EU privacy and data protection law applied to AI: unveiling the legal problems for individuals

Häuselmann, A.N.

1 Introduction

This thesis aims to unveil the legal problems individuals face when EU privacy and data protection law is applied to Artificial Intelligence (AI). This chapter begins with Section 1.1, which outlines the context and social relevance of this research. Sections 1.2 and 1.3 introduce the research question and the methodologies used to answer it. Section 1.4 clarifies the scope of the thesis by explaining the corresponding limitations, and Section 1.5 outlines the structure of this thesis.

1.1 Context and social relevance

The spectacular emergence of algorithms in the last decade has paved the way for the age of AI. In this new era, self-learning algorithms, automated predictions, classifications and various forms of scoring become even more commonplace. There is a growing public concern about the role of AI in daily life.[1] Today, hiring decisions are influenced by AI-powered emotion software capable of detecting personality traits and emotional states of job applicants based on their facial expressions.[2] Companies intend to use AI to 'hack the human brain'[3] and develop the means to allow it to control devices directly with neurodata, for example, by 'typing with thoughts'.[4] In addition, virtual assistants may use 'sniffer' algorithms to identify trigger words uttered by users, indicating statements of preference (e.g. like or love), translate them into keywords, and make these keywords subsequently accessible to advertisers.[5] When analysed with AI, a speech recording can reveal a rich variety of information about an individual, which goes well beyond the individual's identity. This includes information on the individual's emotional state,[6] personality traits, sleepiness, intoxication, physical and mental health, as well as their socioeconomic status.[7]

[1] See < https://www.liberties.eu/en/stories/impact-of-artificial-intelligence-in-everyday-life/44222 > accessed 8 February 2024; Alec Tyson, Emma Kikuchi, 'Growing public concern about the role of artificial intelligence in daily life' Pew Research Center (2023) < https://www.pewresearch.org/short-reads/2023/08/28/growing-public-concern-about-the-role-of-artificial-intelligence-in-daily-life/ > accessed 8 February 2024.
[2] Patricia Nilsson, 'How AI helps recruiters track jobseeker's emotions' *The Financial Times* (New York 3 March 2018) < https://www.ft.com/content/e2e85644-05be-11e8-9650-9c0ad2d7c5b5 > accessed 8 February 2024; For instance, HumeAI which provides AI-powered tools helping recruiters to assess personality traits as well as emotional states of candidates. See < https://hume.ai/products/facial-expression-model/ > and < https://gethume.com/blog5/artificial-intelligence-for-recruiting > accessed 8 February 2024.
[3] Nick Statt, 'Kernel is Trying to Hack the Human Brain—But Neuroscience has a Long Way to Go' *The Verge* (New York 22 February 2017) <https://www.theverge.com/2017/2/22/14631122/kernel-neuroscience-bryanjohnson-human-intelligence-ai-startup> accessed 8 February 2024.
[4] John Constine, 'Facebook is building brain-computer interfaces for typing and skin-hearing' TechCrunch (San Francisco 19 April 2017) < https://techcrunch.com/2017/04/19/facebook-brain-interface/ > accessed 8 February 2024.
[5] Edara Kiran, 'Key Word Determinations From Voice Data' US Patent Number US 8798995B1 (Assignee: Amazon Technologies, Inc.) August 2014 <https://patentimages.storage.googleapis.com/bd/ed/2b/c4c67cc5a9f1ab/US8798995.pdf>, accessed 8 February 2024.
[6] Andreas Nautsch et al, 'Preserving privacy in speaker and speech characterisation' (2019) Vol 58 Computer Speech & Language 441, 444.
[7] For more detailed information and related studies, see Jacob Leon Kröger, Otto Hans/Martin Lutz, Philip Raschke, 'Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference' in Michael Friedewald et al (eds) *Privacy and Identity management. Data for Better Living: AI and Privacy* (Springer 2020) 243.

Nevertheless, real-world examples point to reasoning deficiencies in current AI systems. They generalise, but do not distinguish, and they seem to ignore context. For example, Google's AI system developed for the purpose of recognising child abuse incorrectly classified a father as a child abuser by completely neglecting the situational context of the photograph.[8] These examples inevitably raise the question whether the current EU legal framework for the fundamental rights to privacy and the protection of personal data is fit for purpose when applied to AI.

Machine learning (ML), a major discipline of AI, produces probable yet inevitably uncertain knowledge.[9] In essence, ML-based predictions constitute 'educated guesses or bets, based on large amounts of data'.[10] If such predictions are treated as *facts*, despite their probabilistic nature, this will have real impact on humans. A statistic is factual, but with error margins, and it is not 'absolute'. The output generated by AI also raises questions in terms of fairness. Reasoning deficiencies in another AI discipline called 'automated reasoning' (AR) can lead to severe adverse effects for the individual concerned. Imagine, for example, the father who has been wrongfully classified as a child abuser by Google's AI system. By means of the AI discipline affective computing (AC), machines can access the *emotional life* of individuals, information that is highly personal, intimate and private.[11] Assessing such information may allow entities to intentionally exploit the behaviour, thoughts and decision-making vulnerabilities of individuals. As emotions play an important role in the elicitation of autonomous motivated behaviour[12] and reasoning,[13] access to an individual's emotions can therefore severely affect their personal autonomy and freedoms. For this reason, emotions merit specific protection.

That new technologies have an impact on society is naturally understood. However, the effects of new technologies such as AI cannot be easily predicted until they are widely deployed. Once they have been deployed, they are difficult to change.[14] It is also commonly understood that any disruptive technology entails risks and complex policy challenges. This applies, in particular, to AI and the fundamental rights to privacy and the protection of personal data.

[8] Kashmir Hill, 'A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as A Criminal' *The New York Times* (New York, 21 August 2022) < https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html > accessed 8 February 2024.
[9] Brent Daniel Mittelstadt et al, 'The ethics of algorithms: Mapping the debate' (2016) Vol 3 Iss 2 Big Data & Society 1, 4.
[10] Teresa Scantaburlo, Andrew Charleswoth, Nello Cristianini, 'Machine Decisions and Human Consequences' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 57; Lee A Bygrave, 'Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions' (2021) University of Oslo Faculty of Law Legal Studies Research Paper Series No. 202-35 at 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[11] Rosalind W Picard, *Affective Computing* (MIT Press 1997) 118.
[12] Leen Vandercammen et al, 'On the Role of Specific Emotions in Autonomous and Controlled Behaviour' (2014) Vol 28 Iss 5 European Journal of Personality 413, 445.
[13] Steffen Steinert, Orsolya Friedrich, 'Wired Emotions: Ethical Issues of Affective Brain–Computer Interfaces' (2020) Vol 26 Science and Engineering Ethics 351, 352.
14 Nicolas Carr, *The Big Switch: Rewiring the World, from Edison to Google* (W. W. Norton & Company 2009) N 1 at 87.

As indicated by its title, this thesis is about EU privacy and data protection law. It investigates legislation adopted by the *European Union*.[15] The fundamental right to *privacy* according to Article 7 of the European Union Charter of Fundamental Rights (EUCFR) protects everyone's 'right to respect for his or her private and family life, home and communications'. The fundamental right to the *protection of personal data* enshrined in Article 8 EUCFR grants everyone 'the right to the protection of personal data concerning him or her' ('fundamental right to data protection'). These fundamental rights are closely linked, but not identical,[16] as they differ in terms of material and personal scope.[17] Both fundamental rights are further substantiated in EU secondary law. The most relevant legislation in EU secondary law are the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD). Articles 7-8 EUCFR, GDPR and the ePD form the '*current legal framework*'. The focus lies on the GDPR because it is the most comprehensive and influential piece of legislation. EU secondary law on the fundamental right to privacy, next to the ePD, is scarce if not absent entirely.

AI entails many disciplines such as machine learning, natural language processing, computer vision, affective computing and automated reasoning. When the current legal framework is applied to these AI disciplines, three types of legal problems may occur: (1) legal provisions are violated, (2) legal provisions cannot be enforced and (3) legal provisions are not fit for purpose to protect the fundamental right at stake. I investigate these legal problems from the perspective of *individuals*, meaning natural persons, as they are holders of fundamental rights and thus have an interest in effective protection. The focus is on two types of provisions contained in the current legal framework: principles[18] and enforceable rights.[19] The three types of legal problem are not mutually exclusive. Likewise, a discipline of AI could lead to more than one type of legal problem.

This thesis aims to contribute to scientific knowledge on the suitability of EU privacy and data protection law concerning AI. As opposed to other studies,[20] this thesis considers different AI disciplines because there is nothing like 'the one AI'. With this thesis, I address current gaps in scholarship by

[15] Also, the human right to respect for private and family life, his home and correspondence according to Article 8 ECHR and related case law are considered, because these sources influence the interpretation of the corresponding fundamental rights enshrined in the EUCFR.
[16] Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 223, 228; Herke Kranenborg, Commentary of Article 8 in Steve Peers et al (eds), *The EU Charter of Fundamental Rights* (Hart/Beck 2014) 229.
[17] The material scope of the fundamental right to data protection seems to be broader whereas it is more narrow in terms of personal scope as it excludes legal persons. See Juliane Kokott, Christoph Sobotta 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' (2013) Vol 3 No 4 International Data Privacy Law 222, 225; Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, paras 52, 53 and 87.
[18] Proportionality, Lawfulness, Fairness, Transparency, Accuracy, Purpose limitation, Data minimisation, Confidentiality, Exhaustive enumeration, Accountability.
[19] Informational privacy, bodily privacy, mental privacy, communicational privacy, right of access, right to rectification, right to erasure, right to data portability, right to object, right not to be subject to ADM.
[20] Giovanni Sartor, Francesca Lagioia, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020) Study for the European Parliament's Panel for the Future of Science and Technology < https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf > accessed 8 February 2024; Frederico Marengo, *Privacy and AI: Protecting Individuals' Rights in the Age of AI* (2023).

engaging with relevant strands of computer science relating to the different AI disciplines and three specific types of legal problems. Ultimately, the suitability of the current legal framework depends on the particular AI discipline deployed and the types of legal problems caused by it.

1.2 Research question

This thesis aims to answer the following research question:

To what extent do the developments in AI require a new legal framework for the fundamental rights to privacy and the protection of personal data?

The research is structured into five subquestions:

Subquestion 1: What is AI, and what disciplines exist?
Subquestion 2: What is the current legal framework?
Subquestion 3: What legal problems arise or may arise when the *principles* enshrined in the current legal framework are applied to AI?
Subquestion 4: What legal problems arise or may arise when the *enforceable rights* enshrined in the current legal framework are applied to AI?
Subquestion 5: How should the incompatibilities of the current legal framework identified in Subquestions 3 and 4 be addressed?

Subquestion 1 examines what AI is (and what it is not), the technology of AI and the terminology used. It first elaborates on existing definitions of AI and subsequently focusses on AI disciplines that are most problematic in the context of fundamental rights to privacy and data protection. These disciplines include machine learning, natural language processing, computer vision, affective computing and automated reasoning. By means of brain-computer interfaces (BCI), also known as mind-machine interfaces, machine learning facilitates the processing of mental data, meaning any data used to infer the mental states of an individual including thoughts, beliefs and the underlying psychological mechanisms. Keyword determination systems powered by approaches from the AI discipline natural language processing attempt to identify trigger words that indicate statements of preference (such as ‘like’ or ‘love’) from speech recorded by virtual assistants and translate them into keywords for advertisement purposes. Techniques from the AI discipline computer vision are used to identify individuals based on their gait because the way in which individuals walk constitutes a unique identifier. The AI discipline affective computing facilitates the processing of emotion data, information which is highly sensitive and intimate. The AI discipline of automated reasoning focusses on automated logical reasoning, probabilistic reasoning and common sense reasoning. Subquestion 1 establishes a

proper understanding of what AI is and how it works, which is required for answering Subquestions 3, 4 and 5.

Subquestion 2 introduces the current EU legal framework relating to fundamental rights to privacy and the protection of personal data. It also examines relevant secondary EU law, namely, the General Data Protection Regulation, which is the most relevant piece of secondary EU law in the field of data protection, and the ePrivacy Directive. This subquestion sets the stage for addressing Subquestions 3 and 4, namely, what legal problems arise or may arise when the current legal framework is applied to the AI disciplines introduced in Subquestion 1.

Subquestion 3 discusses what legal problems arise or may arise when the *principles* enshrined in the current legal framework are applied to AI. To identify the legal problems, three types of legal problems are identified, namely, that (1) legal provisions are violated, (2) legal provisions cannot be enforced, and (3) legal provisions are not fit for purpose to protect the fundamental right at stake. The reasoning behind the choice to focus on these three types of legal problems is as follows. Violations of fundamental rights (Type 1) must be prevented. For example, unsupervised ML processes personal data for inexplicit purposes – the processing itself determines the purpose and future use of the personal data processed. Such processing violates the purpose limitation principle, which leads to a Type 1 legal problem. Situations in which legal provisions cannot be enforced (Type 2) are also not acceptable, because they lead to negative consequences for the de facto protection of fundamental rights. For example, the unclear substantive meaning of the fairness principle reduces legal certainty and makes it less likely that it will be enforced by means of private and regulatory enforcement. Provisions that are not fit for purpose to protect the fundamental right at stake (Type 3) point to shortcomings of the current legal framework. For example, the principle of enhancing protection for special data and the legislator's approach to exhaustively enumerate such causes a Type 3 legal problem because it does not keep up with technological developments facilitated by AI. This leads to significant gaps of protection, for example, regarding the processing of new types of sensitive personal data enabled by AI like emotion data, neurodata and mental data. Insights about Type 2 and 3 legal problems are essential when considering how the incompatibilities of the current legal framework identified should be addressed, which is the aim of Subquestion 5.

Subquestion 4 discusses what legal problems arise or may arise when the *enforceable rights* enshrined in the current legal framework are applied to AI. It identifies the same three types of legal problems as discussed in Subquestion 3. Due to the wide scope of the fundamental right to privacy, Subquestion 4 focusses on four dimensions with particular relevance for AI, namely, informational, bodily, mental, and communicational privacy. First, the fundamental right to privacy provides individuals with a form

of informational self-determination,[21] which is an extremely important dimension because AI relies heavily on the processing of information. Second, physical and mental integrity, two elements falling under the term 'private life' as developed in the corresponding case law, [22] are highly relevant. Some AI disciplines, for example, AC and ML, rely on body functions and characteristics (genetic codes, biometrics, physiological information) to gain access to mental states of individuals (thoughts, feelings, emotional states). Finally, communication is an important dimension because AI is prone to interfere with the right to respect confidential communication. AI computes communications in various forms, for instance, by means of NLP and ML. Regarding the fundamental right to data protection, Subquestion 4 focusses on enforceable rights which data subjects have according to the GDPR. They implement the requirements enshrined in the fundamental right to data protection.[23] These enforceable rights are the right of access, the right to rectification, the right to erasure, the right to portability, the right to object and the right not to be subject to automated decision-making.

Subquestion 5 discusses how the incompatibilities of the current legal framework identified in Subquestions 3 and 4 could be addressed. It does so by exploring suitable legal solutions. When referring to legal solutions, I mean (i) new interpretations of existing provisions, (ii) amending existing provisions or (iii) introducing new provisions that can 'solve' the selected legal problems. The verb 'solve' in the latter sense refers to suggestions and recommendations that can contribute to actual solutions to the selected legal problems.

1.3 Methodology

Following a single methodology can limit creativity in research by imposing a standard way of investigating law.[24] For this reason, I use several methodologies. The main research question and the corresponding subquestions determine the methodology.

The *first* method is desk research,[25] consisting of the review and analysis of typical sources in legal research. These are legislation, legislative history, case law and academic literature. To answer Subquestion 1, namely, what AI is and what disciplines exist therein, I focus on the corresponding academic literature in the field. To point to real-world use cases of AI and corresponding issues, I also use a limited number of non-scientific journalistic texts. This also incorporates the most recent

[21] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR 27 June 2017) para 137.
[22] *Denisov v Ukraine* App no 76639/11 (ECtHR 25 September 2018) para 95, *S. and Marper v United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008) *Pretty v United Kingdom* App no 2346/02 (ECtHR 29 April 2002) para 63.
[23] As emphasised by the CJEU in case law relating to the GDPR's predecessor, the DPD, see Case C-131/12, *Google Spain* [2014] ECR I-317 para 69; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081, Opinion of AG Sharpston para 55.
[24] Reza Banakar, Max Travers, 'Introduction' in Reza Banakar, Max Travers (eds) *Theory and Method in Socio-Legal Research* (Hart Publishing 2005) x.
[25] Desk research could also be seen as a research strategy rather than a method.

developments on which no academic publications are available (yet). These complementary sources stem from renowned newspapers[26] and technology-oriented news portals.[27] The goal of desk research as a method is acquiring the necessary theoretical knowledge. Therefore, desk research is particularly used for Subquestions 1 and 2 which introduce the AI disciplines and the current legal framework, respectively. I gathered sources from multiple databases, but mainly from the e-libraries of Leiden University[28] and the Eidgenössische Technische Hochschule (ETH) Zürich.[29] The latter was mainly used for sources relating to AI, as the ETH is a renowned university in the disciplines of engineering and technology.[30] The two databases were analysed using several search terms.[31] Sources obtained from these digital repositories were selected and analysed based on relevance,[32] expertise of the author and topicality.

The *second* method investigates to what extent the law in the books *differs* from the law in action. This method is largely inspired by sociolegal studies, which investigate how law is made, interpreted, and enforced.[33] The methodology vacuum in sociolegal studies helps to maintain the field as a truly interdisciplinary one, which is open to theoretical diversity and innovation.[34] Sociolegal studies typically adopt a variety of theoretical positions and methodologies.[35] Many sociolegal studies have been designed to demonstrate the *actual operation* or *lack of efficacy*.[36] Also, emerging movements such as new legal realism develop approaches that account for how law actually *works* in *practice*.[37] Sociolegal scholar Roscoe Pound long ago noted a divergence between 'law in books' and 'law in action'.[38] As is apparent from the main research question, this thesis investigates to what extent the law in the books *differs* from the law in action when *applied* to the multidisciplinary field of AI. Applying in the latter sense means performing legal analysis concerning the legal provision in question and the AI discipline deployed. This sociolegal approach is also recognisable by the three types of legal problems I discuss in this thesis. All of them concern the law in *action*: legal provisions are violated (Type 1), cannot be enforced (Type 2) or are not fit for purpose (Type 3). To unveil the difference between

[26] https://www.theguardian.com/international; https://www.independent.co.uk/; https://www.forbes.com/.
[27] https://www.wired.com/; https://www.theverge.com/.
[28] <https://www.bibliotheek.universiteitleiden.nl/> accessed 8 February 2024.
[29] <https://library.ethz.ch/en/> accessed 8 February 2024.
[30] <https://ethz.ch/en/news-and-events/eth-news/news/2022/04/eth-in-top-10-for-16-subjects.html> accessed 8 February 2024.
[31] For instance 'AI', 'AI disciplines', 'data protection', 'privacy', 'trade secrets', 'common sense', 'emotion data', 'right to rectification', 'right of access', 'enforcement' etc.
[32] Regarding the scope and limits of this thesis, as outlined in Section 1.4.
[33] Naomi Creutzfeldt, 'Traditions of Studying the Social and the Legal' in Naomi Creutzfeld, Marc Mason, Kirsten McConnachie (eds) *Routledge Handbook of Socio-Legal Theory and Methods* (Routledge 2020) 10.
[34] Reza Banakar, Max Travers, 'Introduction' in Reza Banakar, Max Travers (eds) *Theory and Method in Socio-Legal Research* (Hart Publishing 2005) x, xi.
[35] Naomi Creutzfeldt et al, 'Socio-legal theory and methods: introduction' in Naomi Creutzfeld, Marc Mason, Kirsten McConnachie (eds) *Routledge Handbook of Socio-Legal Theory and Methods* (Routledge 2020) 3.
[36] Carrie Menkel-Meadow, 'Uses and Abuses of Socio-Legal Studies' in Naomi Creutzfeld, Marc Mason, Kirsten McConnachie (eds) *Routledge Handbook of Socio-Legal Theory and Methods* (Routledge 2020) 39.
[37] Shauhin Talesh, Elizabeth Mertz and Heinz Klug, 'Introduction to the Research Handbook on Modern Legal Realism' in Shauhin Talesh, Elizabeth Mertz and Heinz Klug (eds) *Research Handbook on Modern Legal Realism* (Edward Elgar Publishing Limited 2021) 3.
[38] Roscoe Pound, 'Law in Books and Law in Action' (1910) Vol 44 Iss 1 Amercian Law Review 12, 35.

law in the books and law in action, I apply the principles and enforceable rights enshrined in the current legal framework to the AI disciplines. I use this method to answer the main research question, as well as Subquestions 3 and 4. To be clear, I refrain from engaging in empirical research, as one might expect from research inspired by sociolegal studies.[39] Instead, I focus on the difference between law in the books and law in action by performing legal analysis, as exposed by the three types of legal problems identified within this thesis. Type 2 legal problems reveal that the law in the books cannot be enforced in practice, and Type 3 legal problems exposes the lack of efficacy when law in the books operates in practice. To exhibit this, I use text boxes that concisely name and describe each legal problem identified. In addition, I use various tables to illustrate the difference between law in the books and law in action. These tables form the basis for further analysis and serve as a tool for drawing the corresponding conclusions.

The *third* method is legal doctrinal research. Doctrinal legal research relates to the first method, that is, desk research, so it is not entirely a separate method. Traditional doctrinal exploration influences how legal academics approach legal questions.[40] This holds also true for this thesis. Doctrinal legal research is a discipline that takes normative positions and makes choices among values and interests. This is inevitable when some interpretation is preferred over alternative ones. Ultimately, the choice to favour a specific interpretation is determined by giving more weight to some interests than to competing ones.[41] I have used this method mainly in addressing Subquestion 5, when setting the scene for possible legal solutions. I have also used this method when suggesting legal solutions to the six legal problems discussed in Chapter 6. There, the focus lies on the interests of natural persons as holders of the fundamental rights to privacy and the protection of personal data.

1.4 Limitations

Since AI covers a broad range of concepts, this thesis pays particular attention to AI disciplines that are problematic in light of the fundamental rights to privacy and data protection. As already outlined in Section 1.2, these disciplines are machine learning, natural language processing, computer vision, facial recognition, affective computing and automated reasoning. Methods of AI that combine AI with Robotics, i.e. 'Embodied Artificial Intelligence', are not in the scope of this thesis. Applications of Embodied AI such as driverless vehicles, surgical robots and companions pose different questions such as liability issues or ethical issues in the context of robot-human interactions.[42] These questions,

[39] Reza Banakar, Max Travers, 'Introduction' in Reza Banakar, Max Travers (eds) *Theory and Method in Socio-Legal Research* (Hart Publishing 2005) x.
[40] Shauhin Talesh, Elizabeth Mertz and Heinz Klug, 'Introduction to the Research Handbook on Modern Legal Realism' in Shauhin Talesh, Elizabeth Mertz and Heinz Klug (eds) *Research Handbook on Modern Legal Realism* (Edward Elgar Publishing Limited 2021) 1.
[41] Mark Van Hoecke, *Methodologies of Legal Research: What Kind of Method for What Kind of Discipline?* (Hart Publishing 2011) 10.
[42] Cándido García Molyneux, Rosa Oyarzabal, 'What Is a Robot (Under EU Law)?' (2018) Vol 1 RAIL: The Journal of Robotics, AI & Law 11, 12.

however, are not in the scope of this research, as they do not primarily concern the fundamental rights to privacy and the protection of personal data.

In terms of regulatory enforcement, this thesis mainly considers binding decisions adopted by the European Data Protection Board (EDPB). The EDPB consists of representatives of national EU supervisory authorities (SAs) responsible for data protection and the European Data Protection Supervisor (EDPS). Binding decisions aim to ensure the correct and consistent application of the GDPR and come into play where SAs in EU Member States interpret provisions of the GDPR differently. This limitation is bound by the focus of this thesis on EU law and needed for practical reasons, in particular the vast number of decisions adopted by SAs. However, I refer to decisions adopted by SAs occasionally. I do so when regulatory enforcement actions adopted by a specific SA particularly relate to AI and binding decisions of the EDPB are absent. Regarding private enforcement, this thesis focusses on CJEU and ECtHR case law. Occasionally, judgements adopted by Courts on Member States level are considered, in particular if corresponding CJEU and ECtHR case law are missing.

In terms of legal problems, the scope of this research is restricted in five ways. First, and foremost, this research exclusively deals with legal problems with respect to legislation adopted by the *European Union*[43] relating to the fundamental rights to privacy and the protection of personal data. It is devoted primarily to legal problems arising from the perspective of *individuals*, that is, *natural persons*. These two notions are used interchangeably. Obviously, legal problems may also arise for other actors involved, in particular controllers that process personal data by means of AI systems. However, legal problems that arise for controllers and other actors, such as providers of electronic communication services, are not within the scope of this research.

Second, the legal problems are restricted to the *principles* and *enforceable rights* enshrined in the current legal framework and leave out other obligations.[44] The principle of confidentiality contained in the ePD is the key principle of ensuring the confidentiality of communications as protected by the fundamental right to privacy. The principles form the basis for the fundamental right to protection of personal data.[45] Similarly, strong[46] and effective data subject rights[47] constitute a prerequisite for the protection of personal data. In addition, the legislator considers principles and enforceable rights as particularly important from a normative perspective. Distinctions in terms of maximum amounts for

[43] Also, the human right to respect for private and family life, his home and correspondence according to Article 8 ECHR and related case law are considered, because these sources influence the interpretation of the corresponding fundamental rights enshrined in the EUCFR.
[44] For instance the obligations contained in Chapter IV GDPR.
[45] Cécile de Terwangne, Commentary of Article 5 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 313.
[46] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[47] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.

administrative fines contained in Article 83 GDPR indicate that infringements of principles and data subject rights are considered *more serious* than infringements of other provisions.[48]

Third, and as already outlined in Section 1.2, this thesis focusses on four dimensions of the fundamental right to privacy that are particularly relevant in the light of AI, namely, informational, bodily, mental and communicational privacy.

Fourth, in terms of the fundamental right to data protection, I focus on the enforceable data subject rights enshrined in the GDPR. These enforceable rights implement the requirements set out in the fundamental right to data protection.

Fifth, this thesis approaches the fundamental rights to privacy and data protection mainly from a horizontal perspective. Private parties and powerful tech companies in particular are at the forefront of the developments in AI. Therefore, the focus is on horizontal relationships between natural persons and private parties, but not on citizens and government. This becomes apparent from the examples mentioned in Chapters 4 and 5.

1.5 Structure

Each of the subquestions introduced in Section 1.2 merits its own dedicated chapter. This thesis is therefore structured as follows:

Chapter 2 answers the first subquestion, namely, what AI is and what AI disciplines exist. It starts with existing definitions of AI (Section 2.1) and then provides an overview of the AI disciplines that seem to be the most problematic in the context of the fundamental rights to privacy and the protection of personal data (Section 2.2). These disciplines include machine learning, natural language processing, computer vision, affective computing and automated reasoning.

Chapter 3 answers the second subquestion, namely, what the current legal framework is. This chapter starts by describing the current legal framework regarding the fundamental right to privacy (Section 3.1) followed by (Section 3.2), which introduces the fundamental right to data protection. Next, (Section 3.3) discusses the most relevant piece of EU secondary law in data protection, namely, the GDPR. Finally, (Section 3.4) introduces the ePrivacy Directive, whose provisions particularise the fundamental rights to privacy and the protection of personal data in the electronic communications sector.

[48] Article 29 Working Party, 'Guidelines on the application of administrative fines for the purposes of Regulation 2016/679' (WP 253, 3 October 2017) 9; European Data Protection Board, 'Guidelines on the calculation of administrative fines under the GDPR' (Guidelines 4/2022, 16 May 2022) 16.

Chapter 4 answers the third subquestion, namely, what legal problems arise or may arise when the *principles* enshrined in the current legal framework are applied to AI. To identify the legal problems that arise or may arise from applying the current legal framework to AI, in this chapter, three types of legal problems are introduced (Section 4.1). Based on this approach, legal problems are identified for each of the AI disciplines outlined in Chapter 2. It focusses on the *principles* enshrined in the current legal framework. Sections 4.2 - 4.8 deal with the principles enshrined in the GDPR, namely, the lawfulness and proportionality (Section 4.2), fairness (Section 4.3), transparency (Section 4.4), purpose limitation (Section 4.5), data minimisation (Section 4.6), accuracy (Section 4.7) and the principle to enhance protection for special categories of personal data (Section 4.8). Section 4.9 elaborates on the principle concerning the confidentiality of communications as enshrined in the ePD. Finally, Section 4.10 concludes by providing an answer to Subquestion 3, including an overview of which AI disciplines lead to which types of legal problems.

Chapter 5 answers the fourth subquestion, namely, what legal problems arise or may arise when the *enforceable rights* enshrined in the current legal framework are applied to AI. Section 5.1 introduces the approach taken to assess legal problems. Sections 5.2 to 5.5 elaborate on the fundamental right to privacy and discuss four dimensions of privacy that are derived from the elements contained in the text of the fundamental right to privacy and corresponding case law. These four dimensions are informational (Section 5.2), bodily (Section 5.3), mental (Section 5.4), and communicational privacy (Section 5.5). Sections 5.6 to 5.11 do the same for the fundamental right to data protection. I focus on the enforceable rights which data subjects have according to the GDPR because they implement the requirements enshrined in the fundamental right to data protection.[49] These enforceable rights are the right to access (Section 5.6), the right to rectification (Section 5.7), erasure (Section 5.8), portability (Section 5.9), right to object (Section 5.10) and the right not to be subject to automated decision-making (Section 5.11). Section 5.12 concludes.

Chapter 6 answers the fifth subquestion, namely, how the incompatibilities of the current legal framework identified in Chapters 4 and 5 could be addressed. Chapters 4 and 5 strongly underscore the difference between the law in books and the law in action. Chapter 6 discusses how the gaps between the law in books and the law in action can be addressed by means of legal solutions. Because it is impossible to address all legal problems identified in Chapters 4 and 5, it focusses on six specific legal problems (Sections 6.2 - 6.7). These six legal problems are chosen based on the selection criterion effectiveness, urgency and novelty.

[49] As emphasised by the CJEU in case law relating to the GDPR's predecessor, the DPD, see Case C-131/12, *Google Spain* [2014] ECR I-317 para 69; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081, Opinion AG Sharpston para 55.

Chapter 7 answers the main research question of this thesis, namely, to what extent the developments in AI require a new legal framework for the fundamental rights to privacy and the protection of personal data. Section 7.1 answers the main research question. Then Sections 7.2 and 7.3 provide an outlook for future research and other recommendations.