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

Häuselmann, A.N.

7 Conclusion

This chapter draws the conclusions for this thesis. Section 7.1 answers the main research question. Section 7.2 provides recommendations for future legislation and Section 7.3 presents some ideas for future research.

7.1 Answer to the research question

Before providing an answer to the research question, I quickly recap the *AI disciplines*, the *current EU legal framework* and the *three types of legal problems* discussed in this thesis.

AI refers to adaptive machines that can autonomously execute activities and tasks that require capabilities usually associated with humans. In this thesis, I have focussed on five *AI disciplines*: machine learning (ML), natural language processing (NLP), computer vision (CV), affective computing (AC) and automated reasoning (AR). *ML* is a set of computational methods using experience to improve its performance and to make accurate predictions. Three methods are used for ML, i.e. supervised, unsupervised and reinforcement learning. Deep learning (DL) is a particular kind of ML that uses many layers. Approaches in DL feed a large set of input data into an artificial neural network (ANN) that produces successive transformations of the input data. Each hidden layer combines the values in the preceding layer. *NLP* aims to give computers the ability to process human language. It includes both the generation and understanding of natural language. *CV* is a discipline of AI devoted to perceive objects, described as the science and technology of machines that 'see'. *AC*, sometimes called 'emotion AI', is computing that relates to emotions and aims to develop machines with emotional capabilities. *AR* is the discipline that aims to develop computers that can use stored information to answer questions and to draw new conclusions. Research in AR focusses on logical reasoning, probabilistic reasoning and common sense reasoning.

The fundamental right to privacy according to Article 7 EUCFR protects everyone's 'right to respect for his private and family life, his home and communications'. The fundamental right to data protection as enshrined in Article 8 EUCFR grants everyone 'the right to the protection of personal data concerning him or her'. These fundamental rights are closely linked, but they are not identical,[2553] as they differ in terms of material and personal scope.[2554] Both fundamental rights are further substantiated in EU secondary law. The most relevant legislation in EU secondary law is the GDPR and the

[2553] 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.
[2554] 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 exludes 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.

ePrivacy Directive. Article 7 & 8 EUCFR as well as the GDPR and the ePrivacy Directive form the '*current legal framework*'. I have focussed on principles[2555] and enforceable rights[2556] contained in the current EU legal framework.

This thesis distinguishes between *three types of legal problems*: *(1)* legal provisions that are violated, *(2)* legal provisions that cannot be enforced and *(3)* legal provisions that are not fit for purpose to protect the fundamental right at stake. These three types of legal problems arise or may arise when principles and enforceable rights contained in the current EU legal framework are applied to the five AI disciplines.

The main research question of this thesis is:

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?

My answer to that question is as follows. It is *not* needed to establish a *new* legal framework for the fundamental rights to privacy and the protection of personal data. Rather, the current legal framework must be adjusted to ***some extent***. The extent to which this adjustment is needed largely depends on (i) the type of legal problem and (ii) the AI discipline.

(i) Type of legal problem

	Type 1	Type 2	Type 3
Principles	12	4	16
Enforceable rights	11	8	9
Total	**23**	**12**	**25**

Table 7.1 Number of legal problems (per type) distributed among principles and enforceable rights contained in the current legal framework.

A total of sixty[2557] Type 1, 2 and 3 legal problems were identified in this thesis when the principles and enforceable rights enshrined in the current legal framework are applied to the AI disciplines. This is shown in Table 7.1. Type 1 and 3 legal problems arise almost just as often and roughly occur twice

[2555] Proportionality, Lawfulness, Fairness, Transparency, Accuracy, Purpose limitation, Data minimisation, Confidentiality, Exhaustive enumeration, Accountability.
[2556] 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.
[2557] This total must not be confused with the 55 legal problems identified in Chapters 4 and 5 of this thesis. The difference between the two totals is caused by the fact that the elusiveness, interpretability, precision, trade secrets and training data problems each lead to two *types* of legal problems.

as much as Type 2 legal problems. To what extent the current legal framework should be adjusted is highly influenced by the *type* of legal problem.

For *Type 1* legal problems, the current legal framework suffices. These types of legal problems do not necessarily require adjustments of the current legal framework. The solution for these problems is obvious. Violations of provisions contained in the current legal framework need to be enforced through data subjects and/or representative bodies ('private enforcement') as well as through supervisory authorities ('regulatory enforcement'). Thus, regarding Type 1 legal problems, the current legal framework is fit for purpose, provided that violations are in fact enforced.

Conversely, the current legal framework *does not suffice* for Type *2* and *3* legal problems. Unenforceable and 'unfit' provisions are simply not appropriate to protect individuals. These two types of legal problems require either *adjustments* of current provisions or *new interpretations*. In the latter case, judicial action instead of legislative action is needed. Take, for example, the elusiveness problem (Section 4.3.2). The elusive role and meaning of the fairness principle reduces legal certainty and makes it difficult for data subjects to challenge the fairness of processing enabled by AI systems and enforce this principle (Type 2). When interpreted by the CJEU as both procedural and substantive fairness, this principle would prevent potential harm for data subjects resulting from the processing of personal data by AI systems (see Section 6.2.2). In other cases, legislative action is unavoidable. The legislator needs to adjust the provisions in the current legal framework. This applies, for example, to the communication surveillance problem discussed in Section 4.9.3. Article 5 (1) ePD regulates the confidentiality of communication, but excludes human-machine communication services facilitated by AI (e.g. virtual assistants) from its scope. This creates a significant gap of protection (Type 3). The legislator could include new provisions in the future ePrivacy Regulation and specifically regulate the confidentiality of human-machine communication.

In light of the types of legal problems, the *extent* of adjustments to the current legal framework is also influenced by the distinction between *principles* and *enforceable rights*. As shown in Table 7.1, principles cause the *majority* of Type *3* legal problems. Conversely, Type *2* legal problems occur more often with *enforceable rights* than with principles.

(ii) AI disciplines

AI Discipline	Type 1		Type 2		Type 3	
	Principles	**Rights**	**Principles**	**Rights**	**Principles**	**Rights**
Machine Learning	8	9	4	7	15	8
Total	**17**		**11**		**23**	
Natural Language Processing	4	7	3	3	9	7
Total	**11**		**6**		**16**	
Computer Vision	4	3	3	2	7	7
Total	**7**		**5**		**14**	
Affective Computing	7	7	2	5	13	7
Total	**14**		**7**		**21**	
Automated Reasoning	7	3	2	2	7	7
Total	**10**		**4**		**14**	

Table 7.2 Overview of each discipline of AI causing different types of legal problems when applied to the principles and enforceable rights in the current legal framework.

Table 7.2 shows which AI discipline causes which type of legal problem when applied to the principles and enforceable rights in the current legal framework. As apparent from Table 7.2, the current legal framework does *not* suffice regarding all *AI disciplines* discussed in this thesis. Each discipline causes Type 1, 2 and 3 legal problems. The extent of adjustments varies per discipline of AI. I use the number of Type 2 and 3 legal problems as indicators for the extent of adjustments. *ML* and *AC* clearly stand out in terms of number of legal problems. There is a clear need for adjustments of the legal framework with regard to these two AI disciplines. ML leads to thirty-five legal problems, of which eleven are Type 2 and twenty-four are Type 3. *AC* is within the same range and leads to twenty-nine legal problems, of which seven are Type 2 and twenty-one are Type 3. To a *lesser extent*, the AI disciplines NLP, CV and AR also necessitate adjustments of the current legal framework. *NLP* causes twenty-three legal problems, six of which are Type 2 and seventeen are Type 3. *CV* causes slightly fewer legal problems than NLP, i.e. twenty problems, of which five are Type 2 and fifteen are Type 3. *AR* leads to eighteen legal problems, of which four are Type 2 and fourteen are Type 3.

When considered together, the five AI disciplines discussed in this thesis lead to thirty-three Type 2 legal problems and eighty-eight Type 3 legal problems. The Type 2 legal problems expose a clear enforcement problem. Many principles and enforceable rights in the current legal framework cannot

be enforced when applied to AI. The considerably higher total of Type 3 legal problems points to an obvious mismatch between the current legal framework and the developments in AI. Altogether, Type 2 and 3 legal problems unveil a clear need for adjustments of the current legal framework. They also disclose a difference between law in the books and law in action.

With so many legal problems, the question arises what to focus on and how. In my view, the legal problems that are most urgent and have the biggest impact on individuals should be prioritised. The elusiveness, mental data, communication surveillance, trade secrets, verifiability standard and cumulativeness problems discussed in Chapter 6 meet the requirements of urgency and impact. In terms of the how to address these problems, I suggest relying on three types of possible legal solutions: (i) new interpretations of existing provisions through guidelines and courts (ii) amending existing provisions or (iii) introducing new provisions.

Notably, the best solution is *not always* to be found within the current legal framework. The legislator could consider other areas of law, ensuring that these interact properly with the current legal framework for privacy and data protection. EU consumer law, competition law and product safety law are crucial to holistically protect individuals from actual and potential harm caused by AI. In February 2024, the AI Act's compromise text[2558] was published. It remains to be seen whether the legislator is diligent enough to ensure that the current legal framework and the AI Act genuinely complement each other rather than creating confusion about their interplay. When looking at the 'right not to be subject to automated individual decision-making' (Article 22 GDPR) and the 'right to explanation of individual decision-making' (Article 68 c AI Act compromise text),[2559] confusion seems more likely.

7.2 Recommendations for future legislation

Type 2 and 3 legal problems are the most problematic because they relate to situations in which data subjects cannot enforce their rights and to provisions which are not fit for purpose to protect the fundamental rights to privacy and the protection of personal data. The law appears to protect individuals, but in reality this protection is flawed. Future legislation should focus on these two types of legal problems. Admittedly, there is no silver bullet to solve Type 2 and 3 legal problems. Nonetheless, future legislation should put the emphasis on legal provisions that are *effective*. By effective, I mean provisions that are enforceable and fit for purpose to actually protect individuals.

To enact effective legal provisions, I recommend the legislator to use two particular instruments more often: *rebuttable presumptions* and *reversal of proof*.

[2558] AI Act compromise text resulting from the trilogue negotiations <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 8 February 2024.
[2559] Ibid.

The first instrument is rebuttable presumptions. Rebuttable presumptions assume something to be true until proven otherwise. It is an evidentiary instrument and shifts the evidential burden on the party to prove the contrary.[2560] The party to whose detriment the presumption is devised must adduce evidence to demonstrate that it is incorrect. This constitutes the rebuttal. Presumptions are used in law to improve the effectiveness of enforcement or to strengthen the claimant's position.[2561] Thus, presumptions are a particularly suitable instrument to improve enforcement and strengthen the position of individuals as the holders of fundamental rights. Rebuttable presumptions are seen as the least interventionist tool and are common in national liability systems of EU Member States. Also, the EU Commission's proposal for an Artificial Intelligence Liability Directive contains several rebuttable presumptions.[2562] *Rebuttable presumptions of harm* would make provisions contained in the legal framework more effective. My suggested legal solution for the *cumulativeness problem* contains a presumption of harm (see Section 6.7.2) The proposed legal solution consists of redrafting the right not to be subject to ADM and *assumes harm* if profiling or automated inferences is intended to be used for making decisions about the data subject. It requires controllers to perform an assessment of whether the envisaged profiling or automated inferences potentially harm the data subject's interests, rights and freedoms. Data subjects can obtain this assessment from the controller, which allows them to enforce their rights enshrined in the GDPR (e.g. lodging a complaint with an SA or initiate legal proceedings). A rebuttable presumption of harm might also be helpful with respect to the compensation of *non-material damages* caused by infringements of provisions contained in the current legal framework.

The second instrument is reversal of the burden of proof. To enact provisions that are more effective, the legislator should consider *reversal of proof* to favour the rights and interests of natural persons. The burden of proof facilitates courts to arrive at a decision in a legal dispute in favour of one of the parties involved in the case.[2563] Usually, the party that asserts a certain claim must prove it.[2564] With the reversal of the burden of proof, this burden shifts to the other party who must demonstrate that the claim put forward does not stand. Rules on the burden of proof have proven to be successful instruments in EU non-discrimination law.[2565] This instrument translates legal provisions in the 'books' to effective rights that protect individuals. Reversal of the burden of proof may ease problems

[2560] David Bailey, 'Presumptions in EU competition law' (2010) Vol 34 Iss 11 European Competition Law Review 362, 363.
[2561] Cyrill Ritter, 'Presumptions in EU competitionlaw' (2018) Vol 6 Iss 2 Journal of Antitrust Enforcement 189, 206.
[2562] Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to Artificial Intelligence (AI Liability Directive) COM (2022) 496 final at 6, 11, 13 and particularly Articles 3 and 4 <https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf> accessed 8 February 2024.
[2563] Douglas Walton, *Burden of Proof, Presumption and Argumentation* (Cambridge University Press 2014) 1.
[2564] Christopher Roberts, 'Reversing the burden of proof before human rights bodies' (2021) Vol 25 Iss 10 The International Journal of Human Rights 1682, 1684.
[2565] Lilla Farkas, Orlagh O'Farrell, 'Reversing the burden of proof: Practical dilemmas at the European and national level' (2015) document prepared for the European Commission at 9 <https://op.europa.eu/en/publication-detail/-/publication/a763ee82-b93c-4df9-ab8c-626a660c9da8/language-en> accessed 8 February 2024.

of data subjects regarding the enforcement of their rights. My proposed legal solution for the verifiability standard problem makes use of this instrument. I suggest adding an additional paragraph in Article 16 GDPR that broadens the right to rectification regarding the processing of personal data generated by automated means. This empowers data subjects to easily contest the accuracy of such personal data. When data subjects do so, the controller shall either cease processing or rectify the personal data as requested by the data subject, unless it can demonstrate that its own interests to process the personal data in the form as contested by the data subject prevail. Thus, it is the controller that bears the burden of proof. The reversal of the burden of proof makes the right to rectification more effective regarding personal data generated by AI systems.

7.3 Future research

The plethora of legal problems identified in this thesis indicates a clear need for future research. In my view, future research should be interdisciplinary, connecting different disciplines like law, technology, sociology, philosophy, economics and behavioural sciences.

In a world full of probabilistic predictions, scores and other inferences generated by means of AI, the accuracy principle is more important than ever. I call for interdisciplinary research in the fields of computer science and law to better substantiate the accuracy principle. Such research should develop specific standards of accuracy for personal data processed in the context of AI. Information quality, accuracy and completeness in computer science as well as validation accuracy in ML are relevant for this.

There is a clear need for interdisciplinary research with respect to the AI Act, for example, regarding manipulation enabled by AI systems. The AI Act's compromise text bans AI systems that deploy 'subliminal' or 'purposefully manipulative' or 'deceptive' techniques.[2566] However, the effect of 'subliminal techniques' appears to be statistically insignificant.[2567] Interdisciplinary research should further investigate how AI systems could manipulate individuals, how this affects personal autonomy and creates other ethical issues, which techniques are most harmful and effective, how individuals react to manipulation attempts and its economic consequences and how the law should address manipulation. Interdisciplinary research involving the disciplines law, technology, sociology, philosophy, economics and behavioural sciences is needed for this. The results of such research allows the legislator to adopt effective legal provisions which actually protect individuals.

[2566] Article 5 (1) lit a AI Act compromise text <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 8 February 2024.
[2567] Matija Franklin et al, 'The EU's AI Act needs to address critical manipulation methods' *The OECD.AI Policy Observatory* (Paris, 21 March 2023) <https://oecd.ai/en/wonk/ai-act-manipulation-methods?utm_source=substack&utm_medium=email> accessed 8 February 2024; Randolph J Trappey, Arch G Woodside, *Brand Choice* (Palgrave Macmillan London 2005).

In the context of the AI Act, the transparency of AC systems is another topic that requires interdisciplinary research. For example, Article 3 (1) point 34 of the AI Act's compromise text directly relates to AC systems. It defines an emotion recognition system ('ERS') as 'an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data'.[2568] Article 52 (2) compromise text requires deployers of ERS to inform individuals concerned about *the operation of the system*. Accompanying Recital 70 explains that natural persons should be notified when exposed to systems that can identify or infer their emotions or intentions. Thus, deployers of AI systems are not obliged to inform individuals about which *specific emotion* the system detected. This contradicts what Picard, the pioneer in AC, propagated: individuals should be able to know which emotion the machine recognised.[2569] Thus, the AI Act's compromise text does not fill the current loophole in EU data protection law. Interdisciplinary research is needed to explore possible solutions for closing this loophole in a legally and technologically sound manner. Scientists in the fields of computer science, psychology, philosophy and law will need to work together to achieve this goal.

Future research should also explore purely technological solutions.[2570] The problem of common sense discussed in Section 4.7.1 discloses reasoning deficiencies in the AI discipline of automated reasoning. This legal problem certainly meets the priorisation criteria of urgency and impact. But the solution to this problem is not a legal one. Since a long time, scientists had tried to understand and formalise how humans reason and whether reasoning methods may be automatised.[2571] The lack of progress in developing general automated common sense reasoning capabilities underscores that this is a very difficult problem in the field of AI.[2572] Common sense reasoning appears not only to be the hardest problem for AI, but also the most important one.[2573] The solution to this problem is technological, and future research in AI should prioritise it. For example, approaches such as qualitative spatial representation and reasoning[2574] should be further explored.

[2568] Article 3 (1) point 34 AI Act compromise text <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 8 February 2024.
[2569] Rosalind W Picard, *Affective Computing* (MIT Press 1997) 122.
[2570] E.g. randomisation techniques, secure multiparty computation, homomorphic encryption, differential privacy, synthetic data or knowledge-infused learning.
[2571] Marco Gavanelli, Toni Mancini, 'Automated Reasoning' (2013) Vol. 7 No. 2 Intelligenza Artificiale 113.
[2572] Brandon Bennet, Anthony G Cohn, 'Automated Common-sense Spatial Reasoning: Still a Hughe Challenge' in Stephen Muggleton, Nicholas Chater (eds) *Human-Like Machine Intelligence* (Oxford University Press 2021) 405.
[2573] Gary Marcus, Ernest Davis, *Rebooting AI: Buidling Artificial Intelligence we can trust* (Pantheon Books 2019).
[2574] Brandon Bennet, Anthony G Cohn, 'Automated Common-sense Spatial Reasoning: Still a Hughe Challenge' in Stephen Muggleton, Nicholas Chater (eds) *Human-Like Machine Intelligence* (Oxford University Press 2021) 410, 423.

Within this thesis, I have focussed on the potential and actual legal problems for individuals caused by developments in the field of AI. However, I am also fully aware of all the potential and actual benefits for individuals. In essence, everything depends on the *actual use of AI*. Decades ago, Kranzberg put it so accurately: 'Technology is neither good nor bad; nor is it neutral'.[2575] Clearly, such a maxim applies to the use of AI as well.

[2575] Melvin Kranzberg, 'Technology and History: "Kranzberg's Laws"' (1995) Vol 15 Iss 1 Bulletin of Science, Technology & Society 5-13.