care?’, in Simona Demková, *Automated Decision-making and Effective Remedies: The New Dynamics in the Protection of EU Fundamental Rights in the Area of Freedom, Security and Justice* (Edward Elgar Publishing 2023)

Demková S and Hofmann HCH, ‘Chapter 12: General Principles of Procedural Justice’ in Katja Ziegler, Paivi J Neuvonen and Violeta Moreno-Lax (eds), *Research Handbook on General Principles in EU Law* (2022)

der Sloot B van, ‘Principles Relating to Processing of Personal Data’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

Dimitrova D, ‘Limitations to the Right of Access’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

——, ‘Right to Rectification or Erasure of Personal Data and Restriction of Processing’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

Docksey C, ‘Article 24 Responsibility of the Controller’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Domenicucci D and Filpo F, ‘La Tutela Giurisdizionale Effettiva Nel Diritto Dell’Unione Europea’ in Oreste Pollicino and others (eds), *Carta dei Diritti Fondamentali dell’Unione Europea* (Giuffrè Editore 2017)

Donzelli R, ‘Sul «giusto processo» civile «regolato dalla legge»’ [2015] Rivista di Diritto Processuale 942

Doshi-Velez F and others, ‘Accountability of AI Under the Law: The Role of Explanation’ [2017] arXiv.org

Dove ES and Chen J, ‘What Does It Mean for a Data Subject to Make Their Personal Data “Manifestly Public”? An Analysis of GDPR Article 9(2)(e)’ (2021) 11 International Data Privacy Law 107

Draghi M, ‘The Future of European Competitiveness’ (*European Commission*, 2024)

Dunlop CA and Radaelli CM, *Handbook of Regulatory Impact Assessment / Edited by Claire A. Dunlop, University of Exeter, UK ; Claudio M. Radaelli, University of Exeter, UK* (Edward Elgar Publishing 2016)

Dunn P and Giovanni De Gregorio, ‘The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies’ (CEUR Workshop Proceedings 2022)

Dunn P and Gregorio GD, ‘The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age’ (2022) 59 Common Market Law Review

Dupré C, ‘Human Dignity in Europe: A Foundational Constitutional Principle’ (2013) 19 European Public Law

Durst L, ‘Il Trattamento Dei Dati in Ambito Sanitario, In’, *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, a cura di Rocco Panetta.* (Giuffrè Francis Lefebvre 2019)

Dushi D, ‘The Use of Facial Recognition Technology in EU Law Enforcement: Fundamental Rights Implications’ (Global Campus 2020)

Ebers M and others, ‘The European Commission’s Proposal for an Artificial

Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4 J 589

'EDPS Takes Legal Action as New Europol Regulation Puts Rule of Law and EDPS Independence under Threat | European Data Protection Supervisor' (2 December 2024)

Edwards L, 'Expert Opinion: Regulating AI in Europe' (2022)

Edwards L and Veale M, 'Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking For' (LawArXiv 2017) preprint

Elliott A, *Making Sense of AI: Our Algorithmic World* (John Wiley & Sons 2021)

Estella A, 'Trust in Artificial Intelligence: Analysis of the European Commission Proposal for a Regulation of Artificial Intelligence Digital Transformations of Government: Towards a Digital Leviathan?' (2023) 30 Indiana Journal of Global Legal Studies 39

'Explainable AI (XAI)', in Keri Grieman, *Law, Death, and Robots: The Regulation of Artificial Intelligence in High-Risk Civil Applications* (1st ed., Hart Publishing 2024)

'Facial Recognition Is Racist, Sexist & Creepy' (*Reclaim Your Face*) <https://reclaimyourface.eu/> accessed 3 December 2024

'Facial Recognition: The CNIL Orders CLEARVIEW AI to Stop Reusing Photographs Available on the Internet | CNIL' <https://www.cnil.fr/en/facial-recognition-cnil-orders-clearview-ai-stop-reusing-photographs-available-internet> accessed 3 December 2

Fajdiga M, 'Chilling Effect: Turning the Poison into an Antidote for Fundamental Rights in Europe' [2024] Maastricht Journal of European and Comparative Law

Fajdiga M and Zagorc S, ‘Freedom or Feardom of Expression of Judges? Exploring the “Chilling Effect” on Judicial Speech’ (2023) 19 European Constitutional Law Review 249

Fasano G, ‘L’interpretazione estensiva della nozione di “decisione automatizzata” ad opera della Corte di giustizia: una prospettiva più ampia ma ancora fragili tutele per le libertà fondamentali’ (2024) 6 Rivista italiana di informatica e diritto 15

Fasciglione M, ‘An International Mechanism of Accountability for Adjudicating Corporate Violations of Human Rights? Problems and Perspectives’ [2019] Judicial Power in a Globalized World: Liber Amicorum Vincent De Gaetano 179

Ferguson AG, ‘Facial Recognition and the Fourth Amendment’ (2021) 105 Minnesota law review 1105

Ferrari GF, ‘Diritti fondamentali: linee evolutive, diffusione e tipologie’ (UTET 2023)

——, *I diritti nel costituzionalismo globale: luci e ombre / Giuseppe Franco Ferrari* (Prima edizione pubblicata in Italia, Mucchi Editore 2023)

Finck M, ‘Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy’ (Social Science Research Network, 20 June 2017)

——, ‘The Maturation of European Data Law: From Fundamental Rights to Economic Rights’ in Jeremias Adams-Prassl and others (eds), *The Internal Market Ideal: Essays in Honour of Stephen Weatherill* (Oxford University Press 2024)

Fink M, ‘Robo Swarms and Polygraphs: The Future of European Border Management and Its Costs’ (2 July 2024)

Fink M and Finck M, ‘Reasoned A(I)Dministration: Explanation Requirements in EU Law and the Automation of Public Administration’ (2022) 47 European Law Review 376

Fink M, Rauchegger C and De Coninck J, ‘The Action for Damages as a Fundamental Rights Remedy’ in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the ‘Complete System of Remedies’* (Cambridge University Press

2024)

Finocchiaro G, *Intelligenza Artificiale. Quali Regole?* (Il mulino 2024)

Floridi L, *Etica Dell'intelligenza Artificiale: Sviluppi, Opportunità, Sfide* (Raffaello Cortina Editore 2022)

——, 'AI as Agency Without Intelligence: On ChatGPT, Large Language Models, and Other Generative Models' (2023) 36 Philosophy & Technology 15

——, 'Present: AI as a New Form of Agency, Not Intelligence' in Luciano Floridi (ed), *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities* (Oxford University Press 2023) <

——, 'AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018) 28 Minds and Machines 689

——, 'capAI - A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act' (Social Science Research Network 2022) SSRN Scholarly Paper 4064091 <https://papers.ssrn.com/abstract=4064091> accessed 3 December 2024

Formici G, 'Sistemi Di Riconoscimento e Dati Biometrici: Una Nuova Sfida per i Legislatori e Le Corti.' (2019) 39 DPCE Online

Fosch-Villaronga E, Drukarch H and Giraudo M, 'A Legal Sustainability Approach to Align the Order of Rules and Actions in the Context of Digital Innovation', *Technology and Sustainable Development* (Routledge 2023)

FRA, 'Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement', 2019.

Frantziou E, '(Most of) the Charter of Fundamental Rights Is Horizontally Applicable: ECJ 6 November 2018, Joined Cases C-569/16 and C-570/16, Bauer et Al' (2019) 15 European Constitutional Law Review 306

——, '(Most of) the Charter of Fundamental Rights Is Horizontally Applicable: ECJ

6 November 2018, Joined Cases C-569/16 and C-570/16, Bauer et Al' (2019) 15 European Constitutional Law Review 306

——, 'The Horizontal Effect of the Charter: Towards an Understanding of Horizontality as a Structural Constitutional Principle' (2020) 22 Cambridge Yearbook of European Legal Studies 208

Friedman B and others, 'The Watcher and the Watched: Social Judgments About Privacy in a Public Place' (2006) 21 Human-Computer Interaction 235

Fussey P, Davies B and Innes M, '"Assisted" Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing' (2021) 61 The British Journal of Criminology 325

Fuster GG, 'Communication and Modalities for Exercising the Rights of the Data Subject' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

Fuster GG and Gellert R, 'The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right' [2012] International Review of Law, Computers & Technology

Gaito A, 'Riservatezza ed intercettazioni tra norma e prassi' (Aracne Editrice 2011)

Gallese C, 'The AI Act Proposal: A New Right to Technical Interpretability?' (arXiv, 14 March 2023)

Gallese Nobile C, 'Regulating Smart Robots and Artificial Intelligence in the European Union' (2024) 1 Journal of Digital Technologies and Law 33

Gardbaum S, 'The "Horizontal Effect" of Constitutional Rights' (2003) 102 Michigan Law Review 387

Garnelo M, Arulkumaran K and Shanahan M, ‘Towards Deep Symbolic Reinforcement Learning’ (arXiv, 1 October 2016)

Garnelo M and Shanahan M, ‘Reconciling Deep Learning with Symbolic Artificial Intelligence: Representing Objects and Relations’ (2019) 29 Current Opinion in Behavioral Sciences 17

Gellert R, ‘Risk and the Risk-Based Approach: Between Data Protection Risks and Compliance Risks’ in Raphaël Gellert (ed), *The Risk-Based Approach to Data Protection* (Oxford University Press 2020)

Gentile G, ‘Two Strings to One Bow? Article 47 of the EU Charter of Fundamental Rights in the EU Competition Case Law: Between Procedural and Substantive Fairness’ (2020) 4 Market and Competition Law Review 169

——, ‘Between Online and Offline Due Process: The Digital Services Act’ (24 August 2023) <https://papers.ssrn.com/abstract=4550655> accessed 3 December 2024

——, ‘Does Big Brother Exist?: Facial Recognition Technology in the United Kingdom’ in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Georgieva L and Kuner C, ‘Article 9 Processing of Special Categories of Personal Data’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Ghosh A and others, ‘Fundamental Concepts of Convolutional Neural Network’ in Valentina E Balas, Raghvendra Kumar and Rajshree Srivastava (eds), *Recent Trends and Advances in Artificial Intelligence and Internet of Things* (Springer International Publishing 2020)

Glasson J and Therivel R, *Introduction To Environmental Impact Assessment* (4th edn, Routledge 2013)

Gomez-Barrero M and others, ‘Biometrics in the Era of COVID-19: Challenges and Opportunities’ [2021] arXiv:2102.09258 [cs]

Gonzalez Fuster G, *The Essence of the Fundamental Right to Data Protection: Background Paper Commissioned by the European Data Protection Supervisor (EDPS)* (European Data Protection Supervisor (EDPS) 2023) <https://edps.europa.eu/data-protection/our-work/publications/other-documents/2023-11-08-study-essence-fundamental-rights-privacy-and-protection-personal-data_en> accessed 3 December 2024

González NM, ‘The Rights to Privacy and Data Protection and Facial Recognition Technology in the Global North’ in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023)

Gornet M and Maxwell W, ‘The European Approach to Regulating AI through Technical Standards’ (2024) 13 Internet Policy Review

Grabowska-Moroz B, ‘Data Retention in the European Union’ in Marek Zubik, Jan Podkowik and Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer International Publishing 2021)

Grafenstein M von, ‘Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I’ (2020) 6 European Data Protection Law Review 509

Graves L, Nagisetty V and Ganesh V, ‘Does AI Remember? Neural Networks and the Right to Be Forgotten’ <https://uwspace.uwaterloo.ca/handle/10012/15754> accessed 3 December 2024

Greer S, Slowe R and Gerards J, *Human Rights in the Council of Europe and the European Union: Achievements, Trends and Challenges* (Cambridge University Press 2018)

Griffin J, *On Human Rights* (OUP Oxford 2009)

——, ‘Human Rights: Questions of Aim and Approach’ (2010) 120 Ethics 741

Grimm D, ‘Conditions for the Emergence and Effectiveness of Modern Constitutionalism’ in Dieter Grimm (ed), *Constitutionalism: Past, Present, and Future* (Oxford University Press 2016)

Groppi T, *Menopeggio: La democrazia costituzionale nel XXI secolo / Tania Groppi.* (Società editrice il Mulino Spa 2020)

Grossi P, ‘Dignità umana e libertà nella Carta dei Diritti Fondamentali dell’Unione Europea’ in M Siclari (ed.), Contributi allo Studio della Carta dei Diritti Fondamentali dell’Unione Europea (Torino, G Giappichelli, 2003) 41–46.

Grozdanovski L, ‘In Search of Effectiveness and Fairness in Proving Algorithmic Discrimination in EU Law’ (2021) 58 Common Market Law Review

Gültekin-Várkonyi G, ‘Navigating Data Governance Risks: Facial Recognition in Law Enforcement under EU Legislation’ (2024) 13 Internet Policy Review

Gutman K, ‘The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?’ (2019) 20 German Law Journal 884

——, ‘The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?’ (2019) 20 German Law Journal 884

Gutwirth S and others, *Reinventing Data Protection?* (Springer Science & Business Media 2009)

Hacker P, ‘A Legal Framework for AI Training Data—from First Principles to the Artificial Intelligence Act’ (2021) 13 Law, Innovation and Technology 257

——, ‘Comments on the Final Trilogue Version of the AI Act’ (23 January 2024)

<https://papers.ssrn.com/abstract=4757603> accessed 3 December 2024

Han B-C, *Psychopolitics: Neoliberalism and New Technologies of Power* (Verso Books 2017)

Han X and Du Q, 'Research on Face Recognition Based on Deep Learning', *2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC)* (2018)

Hansen M, 'Data Protection Impact Assessment' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024) <https://doi.org/10.1093/law/9780192855220.003.0027> accessed 3 October 2024

Harnad S, 'The Symbol Grounding Problem' (1990) 42 Physica D: Nonlinear Phenomena 335

Hartzog W, 'Two AI Truths and a Lie' (2024) 26 Yale Journal of Law and Technology 595

Hartzog W and Richards N, 'Privacy's Constitutional Moment and the Limits of Data Protection' (2020) 61 Boston College Law Review 1687

Helberger N and Diakopoulos N, 'ChatGPT and the AI Act' (2023) 12 Internet Policy Review

Hert PD, 'Eu Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the Gdpr in the Spirit of Cooperative Federalism', *EU Law Enforcement* (Routledge 2021)

——, 'C4Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration. Topological Understandings of Twisted Boundary Setting in EU Data Protection Law' in Deirdre Curtin and Mariavittoria Catanzariti (eds), *Data at the*

Boundaries of European Law (Oxford University Press 2023)

Hert PD and Bouchagiar G, 'European Biometric Surveillance, Concrete Rules, and Uniform Enforcement: Beyond Regulatory Abstraction and Local Enforcement' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Hijmans H and Scirocco A, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help&#63'; (2009) 46 Common Market Law Review

Hildebrandt M, *Smart Technologies and the End (s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2015)

——, 'Algorithmic Regulation and the Rule of Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20170355

Hill K, 'The Secretive Company That Might End Privacy as We Know It' *The New York Times* (18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> accessed 3 December 2024

——, 'Wrongfully Accused by an Algorithm' *The New York Times* (3 August 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> accessed 3 December 2024

——, 'Clearview AI's Facial Recognition App Called Illegal in Canada' *The New York Times* (4 February 2021) <https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html> accessed 3 December 2024

——, '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 3 December 2024

Hof S van der and others, 'Articles 7 and 8 Fundamental Rights Charter and Article

16 TFEU – Commentary', *Concise European Data Protection, e-Commerce and IT Law* (Kluwer Law International 2018)

Hofmann A, 'The Role of National Courts in Redressing Fundamental Rights Violations by the EU' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU: The Promise of the 'Complete System of Remedies'* (Cambridge University Press 2024)

Houwing L, 'Reclaim Your Face and the Streets. Why Facial Recognition, and Other Biometric Surveillance Technology in Public Spaces, Should Be Banned' in Sven Quadflieg, Klaus Neuburg and Simon Nestler (eds), *(Dis)Obedience in Digital Societies: Perspectives on the Power of Algorithms and Data* (transcript Verlag 2022)

Hu M, 'Biometric Surveillance and Big Data Governance', *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017)

Hutson J and Winters B, 'America's next "Stop Model!" Model Deletion Essay' (2024) 8 Georgetown Law Technology Review 124

S generale della P della R-S sistemi, 'Messaggio di fine anno del Presidente della Repubblica Sergio Mattarella' (*Quirinale*)

Janssen H, Seng Ah Lee M and Singh J, 'Practical Fundamental Rights Impact Assessments' (2022) 30 International Journal of Law and Information Technology 200

——, 'Practical Fundamental Rights Impact Assessments' (2022) 30 International Journal of Law and Information Technology 200

Janssen HL, 'An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making' (2020) 10 International Data Privacy Law 76

Jasserand C, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data'' (Social Science Research Network, 1 June 2016)

<https://papers.ssrn.com/abstract=3230342> accessed 3 December 2024

——, ‘The Future AI Act and Facial Recognition Technologies in Public Spaces: Nice to Have or Strictly Necessary?’ (Social Science Research Network, 15 December 2023) <https://papers.ssrn.com/abstract=4947432> accessed 3 December 2024

——, ‘Biometric Data, Within and Beyond Data Protection’ in Bart Van der Sloot and Sascha van Schendel (eds), *The Boundaries of Data* (Amsterdam University Press 2024) <https://papers.ssrn.com/abstract=4483962> accessed 3 December 2024

——, ‘Article 10: Processing of Special Categories of Personal Data’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED)* (Oxford University Press 2024)

Jedličková A, ‘Ethical Approaches in Designing Autonomous and Intelligent Systems: A Comprehensive Survey towards Responsible Development’ [2024] AI & SOCIETY

jr AG, ‘The Contribution of Societal Constitutionalism to the Legal Theory of Digital Society: Framing and Perspectives’ [2024] Diritto pubblico

Kamara I, ‘Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation “Mandate”’ (2017) 8 European Journal of Law and Technology

Kaminski ME and Urban JM, ‘The Right to Contest Ai’ (2021) 121 Columbia Law Review 1957

Katrak M and Chakrabarty I, ‘Privacy, Political Participation, and Dissent: Facial Recognition Technologies and the Risk of Digital Authoritarianism in the Global South’ in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023)

——, ‘Privacy, Political Participation, and Dissent: Facial Recognition Technologies and the Risk of Digital Authoritarianism in the Global South’ in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023)

Kempeneer S, Ranchordas S and van de Wetering S, ‘AI FAILURE, AI SUCCESS, AND AI POWER DYNAMICS IN THE PUBLIC SECTOR’ (Social Science Research Network, 11 October 2024)

Kindt EJ, ‘A Legal Model for the Use of Biometric Data in the Private Sector’ in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013)

——, ‘Biometric Data, Data Protection and the Right to Privacy’ in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013)

——, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, vol 12 (Springer Netherlands 2013)

——, ‘The Criteria for the Correct “Balancing of Rights”’ in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013)

——, ‘The Need for a Consistent Legal Regulation of Biometric Data’ in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013)

——, ‘The Proportionality Principle as a General Principle of Law Applied to Biometric Data Processing’ in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013)

——, ‘The Risks Involved upon the Use of Biometric Data and Biometric Systems’ in Els J Kindt (ed), *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer Netherlands 2013)

Kissinger HA, Schmidt E and Huttenlocher D, *The Age of AI: And Our Human Future* (Hachette UK 2021)

Kohn M, ‘Clearview AI, TikTok, and the Collection of Facial Images in International Law Comments’ (2022) 23 Chicago Journal of International Law 195

Kolfschooten HV, ‘EU Regulation of Artificial Intelligence: Challenges for Patients’ Rights’ (2022) 59 Common market law review 81

Kosta E, ‘Article 35 Data Protection Impact Assessment’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights’ (2022) 16 Regulation & Governance 212

——, ‘Chapter 3: A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon’ (2022)

Kosta V, ‘Fundamental Rights Mainstreaming in the EU’, *The EU and the Proliferation of Integration Principles under the Lisbon Treaty* (Routledge 2014)

Kostka G, Steinacker L and Meckel M, ‘Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States’ [2021] Public Understanding of Science 09636625211001555

——, ‘Between Security and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the United Kingdom, and the United States’ (2021) 30 Public Understanding of Science 671

Kranenborg H, ‘Article 17 Right to Erasure (“Right to Be Forgotten”)’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

——, ‘Right to an Effective Judicial Remedy against a Supervisory Authority’ in Eleni

Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

——, ‘Right to Lodge a Complaint with a Supervisory Authority’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024)

Kuhlmann S, ‘Government Use of Facial Recognition Technologies under European

Law' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Kuru T, 'C-205/21 VS v Ministerstvo Na Vatreshnite Raboti, Glavna Direktsia Za Borba s Organiziranata Prestapnost: Indiscriminate and Generalised Collection of Biometric and Genetic Data by Law Enforcement Authorities in the EU Is Not Allowed' (2024) 10 European Data Protection Law Review 223

——, 'Lawfulness of the Mass Processing of Publicly Accessible Online Data to Train Large Language Models' [2024] International Data Privacy Law ipae013

Lagioia F, Rovatti R and Sartor G, 'Algorithmic Fairness through Group Parities? The Case of COMPAS-SAPMOC' (2023) 38 AI & SOCIETY 459

Lagioia F and Sartor G, 'Artificial Intelligence in the Big Data Era: Risks and Opportunities', *Legal Challenges of Big Data* (Edward Elgar Publishing 2020)

Lala F, 'Data Collection via Web Scraping: Privacy and Facial Recognition after Clearview' (2023) 16 i-lex 34

Landerer LM, 'Data Retention' [2024] Verfassungsblog <https://verfassungsblog.de/data-retention/> accessed 3 December 2024

Lasagni G, 'Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the "Data Retention Saga"' (GBR 2024)

Lattanzi U, 'The Inapplicability of the Bosphorus Presumption to the European Economic Area Agreement: A Risk for the Coherence of Legal Systems in Europe' (2023) 19 European Constitutional Law Review 441

Laux J, Wachter S and Mittelstadt B, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk' (2024) 18 Regulation & Governance 3

LeCun Y, Bengio Y and Hinton G, 'Deep Learning' (2015) 521 Nature 436

Leczykiewicz D, 'Horizontal Application of the Charter of Fundamental Rights' (Social Science Research Network, 19 September 2013)

Leiser M and Custers B, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 European data protection law review (Internet) 367

——, 'Time Limits for Storage and Review' in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024) <https://doi.org/10.1093/law/9780192855220.003.0005> accessed 31 October 2024

Leiser MR, '"Private Jurisprudence" and the Right to Be Forgotten Balancing Test' (2020) 39 Computer Law & Security Review 105458

Leiser MR and Dechesne F, 'Governing Machine-Learning Models: Challenging the Personal Data Presumption' (2020) 10 International Data Privacy Law 187

Lenaerts K, 'Upholding the Rule of Law through Judicial Dialogue' (2019) 38 Yearbook of European Law 3

——, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779

Lenaerts K and Gutman K, 'The Comparative Law Method and the Court of Justice of the European Union: Interlocking Legal Orders Revisited' in Mads Andenas and Duncan Fairgrieve (eds), *Courts and Comparative Law* (Oxford University Press 2015)

Lenaerts K, Gutman K and Nowak JT, 'Union Law and National Procedures and Remedies' in Koen Lenaerts, Kathleen Gutman and Janek Tomasz Nowak (eds), *EU Procedural Law* (Oxford University Press 2023)

Lenaerts K, Van Nuffel P and Corthaut T, 'Fundamental Rights and General Principles of Union Law' in Koen Lenaerts, Piet Van Nuffel and Tim Corthaut (eds), *EU Constitutional Law* (Oxford University Press 2021)

Leo FD, 'Vecchio e nuovo in materia di intercettazioni telefoniche riguardanti reati

non previsti nel decreto di autorizzazione ("Nota" a Cass. 23 giugno 1986, Frisina)' (1989) 112 Il foro italiano II

Leonelli S, 'What Distinguishes Data from Models?' (2019) 9 European Journal for Philosophy of Science 22

Levantino FP, 'Generative and AI-Powered Oracles: "What Will They Say about You?"' (2023) 51 Computer Law & Security Review 105898

——, '"How Do You Feel Today?" Exploring IHRL and IHL Perspectives on Law Enforcement and Military Uses of Emotion Recognition Technology' (*Opinio Juris*, 15 November 2023) <https://opiniojuris.org/2023/11/15/how-do-you-feel-today-exploring-ihrl-and-ihl-perspectives-on-law-enforcement-and-military-uses-of-emotion-recognition-technology/> accessed 3 December 2024

Levantino FP and Paolucci F, 'Advancing the Protection of Fundamental Rights Through AI Regulation: How the EU and the Council of Europe Are Shaping the Future' (27 June 2024) <https://papers.ssrn.com/abstract=4881656> 3 December 2024

Li SZ, Jain AK and Deng J (eds), *Handbook of Face Recognition* (Springer International Publishing 2024)

Li TC, 'Algorithmic Destruction' (Social Science Research Network 2022) SSRN Scholarly Paper 4066845 <https://papers.ssrn.com/abstract=4066845> accessed 3 December 2024

Liu Z and others, 'Generative Networks' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024)

'Lo Stato', in Roberto Bin, *Diritto costituzionale / Roberto Bin, Giovanni Pitruzzella* (Ventitreesima edizione, G Giappichelli 2022)

Lock T and Martin D, 'Article 47 CFR' in Manuel Kellerbauer, Marcus Klamert and

Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019)

Locke J, *Due trattati sul governo e altri scritti politici / di J. Locke. Patriarca / di R. Filmer ; a cura di L. Pareyson* (3. ed. accresciuta, UTET 1982)

Lodder AR, 'Algorithms: What, How, and Particularly Why?' (Social Science Research Network 2019)

Loewenthal P-J, 'Article 291 TFEU' in Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019)

Loideain NN, 'Lawfulness and Police Use of Facial Recognition in the United Kingdom: Article 8 ECHR and Bridges v. South Wales Police' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Lomborg S, Kaun A and Scott Hansen S, 'Automated Decision-Making: Toward a People-Centred Approach' (2023) 17 Sociology Compass e13097

Longo E, 'The Risks of Social Media Platforms for Democracy: A Call for a New Regulation' in Bart Custers and Eduard Fosch-Villaronga (eds), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice* (TMC Asser Press 2022)

——, 'La "Giustizia Digitale" Tra Nuove Forme Di Efficienza e Garanzia Dei Diritti Costituzionali' (2023) 4 La Nuova Giuridica 187

Longo E, 'Predizione, Profilazione e Giustizia: Le Prospettive Costituzionali', Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche (Edizioni Scientifiche Italiane 2022)

——, Giustizia Digitale e Costituzione: Riflessioni Sulla Trasformazione Tecnica Della Funzione Giurisdizionale (FrancoAngeli 2023)

——, 'Audizione informale per il disegno di legge in materia di «Disposizioni in

materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)'.

Longo E and Pin A, 'Oltre Il Costituzionalismo? Nuovi Principi e Regole Costituzionali per l'era Digitale' [2023] Diritto pubblico comparato ed europeo

Luciano Floridi, 'Passato: L'origine Dell'intelligenza Artificiale', *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide* (Raffaello Cortina Editore 2022)

Lynskey O, *The Foundations of EU Data Protection Law / Orla Lynskey* (University Press 2015)

——, 'The "Europeanisation" of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies 252

——, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 International Journal of Law in Context 162

——, 'Article 8: The Right to Data Protection', *The EU Charter of Fundamental Rights in the Member States* (Hart Publishing 2020)

Lyon D, *The Culture of Surveillance: Watching as a Way of Life* (Kindle, Wiley 2018)

Mackenzie-Gray Scott R and Abrusci E, 'Automated Decision-Making and the Challenge of Implementing Existing Laws' [2023] Verfassungsblog

Madiega T and Mildebrath H, 'Regulating Facial Recognition in the EU' (EPRS | European Parliamentary Research Service 2021)

Malgieri G, *Vulnerability and Data Protection Law* (Oxford University Press 2023)

Malgieri G and Comandé G, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 243

Malgieri G and De Hert P, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not

Necessarily by Judges' in David Gray and Stephen E Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017)

Malgieri G and Santos C, 'Assessing the (Severity of) Impacts on Fundamental Rights' (Social Science Research Network, 25 June 2024) <https://papers.ssrn.com/abstract=4875937> accessed 3 December 2024

Mann M and Smith M, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight' (2017) 40 University of New South Wales Law Journal 121

Mantelero A, 'Human Rights Impact Assessment and AI' in Alessandro Mantelero (ed), *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (TMC Asser Press 2022)

——, 'Regulating AI' in Alessandro Mantelero (ed), *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (TMC Asser Press 2022)

——, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template'

——, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, Legal Obligations and Key Elements for a Model Template' (2024) 54 Computer Law & Security Review 106020

Mantelero A and Esposito MS, 'An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems' (2021) 41 Computer Law & Security Review 105561

Marco Bassini, *Internet e Libertà Di Espressione. Prospettive Costituzionali e Sovranazionali* (Aracne 2019)

Marelli M (ed), 'Data Protection Impact Assessments (DPIAs)', *Handbook on Data Protection in Humanitarian Action* (3rd edn, Cambridge University Press 2024)

Marinucci G and Dolcini E, *Manuale Di Diritto Penale: Parte Generale* (Giuffrè

editore 2012)

Martinico G, ‘Art. 7. Rispetto Della Vita Privata e Della Vita Familiare’, *Carta dei Diritti Fondamentali dell’Unione Europea* (Giuffrè, 2017)

——, *The Tangled Complexity of the EU Constitutional Process: The Frustrating Knot of Europe* (Routledge 2022)

Martinico G and Pollicino O, *The Interaction Between Europe’s Legal Systems: Judicial Dialogue and the Creation of Supranational Laws* (Edward Elgar 2012)

Mattu JA Jeff Larson,Lauren Kirchner,Surya, ‘Machine Bias’ (*ProPublica*)

Mauer M, ‘The Unbearable Lightness of Interfering with the Right to Privacy’ [2024] Verfassungsblog <https://verfassungsblog.de/the-unbearable-lightness-of-interfering-with-the-right-to-privacy/> accessed 3 December 2024

Mazur J and Choińska Z, ‘Chapter 7: European Union Data Protection Law and the Use of Facial Recognition Technology for the Purpose of Fighting Crime’ Elgar (2024)

Mazzini G and Scalzo S, ‘The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts’ (2 May 2022) <https://papers.ssrn.com/abstract=4098809> accessed 3 December 2024

McCarthy J, ‘What Is Artificial Intelligence?’ [2007] Formal Stanford

——, ‘A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955’ (2006) 27 AI Magazine 12

McClellan E, ‘Facial Recognition Technology: Balancing the Benefits and Concerns’ (2020) 15 Journal of Business & Technology Law 363

——, ‘Facial Recognition Technology: Balancing the Benefits and Concerns’ Journal of Business 19

McMullan T, ‘What Does the Panopticon Mean in the Age of Digital Surveillance?’ *The Guardian* (23 July 2015) <https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham> accessed 3 December 2024

Menéndez González N, *The Impact of Facial Recognition Technology Empowered by Artificial Intelligence on the Right to Privacy* (Routledge 2022)

Metikos L, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188

——, 'Explaining and Contesting Judicial Profiling Systems' (2024) 2024 Technology and Regulation 188

Metikoš L and Ausloos J, 'The Right to an Explanation in Practice: Insights from Case Law for the GDPR and the AI Act' (Social Science Research Network, 6 August 2024) <https://papers.ssrn.com/abstract=4996173> accessed 3 December 2024

Meuwese ACM, *Impact Assessment in EU Lawmaking*, vol 61 (1st edn, Wolters Kluwer Law & Business 2008)

Miklaszewicz P and Safjan M, 'Horizontal Effect of the General Principles of EU Law in the Sphere of Private Law' (2010) 18 European Review of Private Law 475

Minsky ML, 'Logical Versus Analogical or Symbolic Versus Connectionist or Neat Versus Scruffy' (1991) 12 AI Magazine 34

Mirkine–Guetzevich B and Cotta S, 'I Metodi Di Studio Del Diritto Costituzionale Comparato' (1951) 16 Il Politico 181

Mittelstadt BD and others, 'The Ethics of Algorithms: Mapping the Debate' (2016) 3 Big Data & Society 2053951716679679

Mobilio G, *Tecnologie di riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative* (ITA 2021)

——, 'L'uso delle tecnologie di riconoscimento facciale da parte delle forze dell'ordine: bandire o non bandire?'

——, 'L'uso delle tecnologie di riconoscimento facciale da parte delle forze

dell'ordine: bandire o non bandire?' (La democrazia della società digitale Tensioni e opportunità Atti del Convegno 3 dicembre 2021 Università di Milano-Bicocca 2023)

——, 'Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies' (2023) 12 Internet Policy Review

——, 'La Corte EDU Condanna Il Ricorso Alle Tecnologie Di Riconoscimento Facciale per Reprimere Il Dissenso Politico: Osservazioni a Partire Dal Caso Glukhin c. Russia' [2024] DPCE ONLINE 695

Moerel L and Storm M, 'Do LLMs "store" Personal Data? This Is Asking the Wrong Question' <https://iapp.org/news/a/do-llms-store-personal-data-this-is-asking-the-wrong-question> accessed 3 December 2024

Morbidelli G, 'La Costituzione' in Lucio Pegoraro and others, *Diritto pubblico comparato* (G Giappichelli Editore 2016)

Morelli A and Pollicino O, 'Metaphors, Judicial Frames, and Fundamental Rights in Cyberspace' (2020) 68 The American Journal of Comparative Law 616

Mourby M and Mackey E, '14. Identity, Profiles and Pseudonyms in the Digital Environment' in Bart Sloot and Sascha Schendel (eds), *The Boundaries of Data* (Amsterdam University Press 2024)

Murray D, 'Facial Recognition and the End of Human Rights as We Know Them?' (2024) 42 Netherlands Quarterly of Human Rights 145

Murray D and Fussey P, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 Israel Law Review 31

Mustert L, 'The EDPB's Second Article 65 Decision - Is the Board Stepping up Its Game? Reports: European Union' (2021) 7 European Data Protection Law Review (EDPL) 416

Nardocci C, ‘Il riconoscimento facciale sul “banco” degli imputati. Riflessioni a partire, e oltre, Corte EDU Glukhin c. Russia’ [2024] BioLaw Journal - Rivista di BioDiritto 279

Nemitz P, ‘Constitutional Democracy and Technology in the Age of Artificial Intelligence’ (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180089

Nikolinakos NT, *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies - The AI Act / by Nikos Th. Nikolinakos.* (1st ed. 2023., Springer International Publishing 2023)

Noble SU, ‘Algorithms of Oppression’, *Algorithms of Oppression* (New York University Press 2018)

Novelli C and others, ‘A Robust Governance for the Ai Act: Ai Office, Ai Board, Scientific Panel, and National Authorities’ (2024) 4 European Journal of Risk Regulation 1

Olsen HP and others, ‘What’s in the Box? The Legal Requirement of Explainability in Computationally Aided Decision-Making in Public Administration’ (Social Science Research Network 2019)

Oreste Pollicino and Giovanni De Gregorio, ‘Constitutional Law in the Algorithmic Society’, *Constitutional Challenges in the Algorithmic Society* (Edited by Hans-W Micklitz, Oreste Pollicino, Amnon Reichman, Andrea Simoncini, Giovanni Sartor and Giovanni De Gregorio, Cambridge University Press 2021)

Pagallo U and Durante M, ‘Human Rights and the Right to Be Forgotten’, *Human Rights, Digital Society and the Law* (Routledge 2019)

Palmiotto F, ‘Preserving Procedural Fairness in The AI Era: The Role of Courts Before

and After the AI Act' [2023] Verfassungsblog <https://verfassungsblog.de/procedural-fairness-ai/> accessed 3 December 2024

——, 'When Is a Decision Automated? A Taxonomy for a Fundamental Rights Analysis' (2024) 25 German Law Journal 210

——, 'The AI Act Roller Coaster: How Fundamental Rights Protection Evolved in the EU Legislative Process' (4 June 2024) <https://papers.ssrn.com/abstract=4904179> accessed 3 December 2024

——, 'Op-Ed: "Is Predictive Policing Prohibited in the EU? Yes, It Should Be"' (*EU Law Live*, 19 December 2024) <https://eulawlive.com/op-ed-is-predictive-policing-prohibited-in-the-eu-yes-it-should-be/> accessed 3 December 2024

Palmiotto F and González NM, 'Facial Recognition Technology, Democracy and Human Rights' (2023) 50 Computer Law & Security Review 105857

Pannacciulli C, 'Profili costituzionali delle intercettazioni di comunicazioni tra inadeguatezza del legislatore e discrezionalità del giudice' [2012] Rivista AIC

Paolucci F, 'Riconoscimento Facciale e Diritti Fondamentali: È La Sorveglianza Un Giusto Prezzo Da Pagare?' [2021] MediaLaws - Rivista di Diritto dei Media

——, 'Due Process of Artificial Intelligence: A Challenge for the Protection of Fundamental Rights', *Digital Single Market and Artificial Intelligence* (Aracne 2024)

——, 'Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights' [2024] Verfassungsblog <https://verfassungsblog.de/shortcomings-of-the-ai-act/> accessed 3 December 2024

——, 'From Global Standards to Local Safeguards: The AI Act, Biometrics, and Fundamental Rights' (1 August 2024) <https://papers.ssrn.com/abstract=4929132> accessed 3 December 2024

Paolucci Federica, 'Verso una normalizzazione della sorveglianza di massa? Big Brothers Watch c. Regno Unito, ultimo atto' [2021] Quaderni costituzionali 981

Parrish R, 'Case C-36/74 Walrave and Koch [1974] ECR 1405' in Jack Anderson (ed), *Leading Cases in Sports Law* (Springer 2013)

Pasquale F, ‘Watching (and Improving) the Watchers’, *The black box society. The secret algorithms that control money and information.* (Harvard University Press 2015)

——, ‘A Rule of Persons, Not Machines: The Limits of Legal Automation’ (2019) 87 George Washington Law Review 1

——, ‘Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication’ in Amnon Reichman and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021)

Peers S and others, ‘Article 47’, *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2021)

Pernice I, ‘Multilevel Constitutionalism in the European Union’ (2002) 27 European law review 511

——, ‘The Treaty of Lisbon and Fundamental Rights’ in Stefan Griller and Jacques Ziller (eds), *The Lisbon Treaty: EU Constitutionalism without a Constitutional Treaty?* (Springer 2008)

——, ‘Multilevel Constitutionalism and the Crisis of Democracy in Europe’ (2015) 11 European Constitutional Law Review 541

Petkova B, ‘Privacy as Europe’s First Amendment’ (2019) 25 European Law Journal 140

Pin A and Scaffardi L, ‘Tra Protezione Dei Dati e Intelligenza Artificiale, in Europa e Oltre’ (2024) 64 DPCE Online

Pinelli C, ‘Legal Certainty and the Tasks of Jurists’ [2019] Diritto pubblico

Pollicino O, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Bloomsbury Publishing 2021)

——, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Bloomsbury Publishing 2021)

——, ‘“Getting the Future Right – Artificial Intelligence and Fundamental Rights”. A

view from the European Union Agency for Fundamental Rights' [2021] BioLaw Journal - Rivista di BioDiritto 7

——, 'The Transatlantic Dimension of the Judicial Protection of Fundamental Rights Online'

——, 'Asimmetrie Valoriali Transatlantiche Tra Self-Regulation, Hard Law e Co-Regolazione (Ovvero Sul Se e Sul Come Regolamentare Le Strategie Contro La Disinformazione on Line)' [2023] Osservatorio sulle Fonti

——, 'Potere Digitale' in Marta Cartabia and Marco Ruotolo (eds), *Potere e Costituzione. Enciclopedia del diritto: i tematici* (Treccani 2023)

——, 'The Quadrangular Shape of the Geometry of Digital Power(s) and the Move towards a Procedural Digital Constitutionalism' (2023) 29 European Law Journal <https://onlinelibrary.wiley.com/doi/abs/10.1111/eulj.12472> accessed 21 August 2023

——, 'L'efficacia Orizzontale Dei Diritti Fondamentali Previsti Dalla Carta La Giurisprudenza Della Corte Di Giustizia in Materia Di Digital Privacy Come Osservatorio Privilegiato' [2024] Rivista di Diritto dei Media - MediaLaws 1

——, 'Regolare l'Intelligenza Artificiale: La Lunga via Dei Diritti Fondamentali' in Oreste Pollicino and others (eds), *La disciplina dell'intelligenza artificiale* (Giuffrè Editore)

—— (eds), *La Disciplina Dell'intelligenza Artificiale* (Giuffrè Editore 2025)

——, 'Regolazione e Innovazione Tecnologica Nell'"ordinamento Della Rete"' [2025] Rivista AIC 1

Pollicino O and Bassini M, 'Art. 8. Protezione Dei Dati Di Carattere Personale', *Carta dei Diritti Fondamentali dell'Unione Europea* (Giuffrè 2017)

Pollicino O and Dunn P, 'Disinformazione e Intelligenza Artificiale Nell'anno Delle Global Elections: Rischi (Ed Opportunità)' (2024) 12 FEDERALISMI. IT IV

——, 'IA e Valori Democratici' in Oreste Pollicino and Pietro Dunn, *Intelligenza Artificiale e Disinformazione* (Egea 2024)

——, *Intelligenza Artificiale e Disinformazione* (Egea 2024)

Pollicino O and Giuseppe Martinico, 'Between Constitutional Tolerance and Judicial Activism: The "Specificity" of the European Judicial Law'

Post R, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten,

and the Construction of the Public Sphere' [2017] SSRN Electronic Journal <http://www.ssrn.com/abstract=2953468> accessed 3 December 2024

Priya A, 'Case Study Methodology of Qualitative Research: Key Attributes and Navigating the Conundrums in Its Application' (2021) 70 Sociological Bulletin 94

Puri A, 'The Group Right to Mutual Privacy' (2023) 2 Digital Society 22

Purtova N, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40

——, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' (2018) 8 International Data Privacy Law 52

Purtova N and Leenes R, 'Code as Personal Data: Implications for Data Protection Law and Regulation of Algorithms' (2023) 13 International Data Privacy Law 245

Quattrocolo S, 'Approaching the Unknown: Some Preliminary Words' in Serena Quattrocolo (ed), *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion* (Springer International Publishing 2020)

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502

Quinn P and Malgieri G, 'The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework' (2021) 22 German Law Journal 1583

Quintel T, 'The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation: The Question of Legitimizing Unlawful Practices Reports: European Union' (2022) 8 European Data Protection Law Review (EDPL) 90

Quintel T and Mitsilegas V, ‘Distinction between Different Categories of Data Subject’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press 2024) <

Raab CD, ‘Information Privacy, Impact Assessment, and the Place of Ethics∗’ (2020) 37 Computer Law & Security Review 105404

Ragazzi FPSM and others, ‘Biometric and Behavioural Mass Surveillance in EU Member States: Report for the Greens/EFA in the European Parliament’ (Greens/EFA 2021)

Ranchordás S, ‘The Invisible Citizen in the Digital State: Administrative Law Meets Digital Constitutionalism’ in J De Poorter, C Oirsouw and G van der Schyff (eds), *European yearbook of constitutional law* (2024)

Ranchordas S and Beck M, ‘Vulnerability in Kaufmann, Mareile and Lomell, Heidi Mork (Eds) Handbook of Digital Criminology. De Gruyter, Forthcoming’ (9 October 2023)

Reempts FV, ‘The Court of Justice of the EU and the Philosopher’s Stone: The Independent Horizontal Direct Effect of Article 47 of the Charter in K.L. v X: ECJ 22 March 2024, Case C-715/20, X (Absence de Motifs de Résiliation)’ (2024) 20 European Constitutional Law Review 482

Renda A, ‘From Impact Assessment to the Policy Cycle: Drawing Lessons from the EU’s Better-Regulation Agenda’ (2016) 9 SPP Technical Papers

Renda et al., ‘Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe’, April 2021

Renzetti S, ‘Qualcosa è Cambiato : Vecchio e Nuovo in Tema Di Intercettazioni’ [2024] Jus : rivista di scienze giuridiche : LXXI, 1, 2024 141

Repetto G, ‘The Constitutional Relevance of the ECHR in Domestic and European Law’ [2013] Intersentia, Cambridge-Antwerp-Portland

Ribeiro G de A, ‘The Effects of Fundamental Rights in Private Disputes’ in Hugh Collins (ed), *European Contract Law and the Charter of Fundamental Rights*, vol 2 (Intersentia 2017)

Richards NM, ‘The Dangers of Surveillance’ (2013) 126 Harvard Law Review 1934

Riva GM, ‘Diritto e Intelligenza Artificiale Generativa : L’istruttoria Del Garante per La Protezione Dei Dati Italiano Su OpenAI e ChatGPT’ [2024] Ciberspazio e diritto : rivista internazionale di informatica giuridica : 25, 1, 2024 153

Rodotà S, ‘Data Protection as a Fundamental Right’ in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer Netherlands 2009)

Rodríguez de las Heras Ballell T, ‘Guiding Principles for Automated Decision-Making in the EU’ (2022) ELI Innovation Paper 28

Rodríguez-Doncel V and others, ‘Introduction: A Hybrid Regulatory Framework and Technical Architecture for a Human-Centered and Explainable AI’ in Víctor Rodríguez-Doncel and others (eds), *AI Approaches to the Complexity of Legal Systems XI-XII* (Springer International Publishing 2021)

Rojszczak M, ‘Data Retention in the Light of Copyright Infringements: Protecting the Status Quo or Seeking a Third Way? (Case C-470/21 La Quadrature Du Net II)’ [2024] Maastricht Journal of European and Comparative Law 1023263X241287402

Rosas A, ‘The Court of Justice of the European Union: A Human Rights Institution?’ (2022) 14 Journal of Human Rights Practice 204

Rossignaud MP and De Kerckhove D, *Oltre Orwell. Il Gemello Digitale.* (Castelvecchi 2020)

Ruggeri A, 'Carte Internazionali Dei Diritti, Costituzione Europea, Costituzione Nazionale: Prospettive Di Ricomposizione Delle Fonti in Sistema' (2007)

Ruotolo M, 'La Sicurezza Nel Gioco Del Bilanciamento' (2009) 49 Astrid rassegna

——, 'Appunti Sulla Dignità Umana' (2010) 4 Direitos Fundamentais & Justiça 123

Russell S and Norvig P, *Artificial Intelligence: A Modern Approach* (4th US ed, Pearson Education 2021)

Sartor G, *L'intelligenza artificiale e il diritto* (Giappichelli 2022)

Scarpino D, 'Intercettazioni e Delitti Di "Criminalità Organizzata" Tra Vecchi Problemi e Nuove Soluzioni' (2024) 64 Cassazione penale 1657

Schabas W and United Nations General Assembly, *The Universal Declaration of Human Rights: The Travaux Préparatoires / [Edited by] William A. Schabas, OC MRIA.* (1st ed., University Press 2013)

Schabas WA, 'Right to Respect for Private and Family Life/Droit Au Respect de La Vie Privée et Familiale' in William A Schabas (ed), *The European Convention on Human Rights: A Commentary* (Oxford University Press 2015)

Scheppele KL, Kochenov DV and Grabowska-Moroz B, 'EU Values Are Law, after All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union' (2020) 39 Yearbook of European Law 3

Schuett J, 'Risk Management in the Artificial Intelligence Act' (2024) 15 European Journal of Risk Regulation 367

Schuilenburg M and Peeters R, *The Algorithmic Society: Technology, Power, and Knowledge* (Routledge 2020)

Schütz P, 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective' in Jan Camenisch and others (eds), *Privacy and Identity Management for Life* (Springer 2012)

Schütze R, '"Delegated" Legislation in the (New) European Union: A Constitutional Analysis' (2011) 74 The Modern Law Review 661

Selwyn N and others, 'Facial Recognition Technology: Key Issues and Emerging Concerns' in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Shepley AJ, 'Deep Learning For Face Recognition: A Critical Analysis' [2019] arXiv:1907.12739 [cs]

Shi Y and Jain AK, 'Uncertainty-Aware Face Recognition' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024)

Shipley DE, 'Due Process Rights before EU Agencies: The Rights of Defense' (2008) 37 Georgia Journal of International and Comparative Law 1

Simoncini A, 'L'algoritmo Incostituzionale: Intelligenza Artificiale e Il Futuro Delle Libertà' (2019) 15 BioLaw Journal-Rivista di BioDiritto 63

Simoncini A and Longo E, 'Fundamental Rights and the Rule of Law in the Algorithmic Society' in Hans-W Micklitz and others (eds), *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press 2021)

Simoncini A and Suweis S, 'Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale' [2019] Rivista di filosofia del diritto 87

Simonelli F and Iacob N, ‘Can We Better the European Union Better Regulation Agenda?’ (2021) 12 European Journal of Risk Regulation 849

Singer R and Goodyear M, ‘FTC Orders Destruction of Algorithms Created From Unlawfully Acquired Data’ (2021) 4 The Journal of Robotics, Artificial Intelligence & Law 11

Sloot B van der, ‘The Right to Be Let Alone by Oneself: Narrative and Identity in a Data-Driven Environment’ (2021) 13 Law, Innovation and Technology 223

Slosser JL, ‘Interpreting the “Quality of Law” at the European Court of Human Rights: Metaphorical Framing and Evaluative Judgment’ (18 September 2018) <https://papers.ssrn.com/abstract=3251277> accessed 3 December 2024

Smuha NA, ‘The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence’ (2019) 20 Computer Law Review International 97

——, ‘From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence’ (2021) 13 Law, Innovation and Technology 57

Smuha NA and Yeung K, ‘The European Union’s AI Act: Beyond Motherhood and Apple Pie?’ (24 June 2024) <https://papers.ssrn.com/abstract=4874852> accessed 3 December 2024

Sobel B, ‘HiQ v. LinkedIn, Clearview AI, and a New Common Law of Web Scraping’ [2020] LinkedIn, Clearview AI, and a New Common Law of Web Scraping (April 21, 2020)

Soori M, Arezoo B and Dastres R, ‘Artificial Intelligence, Machine Learning and Deep Learning in Advanced Robotics, a Review’ (2023) 3 Cognitive Robotics 54

Spaventa E, ‘The Horizontal Application of Fundamental Rights as General Principles of Union Law’ (Hart Publishing 2011)

——, ‘Should We Harmonize Fundamental Rights in the EU? Some Reflections about

Minimum Standards and Fundamental Rights Protection in the EU Composite Constitutional System' (2018) 55 Common Market Law Review

——, 'Fundamental Rights in the European Union' (Oxford University Press 2020)

Stella M, 'La tutela giurisdizionale effettiva nel diritto processuale civile' (Giuffré 2017)

Stocker O, 'Le Second Arret Defrenne. L'égalité de Rétribution Des Travailleurs Masculins e Des Travailleurs Féminin' [1977] Cahier de dr. Eur 180

Suh JJ and Metzger MJ, 'Privacy Beyond the Individual Level' in Bart P Knijnenburg and others (eds), *Modern Socio-Technical Perspectives on Privacy* (Springer International Publishing 2022)

Sumer B and others, 'AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data' in Kostina Prifti and others (eds), *Digital Governance: Confronting the Challenges Posed by Artificial Intelligence* (TMC Asser Press 2024)

Susi M, 'European Convention on Human Rights - Freedom of Expression - Right to Privacy - Responsibility of Internet News Portal for Defamatory Comments Posted by Readers' (2014) 108 The American journal of international law 295

Swan B, 'Facial-Recognition Company That Works With Law Enforcement Says Entire Client List Was Stolen' *The Daily Beast* (26 February 2020)

Szpunar M, 'New Technologies in the Case Law of the Court of Justice – Lessons Learnt and Lessons to Be Learnt' [2024] ERA Forum

Tan Z and Guo G, 'Face Recognition Research and Development' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024) <

Tarchi R and Gatti A, ‘Intelligenza Artificiale e Protezione Dei Dati Personali: Problemi Di Metodo e Di Procedura’ (2024) 64 DPCE Online

——, ‘Intelligenza Artificiale e Protezione Dei Dati Personali: Problemi Di Metodo e Di Procedura’ (2024) 64 DPCE Online

Teubner G, *Constitutional Fragments: Societal Constitutionalism and Globalization* (1st edn, OUP Oxford 2012)

——, ‘Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution Essays’ (2017) 3 Italian Law Journal 193

——, ‘Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?’, *Luhmann and Law* (Routledge 2017)

Thelisson E and Verma H, ‘Conformity Assessment under the EU AI Act General Approach’ (2024) 4 AI and Ethics 113

‘They Will Be Understood as the Assessment of Both the Potential Human Rights Impact of Future Policies and the Actual Hu’

Trapova A, ‘From Public to Private Enforcement – Inclusivity and Copyright Law’ (Social Science Research Network, 2 August 2023) <https://papers.ssrn.com/abstract=4589884> accessed 3 December 2024

Tridimas T, ‘The Rights of Defence’ in Takis Tridimas (ed), *The General Principles of EU Law* (Oxford University Press 2006)

Tridimas T and Gentile G, ‘The Essence of Rights: An Unreliable Boundary?’ (2019) 20 German Law Journal 794

Turing AM, ‘Intelligenza Meccanica, a Cura Di G’ [1994] Lolli, Boringhieri, Torino

Tushnet M, ‘The Issue of State Action/Horizontal Effect in Comparative Constitutional Law’ (2003) 1 International Journal of Constitutional Law 79

Tzanou M, ‘The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection’

——, *The Fundamental Right to Data Protection : Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017)

——, ‘Article 8 LED. Lawfulness of Processing’ in Eleni Kosta and Franziska Boehm (eds), *The EU Law Enfocemente Directive (LED): a commentary* (Oxford University Press 2024)

Tzanou M and Karyda S, ‘*Privacy International and Quadrature Du Net:* One Step Forward Two Steps Back in the Data Retention Saga?’ (2022) 28 European Public Law

Ünver A, ‘Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights | Think Tank | European Parliament’ (European Parliament)

Vacca JR, *Biometric Technologies and Verification Systems* (2007) systems/vacca/978-

Van Cleynenbreugel P, ‘The Commission’s Digital Services and Markets Act Proposals: First Step towards Tougher and More Directly Enforced EU Rules?’ (2021) 28 Maastricht Journal of European and Comparative Law 667

van der Heijden J, ‘Risk as an Approach to Regulatory Governance: An Evidence Synthesis and Research Agenda’ (2021) 11 Sage Open 21582440211032202

van der Sloot B, ‘Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data’ (2014) 5 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 230

——, ‘Do Groups Have a Right to Protect Their Group Interest in Privacy and Should They? Peeling the Onion of Rights and Interests Protected under Article 8 ECHR’ [2017] Group privacy: new challenges of data technologies 197

——, ‘Legal Fundamentalism: Is Data Protection Really a Fundamental Right?’, *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer International

Publishing 2017)

——, ‘The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases’ (2020) 11 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 160

——, ‘The Production of and Control over Data in the AI-Era: The Two Failing Approaches to Privacy Protection’ in Alberto Quintavalla and Jeroen Temperman (eds), *Artificial intelligence and human rights* (Oxford University Press 2023)

Van der Sloot B and Kosta E, ‘Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance’ (2019) 5 Eur. Data Prot. L. Rev. 252

van der Sloot B and van Schendel S, ‘Procedural Law for the Data-Driven Society’ (2021) 30 Information & Communications Technology Law 304

van Schendel S, ‘The Challenges of Risk Profiling Used by Law Enforcement: Examining the Cases of COMPAS and SyRI’ in Leonie Reins (ed), *Regulating new technologies in uncertain times* (TMC Asser Press | Springer 2019)

——, *Regulating Risk Profiling by Law Enforcement: A Task for Data Protection Law, Non-Discrimination Law and Criminal Procedural Law* (2024)

Veale M, Binns R and Edwards L, ‘Algorithms That Remember: Model Inversion Attacks and Data Protection Law’ (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20180083

Vedaschi A and Graziani C, ‘New Dynamics of the “Post-COVID-19 Era”: A Legal Conundrum’ (2023) 24 German law journal 1612

——, ‘New Dynamics of the “Post-COVID-19 Era”: A Legal Conundrum’ (2023) 24 German Law Journal 1612

Vedaschi A and Lubello V, ‘Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective’ (2015) 20 Tilburg Law Review

Viganò F, ‘La Tutela Dei Diritti Fondamentali Della Persona Tra Corti Europee e Giudici Nazionali’ [2019] Quad. cost.

——, ‘Rethinking the Proper Role of Proportionality in the Limitation of Fundamental

Rights', Draft text of the intervention at the international conference (Riga, 2-3 September 2021): 'EUnited in Diversity: Between Common Constitutional Traditions and National Diversities' 4th Panel: 'Limitation on the exercise of fundamental rights'

Villafuerte-Guerrero G, 'Facial Recognition Systems under the European Union's Artificial Intelligence Act Seccion III: Dossier' (2024) 15 Revista de la Facultad de Jurisprudencia (RFJ) 173

Villaronga EF, Kieseberg P and Li T, 'Humans Forget, Machines Remember: Artificial Intelligence and the Right to Be Forgotten' (2018) 34 Computer Law & Security Review 304

Villaschi P, 'La Sentenza n. 170 Del 2023: La Corte Costituzionale Chiarisce Il Perimetro Della Nozione Di Corrispondenza e Torna Sull'interpretazione Della Legge n. 140 Del 2003' [2023] Rivista di Diritto dei Media - MediaLaws

Violante L, 'Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi' [2022] BioLaw Journal - Rivista di BioDiritto 145

Vukobrat N and others, 'Chapter 4 - Implementation of Two Factor Authentication Using Face and Iris Biometrics' in Bharat Bhushan and others (eds), *Blockchain Technology Solutions for the Security of IoT-Based Healthcare Systems* (Academic Press 2023)

Wachter S, 'Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond' (2024) 26 Yale Journal of Law and Technology

Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business' (2019) 2019 Columbia Business Law Review 494

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law

Walt J van der, *The Horizontal Effect Revolution and the Question of Sovereignty* (De Gruyter 2014)

Wang P, Fan E and Wang P, 'Comparative Analysis of Image Classification Algorithms Based on Traditional Machine Learning and Deep Learning' (2021) 141 Pattern Recognition Letters 61

Warren SD and Brandeis L, 'The Right to Privacy' (1890) 4, no.5 Harvard Law Review 193

Warthon M, 'Artificial Intelligence and Freedom of Assembly' in Jeroen Temperman and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (Oxford University Press 2023)

Weber M, *Diritto / Max Weber ; a cura di Werner Gephart e Sigfried Hermes ; edizione italiana a cura di Massimo Palma* (Donzelli Editore 2016)

Werro F, 'The Right to Inform v. The Right to Be Forgotten: A Transatlantic Clash' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1401357

'What's the Difference Between AI and Regular Computing? | Royal Institution' (12 December 2023) <https://www.rigb.org/explore-science/explore/blog/whats-difference-between-ai-and-regular-computing> accessed 3 December 2024

Whitman JQ, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2003) 113 Yale Law Journal 1151

Wiener JB, 'Risk Regulation and Governance Institutions' (OECD 2010)

Wiener N, *Cybernetics or Control and Communication in the Animal and the Machine* (MIT press 2019)

Woods L, 'Zakharov v. Russia (Eur. Ct. H.R.)' (2016) 55 International Legal Materials 207

Wouters J and Ovádek M, 'Concepts and Language of Human Rights in the EU' in Jan Wouters and Michal Ovádek (eds), *The European Union and Human Rights: Analysis, Cases, and Materials* (Oxford University Press 2021)

Wright D and De Hert P, 'Introduction to Privacy Impact Assessment' in David Wright and Paul De Hert (eds), *Privacy Impact Assessment*, vol 6 (Springer Netherlands 2012)

Xenidis R, 'Shaking the Normative Foundations of EU Equality Law: Evolution and Hierarchy between Market Integration and Human Rights Rationales' (Social Science Research Network, 2017)

Xenidis R and Senden L, *EU Non-Discrimination Law in the Era of Artificial Intelligence : Mapping the Challenges of Algorithmic Discrimination* (Kluwer Law International 2020)

Yeung K, 'Algorithmic Regulation: A Critical Interrogation' (2018) 12 Regulation & Governance 505

——, 'Recommendation of the Council on Artificial Intelligence (OECD)' (2020) 59 International Legal Materials 27

——, 'Constitutional Principles in a Networked Digital Society' (Social Science Research Network, 3 March 2022)

Zalnieriute M, 'From Data Retention to Facial Recognition Technologies: Counter-Terrorism Implications for Human Rights and the Rule of Law' (Social Science Research Network 2021)

——, 'Against Procedural Fetishism: A Call for a New Digital Constitution' (2023)

30 Indiana Journal of Global Legal Studies 227

——, ‘Against Procedural Fetishism in the Automated State’ in Monika Zalnieriute and Zofia Bednarz (eds), *Money, Power, and AI: Automated Banks and Automated States* (Cambridge University Press 2023)

——, ‘Glukhin v. Russia. App. No. 11519/20. Judgment’ (2023) 117 American Journal of International Law 695

——, ‘Power and Protest: Facial Recognition and Public Space Surveillance’ in Monika Zalnieriute and Rita Matulionyte (eds), *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Zalnieriute M and Matulionyte R (eds), ‘The Cambridge Handbook of Facial Recognition in the Modern State’, *The Cambridge Handbook of Facial Recognition in the Modern State* (Cambridge University Press 2024)

Zanfir-Fortuna G, ‘Article 15 Right of Access by the Data Subject’ in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Zecca D, *La Tutela Costituzionale Della Segretezza Delle Comunicazioni e Della Corrispondenza Alla Prova Delle Tecnologie Emergenti: Profili Comparati* (Editoriale Scientifica 2023)

——, ‘La Tutela Costituzionale Della Segretezza Delle Comunicazioni Fra Avvento Dell’era Digitale e Crisi Del Paradigma Tradizionale Nella Ricerca Della Prova’, in Davide Zecca, *La tutela costituzionale della segretezza delle comunicazioni e della corrispondenza alla prova delle tecnologie emergenti: profili comparati* (Editoriale Scientifica 2023)

——, ‘L’evoluzione Delle Comunicazioni e Dei Mezzi Di Ricerca Della Prova: Le Garanzie Nelle Costituzioni Democratico-Sociali’, in Davide Zecca, *La tutela costituzionale della segretezza delle comunicazioni e della corrispondenza alla prova delle tecnologie emergenti: profili comparati* (Editoriale Scientifica 2023)

Zeng S, Zhao Y and Li S, ‘Comparison Between the Traditional and Deep Learning Algorithms on Image Matching’, *2022 IEEE/ACIS 22nd International Conference on*

Computer and Information Science (ICIS) (2022)

Zhang X, 'Convolutional Neural Networks and Architectures' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024)

——, 'Convolutional Neural Networks and Architectures' in Stan Z Li, Anil K Jain and Jiankang Deng (eds), *Handbook of Face Recognition* (Springer International Publishing 2024)

Zhou Z-H, *Machine Learning* (Springer Nature 2021)

Ziccardi G, 'Global Surveillance Activities and Digital Mining of Citizens' Data Balancing Security Issues and Civil Rights' [2018] Ragion pratica

Zubik M, Podkowik J and Rybski R, 'Judicial Dialogue on Data Retention Laws in Europe in the Digital Age: Concluding Remarks' in Marek Zubik, Jan Podkowik and Robert Rybski (eds), *European Constitutional Courts towards Data Retention Laws* (Springer International Publishing 2021)

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Barack Obama's Books of 2019* (Profile Books 2019).