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

Häuselmann, A.N.

6 Addressing the legal problems

This chapter aims to answer Subquestion 5, i.e. how should the incompatibilities of the current legal framework identified in Chapters 4 and 5 be addressed. Chapters 4 and 5 strongly emphasise the difference between the law in books and the law in action by unveiling, in total, 55 legal problems when the current legal framework is applied to AI. This chapter discusses how the gaps between the law in books and the law in action can be addressed by means of legal solutions.

This chapter is structured as follows. Section 6.1 starts by introducing the selected legal problems, the selection criteria and the approach taken to address the legal problems. Section 6.2 discusses the elusiveness problem, Section 6.3 the mental data problem, Section 6.4 the communication surveillance problem, Section 6.5 the trade secret problem, Section 6.6 the verifiability standard problem and Section 6.7 the cumulativeness problem. Section 6.8 concludes.

6.1 Approach

In Chapters 4 and 5, 55 legal problems were identified when the current legal framework is applied to the AI disciplines introduced in Chapter 2. Because it is impossible to address all of them in sufficient depth in this chapter, I focus on six selected legal problems, as shown in Table 6.1.

Problem	Principle / Right	Type	AI Disciplines
Elusiveness	Fairness	2, 3	ML, NLP, CV, AC, AR
Mental data	Exhaustive enumeration	3	ML, AC
Communication surveillance	Confidentiality	3	ML, NLP, AC
Trade secrets	Access	2, 3	ML, NLP, CV, AC, AR
Verifiability standard	Rectification	3	ML, AC
Cumulativeness	Automated decision-making	3	ML, NLP, CV, AC, AR

Table 6.1 Overview of legal problems addressed in this chapter, principle/right concerned, type of legal problem (1, 2, 3) and AI disciplines concerned.

The decision to focus on the six selected legal problems contained in Table 6.1 is based on three selection criteria: effectiveness, urgency and novelty. I have chosen these selection criteria because I want to focus on the problems unique to AI that are most urgent and seem to have the highest impact, either by their weight (influencing several other problems) or by their sensitive nature. Choosing isolated legal problems such as the storage, verification and restriction problem would not be very effective because they are not closely intertwined with other legal problems, as is the case with the six selected legal problems. Solving these six legal problems would address simultaneously eight highly related legal problems, i.e. the manipulation, sabotage, emotion data, location data, neurodata, information restriction, unverifiable data and subjectiveness. In terms of urgency, some of the

remaining legal problems are less pressing. This applies to the transmission and restricted scope problem. The right to data portability, to which these two legal problems relate, is not a classic data protection right as it mainly aims to facilitate the transfer of personal data from one controller to another. Thus, this right stimulates competition and innovation in data-driven markets and does not entirely align with the nature of the fundamental right to data protection.[2136] In terms of novelty as a selection criterion, some legal problems are not 'new' but well known for quite a while, such as opacity, interpretability or training data problems.

Let me explain why I discuss exactly these six legal problems. First, the *elusiveness problem* is important to solve as it relates to the fairness principle, which is under great pressure considering that ten legal problems relate to this principle. In addition, the elusiveness problem raises two other legal problems, namely, the manipulation and sabotage problem. A substantively sound fairness principle may address these three problems together and could also prove helpful for other potential challenges caused by AI. Second, the *mental data problem* is very pressing due to the highly sensitive nature of mental data as it relates to the core of an individual's private sphere. Finding a solution for the mental data problem might simultaneously solve the emotion data, neurodata and location data problem, as these problems essentially arise due to the principle of enhancing protection for special data and the approach taken to enumerate such data exhaustively. Third, the *communication surveillance* problem reveals that virtual assistant services are able to intercept, analyse and otherwise process both human-machine and interpersonal communication which is problematic in terms of communicational privacy. Fourth, the *trade secrets* problem is particularly pressing as it allows controllers to restrict access to personal data, which prevents individuals from enforcing other data subject rights. This is problematic because the right of access constitutes a conditio sine qua non for the enforcement of other data subject rights, for example the right to rectification or erasure. Solving the trade secrets problem simultaneously address the inherently related information restriction problem. Fifth, the *verifiability standard* problem deserves particular attention because some AI disciplines are prone to generate inaccurate personal data, which is both problematic regarding the right to rectification and the accuracy principle. An effective solution is needed for people to seek the rectification of inaccurate personal data, as the processing of such data might be harmful to the individuals concerned. Solving the verifiability standard problem might also address two closely-related legal problems, namely, the unverifiable data and subjectivity problems. Sixth, the *cumulativeness* problem should be solved because there is a need for protection against ADM facilitated by AI. Important decisions about individuals are increasingly influenced by personal data generated through AI. Controllers increasingly rely on algorithmic tools to support their decision-making.[2137] Such data might be

[2136] Inge Graef, Martin Husovec, Nadezhda Purtova, 'Data portability and data control: Lessons for an emerging concept in EU law' (2018) Vol 19 No 6 German Law Journal 1360-1398.
[2137] Jan Biermann, John Horton, Johannes Walter, 'Algorithmic Advice as a Credence Good' (2022) Centre for European Economic Research Discussion Paper No 22-071 1, 2 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4326911 > accessed 8 February 2024.

inaccurate, which could lead to detrimental effects for individuals (e.g. in an employment or financial context).

As shown in Table 6.1, in this chapter, Type 1 legal problems will not be discussed. The solution for such problems is obvious: violations of provisions contained in the current legal framework must be enforced through data subjects and/or representative bodies going to court ('private enforcement') and through supervisory authorities ('regulatory enforcement'). Without oversimplifying the issues at stake, the first step towards improved regulatory enforcement may be harmonisation of some procedural aspects of regulatory GDPR enforcement. In 2023, the EDPB sent a wish list to the European Commission, which points to current weaknesses in terms of cross-border cooperation between SAs.[2138] After receiving this wish list, the European Commission launched an initiative to adopt a proposal in the form of a regulation to specify and harmonise procedural rules relating to the *regulatory* enforcement of the GDPR.[2139] This initiative aims to harmonise some aspects of the administrative procedures the national SAs apply in cross-border cases and to support a smooth functioning of the GDPR cooperation and dispute resolution mechanisms. Another step towards improved regulatory enforcement could be to provide SAs with more financial resources. The latter seems to be needed both on EU and Member State level.[2140]

After discarding the 23 Type 1 legal problems and the eight related legal problems that can be addressed by solving the elusiveness, verifiability standard, trade secrets and mental data problem,[2141] eighteen legal problems remain that will not be discussed. However, these remaining eighteen legal problems are not necessarily less relevant. They simply do not appear on the top of the list when applying the selection criterion effectiveness, urgency and novelty.

Sections 6.2 through 6.7 discuss how the gap (i.e. the identified legal problems) between technology (AI) and the law (legal framework) might be closed. Essentially, these gaps might be closed by either changing the technology or the law (or both). Thus, two types of solutions may address the six selected legal problems: technological solutions and legal solutions. The former refers to solutions relating to the design of and applications of AI or techniques used for it. The latter refers to new or revised legislation as well as detailing existing legislation through policies or re-interpretation by courts. The

[2138] See < https://edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf > accessed 8 February 2024.
[2139] See <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en> accessed 8 February 2024.
[2140] The EDPB and EDPS have jointly sent an open letter to the European Parliament and European Council expressing concerns about the budget for 2023; see <https://edps.europa.eu/system/files/2022-09/22-09-12_edps-edpb-open-letter-budget-2022_en.pdf> accessed 8 February 2024; EDPB, 'Overview on resources made available by Member States to the Data Protection Supervisory Authorities' (2022) <https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf> accessed 8 February 2024.
[2141] As outlined in the previous paragraph, namely manipulation, sabotage, emotion data, location data, neurodata, information restriction, unverifiable data and subjectiveness problems.

focus is on legal solutions, although it is important to stress that nonlegal solutions, technological solutions in particular, may exist or can be developed. In terms of technological solutions, approaches such as randomisation techniques,[2142] secure multiparty computation,[2143] homomorphic encryption,[2144] differential privacy,[2145] synthetic data[2146] or knowledge-infused learning[2147] should be further explored.

When referring to legal solutions, I mean (i) new interpretations of existing provisions through policies and courts, (ii) amending existing provisions or (iii) introducing new provisions that may '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. In some cases, it might be sufficient to simply interpret existing provisions in a new manner (i). This applies, for example, to the fairness principle. Re-interpreting legislation should ideally occur through judicial action performed by courts, i.e. the CJEU. New interpretations should also be reflected in regulatory guidance, for example, in guidelines established by the EDPB. In other cases, it might be necessary to tweak or completely redraft existing provisions (ii). This applies to the approach to exhaustively enumerate special categories of personal data, the right to rectification, the exceptions mentioned in the TSD and the right not to be subject to ADM. If a new interpretation or redrafting of existing provisions is not sufficient to solve the legal problem, it might be necessary to introduce new provisions (iii). This applies to the communication surveillance problem.

Let me briefly explain how I proceed when discussing solutions that could solve the selected legal problems. For each legal problem, I first set the scene and then propose concrete legal solutions to solve it. As a first step, I further examine the selected Type 2 and 3 legal problems and introduce additional analysis and interpretations that may be helpful in addressing these problems. In the second step, I provide concrete legal solutions for each legal problem discussed, namely, by proposing (i) a

[2142] Durga Prasad, Adi Narayana Reddy, Devara Vasumathi, 'Privacy-Preserving Naive Bayesian Classifier for Continuous Data and Discrete Data' in Raju Surampudi Bapi et al (eds) *First International Conference on Artificial Intelligence and Cognitive Computing* (Springer Nature 2019) 289-299; Ling Guo, 'Randomization Based Privacy Preserving Categorical Data Analysis' (DPhil thesis, University of North Carolina 2010) < http://csce.uark.edu/~xintaowu/publ/DissertationLing.pdf > accessed 8 February 2024; Klaus Jansen et al (eds), *Approximation, Randomization, and Combinatorial Optimization* (Springer 2004).
[2143] Peter Laud, Liina Kamm (eds), *Applications of Secure Multiparty Computing* (IOS Press BV 2015); Ronald Cramer, Ivan Bjerre Damgård, Jesper Buus Nielsen, *Secure Multiparty Computation and Secret Sharing* (Cambridge University Press 2015).
[2144] Justin Zhan, 'Using Homomorphic Encryption For Privacy-Preserving Collaborative Decision Tree Classification' (IEEE Symposium on Computational Intelligence and Data Mining, Honolulu 2007) <https://ieeexplore.ieee.org/document/4221360> accessed 8 February 2024; Zhiqiang Yang, Sheng Zhong, Rebecca N Wright, 'Privacy-Preserving Classification of Customer Data without Loss of Accuracy' (2005) <https://www.cs.columbia.edu/~rwright/Publications/sdm05.pdf > accessed 8 February 2024.
[2145] Cynthia Dwork, Aaron Roth, *The Algorithmic Foundations of Differential Privacy* (Now Publishers Inc 2014); Cynthia Dwork, 'Differential Privacy' in Michele Bugliesi et al (eds) *Automata, Languages and Programming* (Springer 2006) 1-12.
[2146] Sergey I Niolenko, 'Synthetic Data for Deep Learning' (2019) <https://arxiv.org/pdf/1909.11512.pdf> accessed 8 February 2024; Khaled El Emam, Lucy Mosquera, Richard Hoptroff, *Practical Synthetic Data Generation* (O'Reilly Media Inc 2020).
[2147] Manas Gaur et al, 'Knowledge-Infused Learning: A Sweet Spot in Neuro-Symbolic AI' (2022) Vol 26 Iss 4 IEE Internet Computing, 5-11; Ugur Kursuncu, Manas Gaur, Amit Sheth, 'Knowledge Infused Learning (K-IL): Towards Deep Incorporation of Knowledge in Deep Learning' (2020) <https://arxiv.org/pdf/1912.00512.pdf > accessed 8 February 2024.

new interpretation of the relevant provision, where possible. Thus, preference is given to new interpretations of existing legislation through judicial action by the CJEU or through guidelines. If this is impossible, I suggest (ii) amendments of existing provisions or (iii) entirely new provisions. The third step wraps up by means of a short conclusion.

6.2 Fairness principle – the elusiveness problem

The elusiveness problem (Type 2)

AI systems are likely to process personal data in a way that would typically be considered as unfair. 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 the fairness principle accordingly.

6.2.1 Setting the scene

As indicated[2148] in Section 4.3, scholars distinguish two types of fairness, i.e. procedural and substantive fairness. *Procedural fairness* refers to formal or process-oriented requirements[2149] focussing on whether the data have been obtained or processed through unfair means, e.g. by deception or without the knowledge of the individual concerned.[2150] Eskens as well as Wachter and Mittelstadt interpret fairness as a mere proxy for transparency[2151] which essentially falls under procedural fairness as it merely focusses on formal transparency requirements. According to their views, fairness does not merit an independent meaning because it solely relates to transparency, it is not defined in the GDPR and it only appears in the context of lawfulness or transparency.[2152] Eskens interpretation of fairness as mere transparency is backed by the argument that 'fair processing' is never mentioned in the GDPR.[2153]

[2148] Parts of Section 4.3 and Section 6.2 resulted in a publication see Andreas Häuselmann, Bart Custers, 'Substantive fairness in the GDPR: Fairness Elements for Article 5.1a GDPR' (2024) Vol 52 Computer Law & Security Review 105942.
[2149] Inge Graef, Damien Clifford, Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) Vol 8 No 3 International Data Privacy Law 200, 203.
[2150] Cecile 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) 314.
[2151] Sarah Johanna Eskens, 'Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It? (2016) Master thesis, University of Amsterdam 27 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010> accessed 8 February 2024; Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 581-582.
[2152] Sarah Johanna Eskens, 'Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It? (2016) Master thesis, University of Amsterdam 27 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010> accessed 8 February 2024; Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 582.
[2153] Sarah Johanna Eskens, 'Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It? (2016) Master thesis, University of Amsterdam 27 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752010> accessed 8 February 2024.

I think such an interpretation of fairness is not convincing. First, none of the terms mentioned in the data protection principles are defined as such in Article 4 GDPR. Rather, *some* of these principles are further substantiated in the GDPR. Article 6 GDPR, for example, implements the lawfulness principle by enumerating six legal grounds for processing. Articles 12-14 GDPR further substantiate the transparency principle by imposing specific information obligations on controllers. Other principles, such as accuracy and data minimisation, are not further substantiated in the GDPR. Second, the fact that Article 5 (1) lit a GDPR mentions fairness together with lawfulness, and transparency does not imply that these notions mean the same. If so, the legislator would not have introduced these three distinct notions and mentioned in Recital 39 GDPR that 'any processing shall be lawful *and* fair'. Of course, recitals do not have binding legal value in EU law, but they are helpful to determine the nature of a provision and expand an ambiguous provision's scope.[2154] Fourth, the claim that 'fair processing' is never mentioned in the GDPR is simply wrong. Article 5 (1) lit a GDPR literally states that 'personal data shall be processed [..], *fairly*', which is another linguistic form of expressing 'fair processing'. Fifth, regulatory enforcement at the EU level confirms that the fairness principle has an independent meaning.[2155]

Thus, the interpretation of fairness as merely procedural fairness is not convincing. Principles are open norms. They allow judges to adjust the law to changing circumstances when approaching contemporary problems. As open norms, principles are well suited to adjust data protection legislation to changing technological circumstances to achieve the goals set by the fundamental right to data protection, including legislative goals pursued by the GDPR. The latter particularly aims to achieve a consistent and high level of protection for personal data (Recitals 6 and 10), a strong and coherent data protection framework (Recital 7) and effective protection[2156] (Recital 11). The fairness principle's breadth of scope and its open texture[2157] make it a particularly suitable candidate to host normative parameters beyond transparency and to prevent data subjects from unwarranted discrimination, power imbalance and risk of vulnerability.[2158] *Substantive fairness* is more promising and suitable to solve fairness issues concerning the processing of personal data by AI systems. It aims at preventing adverse

[2154] Tadas Klimas, Jflrate Vaitiukait, 'The Law of Recitals in European Community Legislation' (2008) Vol 15 No 1 ILSA Journal of International & Comparative Law 61, 63.
[2155] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022 paras 22, 477; Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), adopted on 5 December 2022 para 226, 444; Binding Decision 5/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its WhatsApp service (Art. 65 GDPR), adopted on 5 December 2022.
[2156] Case C-645/19 [2021] *Facebook Ireland* ECR I-483 para 45; Case C-319/20, *Meta Platforms Ireland Limited* [2022] ECR I-322 para 73.
[2157] Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Autmated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 260.
[2158] 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 22, 23 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.

effects in concrete circumstances, in particular when conflicting interests need to be balanced.[2159] Also, EU primary sources seem to refer to a substantive conception of fairness.[2160] Interpreting fairness as substantial fairness complies with the CJEU's approach to favour the interpretation of a provision which is the most effective. According to settled case law, if a provision of EU law is open to several interpretations, preference must be given to the interpretation that ensures and maintains the effectiveness of the provision in question.[2161] Both regulatory guidance[2162] and regulatory enforcement at the EU level[2163] point to substantive fairness by mentioning *reasonable expectations* of the data subjects, possible *adverse consequences* of processing and effects of *power imbalance* as relevant factors of the fairness principle. Therefore, I suggest that fairness, in addition to procedural fairness covered by transparency obligations, be interpreted as *substantive fairness.* I further explain this concept in Section 6.2.2. Before doing so, I quickly elaborate on how the notion of fairness is interpreted in two other fields of EU law, namely, consumer protection and competition law. These two areas of law are particularly relevant because they deal with notions of fairness. This might provide helpful information to further substantiate this notion under data protection law. Fairness under these areas of law could therefore inform the principle of fairness under data protection law.[2164]

In consumer protection law, fairness focusses on the decision capacity of consumers. Fairness acts as the substantive standard against which the legality of contractual terms and commercial practices are tested.[2165] Under the Unfair Terms Directive (UTD),[2166] 'good faith' and 'no significant imbalance' are components of fairness that must be examined together. The principle of good faith has its roots in Roman law[2167] under the term 'bona fides'. Applying the principle of good faith in the context of consumer law requires the contracting parties to take each other's interests into account in order to achieve a fair balance.[2168] A contractual term is unfair if, contrary to the requirement of good faith, it

[2159] Gianclaudio Malgieri, 'The concept of Fairness in the GDPR' (FAT* '20: Conference on Fairness, Accountability, and Transparency, Barcelona, January 2020) 2, 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3517264> accessed 8 February 2024.
[2160] 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) Vol 4 No 2 Market and Competition Law Review 169, 177.
[2161] Case C-31/17 *Cristal Union* [2018] ECR I-168 para 41; Case C-517/07 *Afton Chemical* [2008] ECR I-751 para 43; Case C-152/13 *Holger Forstmann Transporte* [2014] ECR I-2184 para 26.
[2162] European Data Protection Board, 'Guidelines on Article 6(1)(b) GDPR' (Guidelines 2/2019, 8 October 2019), at 6.
[2163] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022 paras 219-220; Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), adopted on 5 December 2022 paras 223-224; Binding Decision 5/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its WhatsApp service (Art. 65 GDPR), adopted on 5 December 2022.
[2164] Milda Mačėnaitė, 'Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law' in Mor Bakhoum et al (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Nature 2018) 361.
[2165] Inge Graef, Damien Clifford, Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) Vol 8 No 3 International Data Privacy Law 200, 204.
[2166] Articles 3-5 of the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ 01993L0013 further on UTD.
[2167] Hugh Collins, 'Good Faith in European Contract Law' (1994) Vol 14 No 2 Oxford Journal of Legal Studies 229, 250.
[2168] Mahmoud Fayyad, 'Measures of the Principle of Good Faith in European Consumer Protection and Islamic Law, a Comparative Analysis' (2014) Vol 28 Arab Law Quarterly 205, 208; Martin Schermaier, 'Bona Fides in Roman Contract

causes a significant imbalance to the detriment of the consumer.[2169] In order to pass the fairness test under the UTD, a term must not necessarily have been individually negotiated, it must be contrary to good faith and cause a significant imbalance in the contracting parties' rights and obligations to the detriment of the consumer. In addition, when assessing good faith, particular regard should be given to the strength of the bargaining positions of the parties.[2170] From the UTD, I define *good faith* as preventing *imbalances* between the interests of the seller and consumer that are to the detriment of the consumer as a component of fairness. In the Unfair Commercial Practices Directive (UCPD),[2171] fairness focusses on the average consumer's capacity to make informed autonomous decisions.[2172] A commercial practice is unfair if it is contrary to professional diligence and distorts or is likely to distort the consumer's economic behaviour,[2173] causing the consumer to act transactionally in a way he would have otherwise not done.[2174]

Article 5 UCPD divides fairness into three levels. The UCPD protects from misleading and aggressive commercial practices and contains a blacklist of practices that are deemed de facto unfair.[2175] Aggressive practices prohibit coercion and undue influence.[2176] The prohibition of misleading practices protects consumers from taking transactional decisions that they would not have taken in the absence of false or untruthful information provided by the trader.[2177] Thus, from the UCPD I derive undue *interferences* with a consumer's *autonomy* as a component of fairness. What also follows from the concept of fairness under EU consumer law is the rationale to protect the *weaker party* (i.e. a consumer) vis-à-vis the *stronger party* (i.e. trader).[2178]

The exact meaning of fairness in EU competition law is controversial,[2179] and it is not clear what constitutes 'fair' or 'unfair' behaviour.[2180] This is, among other reasons, due to the fact that fairness depends on the context as the legality of practices under competition, law is evaluated on the basis of

Law' in Reinhard Zimmermann, Simon Whittaker (eds) *Good Faith in European Contract Law* (Cambridge University Press 2000) 65.
[2169] Article 3 (1) UTD.
[2170] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 177.
[2171] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market OJ L 149/22 furtheron 'UCPD'.
[2172] Inge Graef, Damien Clifford, Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) Vol 8 No 3 International Data Privacy Law 200, 204.
[2173] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 180.
[2174] Sarah Brown, 'European regulation of consumer credit: enhancing consumer confidence and protection from a UK perspective?' in James Devenney et al (eds) *Consumer credit, debt and investment in Europe* (Cambridge University Press 2012) 74.
[2175] Inge Graef, Damien Clifford, Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) Vol 8 No 3 International Data Privacy Law 200, 204.
[2176] Article 8 UCPD.
[2177] Article 6 UCPD.
[2178] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 182.
[2179] 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) Vol 4 No 2 Market and Competition Law Review 169, 170.
[2180] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 146.

anticompetitive nature or effects in the specific circumstances of a case.[2181] However, anticompetitive effects are considered unfair because they ultimately deprive consumers of the power to arbitrate the marketplace, which underscores the social rationale of EU competition policy.[2182] In EU competition law, Article 102 TFEU prohibits certain unfair behaviour as abuse of a dominant position.[2183] Such abuse consists, for example, of imposing unfair purchase or selling prices as well as other unfair trading conditions, limiting production, markets or technical development to the prejudice of consumers.[2184] Ultimately, Article 102 TFEU aims at regulating the abuse of market power, and it has been argued that unfairness in the context of competition law simply means exploitation.[2185] In competition law, fairness is pivotal for a pluralistic market in which companies shall not exploit dominant positions and consumers can efficiently use their financial resources.[2186] Exploitation presupposes power inequalities between the parties concerned. In this context, power relates to the ability of private parties to influence one another to their respective preferred outcomes.[2187] In case of power inequalities, one party uses its stronger position vis-à-vis the weaker party to obtain outcomes that it could not have achieved without that disparity in power.[2188] Thus, from EU competition law, I derive two components of fairness: i) non-exploitation of dominant positions and ii) recalibrating power inequalities.

Table 6.2 lists the components of (un)fairness according to EU consumer protection and competition law. As will be illustrated in Section 6.2.2, these components are also helpful to substantiate the fairness principle under EU data protection law.

Components of (un)fairness	**Area of EU law**
Preventing unfair imbalances between the parties to the detriment of *the consumer by means of the concept of good faith*	Consumer protection
Exercising undue influence on the consumer's *autonomy*	Consumer protection
Protecting the weaker party (consumer) from the stronger party (trader)	Consumer protection
Non-exploitation of dominant positions	Competition law
Recalibrating *power inequalities*	Competition law

Table 6.2 Components of 'un'fairness according to EU consumer protection and competition law.

[2181] Inge Graef, Damien Clifford, Peggy Valcke, 'Fairness and enforcement: bridging competition, data protection, and consumer law' (2018) Vol 8 No 3 International Data Privacy Law 200, 204.
[2182] Damien Gerard, 'Fairness in EU Competition Policy: Significance and Implications' (2018) Vol 9 No 4 Journal of European Competition Law & Practice 211-212.
[2183] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 146.
[2184] Article 102 TFEU.
[2185] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 184.
[2186] 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) Vol 4 No 2 Market and Competition Law Review 169, 177.
[2187] Daniel D Barnhizer, 'Inequality of bargaining power' (2005) Vol 76 Iss 1 University of Colorado Law Review 139,159.
[2188] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 173.

6.2.2 Solution: interpretation including substantive fairness

Fairness relates to both procedural and substantive fairness. The provisions in the GDPR and the corresponding recitals mostly refer to procedural fairness and provide clarity and protection in that respect. Procedural fairness contributes to fairness by elevating the controller's accountability duty to ensure effective compliance with data protection principles in the concrete case at stake. However, the lack of clarity regarding the substantive meaning of fairness creates the elusiveness problem. In this section, I argue that including substantive fairness can solve this problem. Substantive fairness, as suggested here, has two main elements.

First, substantive fairness focusses on the *outcome* or *consequences* of a process[2189] as opposed to procedural fairness which examines the fairness of the procedure by which that outcome was reached.[2190] To focus on the *outcome* or *consequence* of a certain processing activity in the context of the fairness principle neatly aligns with other provisions in the GDPR. For example, if a controller intends to further process personal data for purposes other than those for which the personal data have been initially collected, the possible consequences of such further processing must be considered.[2191] Articles 13 (2) lit f and 14 (2) lit g GDPR[2192] oblige controllers to inform data subjects about the envisaged consequences of ADM and profiling. Article 35 (1) GDPR requires controllers to assess 'the *impact* of the envisaged processing operations on the protection of personal data' where such processing operations are 'likely to *result* in a high risk to the rights and freedoms of natural persons'. In addition, Recital 150 GDPR requires supervisory authorities to take the consequences of a GDPR infringement into consideration when determining any administrative fine to be imposed on a controller.

The second major element of substantive fairness concerns fairness between *the parties* in question.[2193] It recalibrates imbalanced situations and is used in other areas of law, such as employment law.[2194] In the context of data protection law, substantive fairness as suggested here concerns fairness between the *controller* and the *data subject*. This element of substantive fairness aligns with other provisions in the GDPR. The relationship between controller and a data subject is mentioned in Article 6 (4) lit b and Recital 50 GDPR. According to these provisions, the controller needs to take its relationship with the data subject into consideration. The same applies in the context of the Legitimate Interest Assessment. When assessing whether to rely on its legitimate interest for a certain processing

[2189] Stephen A Smith, 'In Defence of Substantive Fairness' (1996) Vol 112 Iss 1 Law Quarterly Review 138-158.
[2190] Pinar Akman, *The Concept of Abuse in EU Competition Law* (Hart Publishing Ltd 2012) 166.
[2191] Article 6 (4) lit d and Recital 50 GDPR.
[2192] See also Recital 60 GDPR.
[2193] Stephen A Smith, 'In Defence of Substantive Fairness' (1996) Vol 112 Iss 1 Law Quarterly Review 138-158.
[2194] 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) Vol 4 No 2 Market and Competition Law Review 169, 173.

activity, the controller needs to take the reasonable expectations of data subjects into account, based on the controller's relationship with the data subjects.[2195]

It is often easier to determine whether a particular outcome is unfair rather than to agree on whether the outcome is fair.[2196] This is indicated in the title of the two major directives in EU consumer protection law which both use the term 'unfair'. Likewise, EU competition law explicitly prohibits certain unfair behaviour as abuse of a dominant position.[2197] Therefore, I suggest focussing on components of fairness that may lead to unfair processing of personal data, rather than to fair processing. Table 6.3 lists the components that must be considered when assessing fairness in the context of processing personal data. The components are divided into the two major elements of substantive fairness, i.e. fairness between the parties and fairness of the outcome.

Components concerning fairness between the parties	
No power inequalities / dominant positions	Is the controller exploiting power inequalities and/or dominant market positions?
Vulnerability	Is the data subject vulnerable?
Good faith	Does the balancing of interests violate the concept of good faith?
Components concerning fairness of the outcome	
Autonomy	Is it likely that the processing will negatively affect the data subject's autonomy and, in particular, decisional privacy?
Non-manipulation	Does the processing create risks regarding the manipulation of the data subject?
No detrimental effects	Does the processing likely lead to detrimental effects for the data subject, e.g. due to the nature of the personal data processed?
Accuracy	Is the processed personal data likely to be inaccurate or is it difficult to determine the accuracy of the processed personal data?
Non-discrimination	Is the outcome of the processing likely to be discriminatory?

Table 6.3 Components of substantive fairness to be considered under the fairness principle in EU data protection law.

The components of substantive fairness listed in Table 6.3 comprehensively protect data subjects from unfair processing because they focus on both the relationship between the data subject and the controller *as well as* on possibly unfair outcomes of processing. These components of substantive fairness specifically address the legal problems identified in this thesis. Obviously, it might be necessary to add additional components in the future as new or additional legal problems arise.

[2195] Recital 47 GDPR.
[2196] Francis Herbert Buckley, 'Three Theories of Substantive Fariness' (1990) Vol 19 Hofstra Law Review 33, 56.
[2197] Article 102 TFEU.

At first sight, it might be surprising that the component '*power inequalities/dominant positions*' should be assessed in the context of fairness under data protection law, as these concepts originate from EU consumer and competition law, which have different legislative aims. Nevertheless, there is often a power inequality between the controller and data subject: It is the controller that determines the purpose of processing, the legal basis for processing, how long data will be stored, whether personal data are accurate, with whom data will be shared and for which purposes personal data will be further processed after collection. Data subjects have enforceable rights, but they cannot influence most of the decisions the controller takes regarding these rights. There is a clear power inequality between the data subjects and the controller, and this power inequality should be considered when assessing fairness in data protection law. In terms of *abusing dominant positions*, which is a concept from EU competition law, competition authorities increasingly take non-compliance into consideration when assessing whether an undertaking abuses its dominant position or engages in other anti-competitive practices.

The Bundeskartellamt, which is Germany's Competition Authority, initiated proceedings due to Google's data processing terms, which allegedly amount to prohibited anticompetitive practices.[2198] AG Rantos argued that competition authorities may take compliance with the rules enshrined in the GDPR into consideration when examining an undertaking's conduct under EU competition law.[2199] The CJEU followed the AG's opinion, provided that the competition authority fulfils its duty of 'loyal cooperation' and consults the competent data protection supervisory authority.[2200] Also, the circumstance in which a controller holds a dominant market position is a relevant factor when assessing whether consent according to Article 4 (11) GDPR is freely given, because a dominant market position affects the freedom of choice of the data subject.[2201] Thus, the CJEU confirms that dominant market position and power imbalance are relevant factors to be considered in the context of data protection law. For this reason, it must be possible to also consider a controller's dominant market position and power imbalances between the controller and the data subject when assessing fairness in EU data protection law.

Vulnerability is mentioned in Recital 75 GDPR in the context of security of processing. The recital states that children must be considered in particular as 'vulnerable natural persons'. However, it is not only children who are potentially vulnerable data subjects. In my view, data subjects are also particularly vulnerable when special categories of personal data relating to them are being processed. Due to the sensitivity of such data, processing is particularly eligible to create harm.[2202] Vulnerability

[2198] See < https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html > accessed 8 February 2024.
[2199] Case C-252/21 *Meta Platforms Inc.* [2022] ECR I-704, Opinion of AG Rantos paras 23-33.
[2200] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 paras 56-63.
[2201] Ibid paras 148-149, 154.
[2202] Art 29 Working Party, 'Advice paper on special categories of data ('sensitive data')' (20 April 2011) at 4.

also plays an important role in the processing of emotion data. In fact, revealing emotions makes an individual potentially more vulnerable.[2203] Although not specifically mentioned in any specific provisions, data protection law arguably manifests the idea that data subjects are vulnerable to power imbalances created by digital technologies[2204] simply by regulating the processing of personal data. It therefore seems reasonable to assess the vulnerability[2205] of data subjects in the context of the fairness principle, and not only in the context of other provisions in the GDPR such as provisions relating to consent, DPIAs and ADM.[2206]

Traditional conceptions of *good faith* have their roots in virtue ethics as well as Roman law and essentially refer to the idea of acting in good conscience or not unconscionably, which would prevent taking advantage of another's trust.[2207] The classical notion of bona fides is today enjoying a renaissance and helps modern lawyers to solve current issues.[2208] This applies particularly to virtue ethics. For example, it has been suggested to adopt a virtue ethics approach to privacy regulation.[2209] Virtue ethics focusses on the notion of the good or virtuous person.[2210] Aristotle is seen as the dominant influence on the conceptual profile of virtue.[2211] He conceptualised virtues as character traits[2212] such as such as honesty, courage and patience that promote the performance of right or excellent actions.[2213] In particular, the virtues honesty and trust[2214] seem to relate to the concept of good faith. Good faith is well suited to prevent controllers from taking advantage of their stronger position and should therefore be considered when assessing the fairness of processing. In fact, some have argued to broaden the understanding of the fairness principle in data protection law with the aim to prevent processing contrary to good faith.[2215]

The fairness components *autonomy* and non-*manipulation* are closely related. The essence of autonomy is indicated by the etymology of the term: autos (self) and nomos (rule or law).[2216] The ruling

[2203] Aaron Ben-Ze'Ev, *The Subtlety of Emotions* (MIT Press 2000) 183.
[2204] Ryan Calo, 'Privacy, Vulnerability, and Affordance' (2017) Vol 66 Iss 2 Depaul Law Review 591, 592-593; Gianclaudio Malgieri, Jędrzej Niklas, 'Vulnerable data subjects' (2020) Vol 37 Computer Law & Security Review 2-16.
[2205] For an extensive analysis of vulnerable data subjects, see Gianclaudio Malgieri, Vulnerable People and Data Protection Law (Oxford University Press 2022).
[2206] Gianclaudio Malgieri, Jędrzej Niklas, 'Vulnerable data subjects' (2020) Vol 37 Computer Law & Security Review 2-16.
[2207] Hugh Collins, 'Good Faith in European Contract Law' (1994) Vol 14 No 2 Oxford Journal of Legal Studies 229, 250.
[2208] Martin Schermaier, 'Bona Fides in Roman Contract Law' in Reinhard Zimmermann, Simon Whittaker (eds) *Good Faith in European Contract Law* (Cambridge University Press 2000) 89.
[2209] Bart van der Sloot, *Privacy as Virtue* (Cambridge University Press 2017) 107-143.
[2210] Nathan R Kollar, 'Virtue Ethics' in John K Roth (ed) *Ethics* (Salem Press Inc 2005) 562.
[2211] Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting* (OUP 2016) 18.
[2212] Bart van der Sloot, *Privacy as Virtue* (Cambridge University Press 2017) 109.
[2213] Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting* (OUP 2016) 18.
[2214] The virtues honesty and trust are related; see Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting* (OUP 2016) 121. See also Aimee van Wynsberghe, 'Artificial intelligence: from ethics to policy' (2020) study prepared for European Parliament, 12.
[2215] Milda Mačėnaitė, 'Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law' in Mor Bakhoum et al (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Nature 2018) 368.
[2216] Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge University Press 1988) 12, 18.

idea of personal autonomy is 'that people should make their own lives',[2217] which means facing freely both existential and everyday choices.[2218] A person is considered to be autonomous when her decisions and actions are her own and thus self-determined,[2219] i.e. a person acts but is not acted upon.[2220] Autonomy is closely related to privacy, partly because privacy seems to be a precondition for autonomy.[2221] It has become one of the core pillars of the fundamental right to privacy under case law adopted by the ECtHR.[2222]

External influences such as manipulation constitute threats to personal autonomy.[2223] The concept of decisional privacy is well suited to address concerns about manipulation.[2224] Decisional privacy refers to being free to make personal decisions and choices.[2225] This erodes when manipulation invades internal thought processes, affects free will or interferes with an individual's self-interest.[2226] As explained in Section 4.3.3, manipulation aims to influence people's choices in ways that circumvent or counter rational decision-making.[2227] It refers to exercising direct influence on an individual's beliefs, desires or emotions to the detriment of individual self-interest[2228] and may involve the act of altering the actual choices available to a person or changing this person's perception of those choices.[2229] Fairness in data protection law should take into account autonomy and non-manipulation because processing of personal data by means of AI generates personal data that might be used in a way that negatively affects the data subject's autonomy. AC generates emotion data that could be used to the detriment of the data subject. Emotions play an important role in the elicitation of autonomous motivated behaviour.[2230] According to research in behavioural science, especially psychology, emotions

[2217] Joseph Raz, *The Morality of Freedom* (Oxford University Press 1986) 369.
[2218] Daniel Susser, Beate Roessler, Helen Nissenbaum 'Technology, autonomy, and manipulation' (2019) Vol 8 Iss 2 Internet Policy Review 1, 8.
[2219] Gerald Dworkin, *The Theory and Practice of Autonomy* (Cambridge University Press 1988) 13.
[2220] See Berlin, which explains the concept of autonomy under the heading positive liberty: 'Isaiah Berlin, *Liberty* (Hendry Hardy ed Oxford University Press 1969) 185; Marijn Sax, *Between Empowerment and Manipulation* (Kluwer Law International B.V. 2021) 131.
[2221] Hildebrandt Mireille, Koops Bert-Jaap, 'The challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) Vol. 73 (3) The Modern Law Review 428, 435.
[2222] Bart van der Sloot, 'Decisional privacy 2.0: the procedural reqirements implicit in Article 8 ECHR and its potential impact on profiling' Vol 7 No 3 International Data Privacy Law 190, 192, *Munjaz v the United Kingdom* App no 2913/06 (17 July 2012) para 80; *NB v Slovakia* App no 29518/10 (12 June 2012); *IG and others v Slovakia* App no 15966/04 (13 November 2012); *VC v Slovakia* App no 18968/07 (8 November 2011).
[2223] Lawrence Haworth, 'Dworkin on Autonomy' (1991) Vol 102 Ethics 129, 136.
[2224] Marjolein Lanzig, 'Strongly Recommended: Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies' (2019) Vol 32 Philosophy & Technology 549-568.
[2225] Bart van der Sloot, 'Decisional privacy 2.0: the procedural reqirements implicit in Article 8 ECHR and its potential impact on profiling' Vol 7 No 3 International Data Privacy Law 190, 192.
[2226] Francisco Lupiáñez-Villanueva et al, 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation' (2022) Final Report produced by European Innovation Council and SMEs Executive Agency on behalf of the European Commission 92 < https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418 > accessed 8 February 2024.
[2227] Allen W Wood, 'Coercion, Manipulation, Exploitation' in Christian Coons, Michael Weber (eds) *Manipulation* (Oxford University Press 2014) 35.
[2228] Anne Barnhill, 'What is Manipulation?' in Christian Coons, Michael Weber (eds) *Manipulation* (Oxford University Press 2014) 52.
[2229] Ruth Faden, Tom Beachamp, Nancy King, *A History and Theory of Informed Consent* (Oxford University Press 1986) 354.
[2230] 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.

constitute powerful, pervasive and predictable drivers of decision-making.[2231] Emotions can have significant effects on economic transactions and play a powerful role in everyday economic choices.[2232] Likewise, accurate predictions generated by means of ML through the processing of personal data (e.g. purchase history) might be used to manipulate data subjects through tailored recommendations in a way that actions of the data subject are no longer self-determined.

Detrimental effects are at the core of substantive fairness because they directly refer to the *outcome* or *consequences* of a process.[2233] Output generated by AI systems may have detrimental effects for data subjects in many ways. Predictions facilitated by ML approaches, such as negative score values, can prevent the data subject from obtaining a loan to buy a house, a mobile subscription or health insurance coverage. The emotional state of an applicant detected during an automated video assessment can play a role when the hiring manager decides whether the applicant will be invited for the second round of interviews. Such detrimental effects generated by means of AI are generally problematic in terms of substantive fairness. They become even more problematic when the output generated by AI systems is *inaccurate* or *likely* to be inaccurate. Inaccurate personal data may pose significant risks, for example, in the form of economic or reputational harm.[2234] Predictive profiling powered by ML may be used to predict an individual's behaviour, character, risk (e.g. score values) and to treat the individual accordingly.[2235] Predictions can hardly be absolutely certain and are poorly verifiable in the sense that they cannot be verified in advance or sometimes not at all (e.g. the individual is a 'high credit risk' or 'likely to buy a house in two years').[2236] Essentially, ML-based predictions or classifications constitute 'educated guesses based on large amounts of data'.[2237] Inference 'is always an invasion of the unknown, a leap from the known'.[2238] Examples include predictions about a customer's future life such as estimated advancements in career,[2239] credit risk scores, life expectancy scores or future health.[2240] Emotion data generated by means of AC can also be inaccurate.

[2231] Jennifer S Lerner et al, 'Emotion and Decision Making' (2015) Vol 66 Annual Review of Psychology 799, 802.
[2232] Jennifer S Lerner, Deborah A Small, George Loewenstein, 'Heart Strings and Purse Strings' (2004) Vol 15 No 5 American Psychology Society 337-340.
[2233] Stephen A Smith, 'In Defence of Substantive Fairness' (1996) Vol 112 Iss 1 Law Quarterly Review 138-158.
[2234] Danielle Keats Citron, Daniel J Solove, 'Privacy Harms' (2022) Vol 102 Iss 3 Boston University Law Review 793, 817.
[2235] Helena U Vrabec, 'Uncontrollable: Data Subject Rights and the Data-driven Economy' (Dissertation, Leiden University 2019) 220; Hans Lammerant, Paul de Hert, 'Predictive profiling and its legal limits: Effectiveness gone forever' In Bart van der Sloot et al (eds) *Exploring the boundaries of big data* (2016 Amsterdam University Press/WRR) 145-173.
[2236] Sandra Wachter, Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Issue 2 Columbia Business Law Review 494, 510.
[2237] 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.
[2238] John Dewey, *The Middle Works of John Dewey, Volume 9, 1899-1924* (Carbondale Southern Illinois University Press 1980) 165.
[2239] Gianclaudio Malgieri, 'Trade Secrets v. Personal Data: A Possible Solution for Balancing Rights' (2016) Vol 6 No 2 International Data Privacy Law 102, 113-114; Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 495, 607.
[2240] OECD Working Party on Security and Privacy in the Digital Economy JT03357584 (2014) <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en> accessed 8 February 2024.

According to an extensive study on affect recognition from facial expressions, it is not possible to confidently infer happiness from a smile, anger from a scowl or sadness from a frown because these emotion categories are more variable in their facial expressions.[2241] Other means to detect emotions, for example, based on speech (see Section 2.2.4.2) and physiological data (see Section 2.2.4.3), have been challenged due to a lack of scientific consensus whether such methods can ensure accurate or even valid results.[2242] It has been argued to broaden the understanding of the fairness principle in data protection law with the aim to prevent processing, which might have detrimental effects for the data subjects concerned.[2243]

Simply putting someone at risk may have a detrimental effect for the data subject, even if that risk never materialises. Harms relating to the processing of inaccurate personal data are highly contextual and depend on how such data are subsequently used. Adverse effects and actual harm depend on various factors such as by which controller the personal data are used, to whom it is disclosed and whether it is shared with other controllers.[2244] In any case, inaccurate personal data inherently causes the risk of possible detrimental effects, regardless of whether this risk materialises. Therefore, the accuracy of personal data also should be considered when assessing fairness in data protection law.

That *discrimination* must be considered in the context of substantive fairness is obvious. There are many examples that processing personal data by means of AI systems may lead to discriminatory outcomes. Due to deficiencies in reasoning capabilities, AI systems may generate discriminatory output. Google's photo app automatically classified images of black people as gorillas.[2245] In New Zealand, a man of Asian descent had his passport application rejected because the software that approves photos claimed his eyes were closed.[2246] Face recognition systems perform poorly in recognising individuals of different ethnicities. For example, face recognition software of Hewlett Packard could not recognise dark-coloured faces as faces.[2247] ADM based on ML could discriminate by means of classes or groups that lead to emergent forms of discrimination based on patterns that have little or

[2241] Lisa Feldman Barrett et al. 'Emotional Expressions Reconsidered' (2019) Vol 20 (1) Psychological Science in the Public Interest 1, 46.
[2242] Kate Crawford et al, 'AI Now Report' (2019) AI Now Institute 12 <https://ainowinstitute.org/publication/ai-now-2019-report-2> accessed 8 February 2024.
[2243] Milda Mačėnaitė, 'Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law' in Mor Bakhoum et al (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law* (Springer Nature 2018) 368.
[2244] Danielle Keats Citron, Daniel J Solove, 'Privacy Harms' (2022) Vol 102 Iss 3 Boston University Law Review 793, 817-818.
[2245] Crawford Kate, 'Artificial Intelligence's White Guy Problem' *The New York Times* (New York, 25 June 2016) <https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html> accessed 8 February 2024.
[2246] Titcomb James, 'Robot passport checker reject Asian man's photo for having his eyes closed' The Telegraph (London, 7 December 2016) <https://www.telegraph.co.uk/technology/2016/12/07/robot-passport-checker-rejects-asian-mans-photo-having-eyes/> accessed 8 February 2024.
[2247] Frederik Zuiderveen Borgesius, 'Discrimination, artificial intelligence, and algorithmic decision-making'(2019) Report for the Anti-discrimination department of the Council of Europe, 17 <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> accessed 8 February 2024.

no intuitive meaning to human practice and thus are socially unrecognisable.[2248] Newly identified classes or groups by means of ML arguably facilitate new forms of social classification with far-reaching socioeconomic consequences,[2249] such as new types of socioeconomic stratification and social hierarchies,[2250] and could consequently lead to new forms of discrimination.[2251] AI may reflect the conscious and unconscious biases of the people who assemble it and thus produce biased outcomes.[2252] This is called encoded bias because the designer's values are 'frozen into the code, effectively institutionalising those values'.[2253] The interests, needs and life experiences of the AI developers will be reflected in the AI they develop,[2254] potentially including stereotyped thinking in terms of traditional gender roles[2255] or racial/ethnic prejudices.

Because humans label much of the training data, human biases and cultural assumptions may be transmitted by classification choices.[2256] Discriminatory attitudes and stereotypes of developers are translated and reflected in the AI system they build.[2257] The developer's prejudices may be reinforced within the ADM system,[2258] and because ML algorithms are applied to every case in which ADM is deployed, they arguably have a bigger potential to discriminate systematically than human decision makers who may discriminate on a case-by-case basis.[2259] This is not only a theoretical concern. Diversity in the ML and AI community is, in fact, an issue. A study that focussed on the 4,000 researchers who published at leading AI and ML conferences disclosed that 88% of the contributions was by from men and only 12% by women.[2260] People that investigate, design and develop AI systems tend

[2248] Monique Mann, Tobias Matzner 'Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination' (2019) Vol 6 Iss 2 Big Data & Society 2, 6 < https://journals.sagepub.com/doi/pdf/10.1177/2053951719895805> accessed 8 February 2024.
[2249] Shoshana Zuboff, *The age of surveillance capitalism* (PublicAffairs 2019).
[2250] Stratification typically focus on income, wealth, occupational structures, social mobility etc see Cecilia L Ridgeway, 'Why Status Matters for Inequality' (2013) Vol 79 Iss 1 American Sociological Review 1, 3.
[2251] Raphaële Xenidis, 'Tuning EU equality law to algorithmic discrimination> Three pathways to resilience' (2020) Vol 27 Iss 6 Maastricht Journal of European and Comparative Law 7636, 752.
[2252] Brent Daniel Mittelstadt et al, 'The ethics of algorithms: Mapping the debate' (2016) Vol 3 Iss 2 Big Data & Society 1, 7.
[2253] Kevin Macnish, 'Unblinking the eyes: the ethics of automating surveillance' (2012) Vol 14 Ethics and Information Technology 151, 158.
[2254] Alex Campolo et al, 'AI Now Report' (2017) 15 <https://ainowinstitute.org/publication/ai-now-2017-report-2> accessed 8 February 2024.
[2255] Janneke Gerards, Raphaële Xenidis, 'Algorithmic discrimination in Europe: Challenges and Opportunities for geneder equality and non-discrimination law' (2021) at 51 study prepared for the European Commission <https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1> accessed 05 May 2021.
[2256] Alex Campolo et al, 'AI Now Report' (2017) 15 <https://ainowinstitute.org/publication/ai-now-2017-report-2> accessed 8 February 2024.
[2257] Janneke Gerards, Raphaële Xenidis, 'Algorithmic discrimination in Europe: Challenges and Opportunities for geneder equality and non-discrimination law' (2021) at 41 study prepared for the European Commission <https://op.europa.eu/en/publication-detail/-/publication/082f1dbc-821d-11eb-9ac9-01aa75ed71a1> accessed 8 February 2024.
[2258] Kevin Macnish, 'Unblinking the eyes: the ethics of automating surveillance' (2012) Vol 14 Ethics and Information Technology 151, 158.
[2259] Indrė Žliobaitė, 'Measuring discrimination in algorithmic decision making' (2017) Vol 31 Data Mining Knowledge Discovery 1060, 1063.
[2260] Mantha Yoan, Hudson Simon, 'Estimating the Gender Ratio of AI researchers Around the World' <https://medium.com/element-ai-research-lab/estimating-the-gender-ratio-of-ai-researchers-around-the-world-81d2b8dbe9c3> accessed 8 February 2024.

to be male, highly educated and very highly paid.[2261] The AI Now Institute found that there is a diversity crisis in the AI sector across gender and race. It found that more than 80% of AI professors are men and in the private sector only 15% of AI research staff at Facebook and 10% at Google are women. When considering diversity in terms of skin colour, the picture looks even worse: only 2.5% of Google's workforce is black, while Facebook and Microsoft are each at 4%.[2262] Therefore, it seems very important to also consider non-discrimination when assessing fairness in the context of data protection law.

6.2.3 Conclusion

In this section, I have outlined that the legal solution to solve the elusiveness problem consists of interpreting the fairness principle in data protection law as both procedural and substantive fairness. The provisions in the GDPR and the corresponding recitals provide clarity with respect to procedural fairness. Substantive fairness, as suggested here, contains two main elements: fairness between the parties and fairness of the outcomes. Table 6.2 contains six components of substantive fairness, distributed over the two main elements of substantive fairness. These components are no power inequalities/dominant positions, vulnerability, good faith, autonomy, non-manipulation, detrimental effects, accuracy and non-discrimination. They indicate *unfairness*. My *solution* to the elusiveness problem is to adopt extensive EDPB guidelines on the principle of fairness and include these components of substantive fairness. In fact, both regulatory guidance[2263] and regulatory enforcement at the EU level[2264] already point to at least three components[2265] of substantive fairness proposed. However, specific regulatory guidance on the principle of fairness does not yet exist, although this principle merits further substantiation in detailed guidelines. To consider the suggested components of substantive fairness is in line with the CJEU's settled case law to give preference to the method of interpretation that ensures and maintains the effectiveness of the provision.[2266] To ultimately 'solve' the elusiveness problem, judicial action is needed. Thus, the CJEU should interpret fairness in EU data protection law as referring to both procedural and substantive fairness.

[2261] Alex Campolo et al, 'AI Now Report' (2017) 5 <https://ainowinstitute.org/publication/ai-now-2017-report-2> accessed 8 February 2024.
[2262] Sarah West, Meredith Whittacker, Kate Crawford 'Discriminating AI Systems: Gender, Race and Power' (2019) AI Now Institute 3 <https://ainowinstitute.org/publication/discriminating-systems-gender-race-and-power-in-ai-2> accessed 8 February 2024.
[2263] European Data Protection Board, 'Guidelines on Article 6(1)(b) GDPR' (Guidelines 2/2019, 8 October 2019), at 6.
[2264] Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR), adopted on 5 December 2022 paras 219-220, 222-223; Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR), adopted on 5 December 2022 paras 223-224, 226-227; Binding Decision 5/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its WhatsApp service (Art. 65 GDPR), adopted on 5 December 2022.
[2265] These are possible (i) adverse consequences of processing which is the same as my suggested component *detrimental effects*, (ii) the data subject's autonomy and (iii) effects of power imbalance which essentially relate to my suggested component of *power inequalities.*
[2266] Case C-31/17 *Cristal Union* [2018] ECR I-168 para 41; Case C-517/07 *Afton Chemical* [2008] ECR I-751 para 43; Case C-152/13 *Holger Forstmann Transporte* [2014] ECR I-2184 para 26.

The advantage of this approach is that controllers can and should consider these components when performing a Data Protection Impact Assessment (DPIA) as required by Article 35 GDPR. According to this provision, controllers must carry out a DPIA if the envisaged processing is likely to result in a high risk to the rights and freedoms of data subjects. This is particularly the case when the controller uses 'new technologies'[2267] for processing, which arguably applies to processing by AI systems. My proposal is also in line with teleological interpretation in EU law, which tasks the CJEU to give concrete expressions to notions that are too general or of which the meaning is unclear.[2268]

6.3 Enhanced protection for 'special data' – the mental data problem

The mental data problem (Type 3)

ML and AC facilitate the processing of mental data, i.e. any data used to infer mental states of individuals including thoughts, beliefs and underlying mechanisms and processes. Mental data are inherently sensitive and form the core of an individual's private sphere. Despite this, mental data are not specifically protected under the GDPR because the approach to enumerate special categories of personal data exhaustively cannot keep up with the developments in AI. This principle creates a significant gap of protection and is not fit for purpose to protect the fundamental right to data protection.

6.3.1 Setting the scene

As outlined in Section 4.8.3, the approach to exhaustively enumerate special data fails. It cannot keep up with technological developments in AI that facilitate unprecedented ways to generate or otherwise process new types or categories of sensitive personal data. Mental data forms the core of an individual's private sphere.[2269] They may contain information concerning unexecuted behaviour, such as unuttered thoughts and intended actions,[2270] information previously inaccessible to others. Therefore, mental data are particularly sensitive and in need of specific protection.

To solve the mental data problem and other legal problems inextricably linked to it (i.e. emotion data, location data and neurodata problems), new or revised legislation is unavoidable. This is due to the wording of Article 9 (1) GDPR, which does not provide any room to broaden the scope of this

[2267] Article 35 (1) GDPR.
[2268] Pierre Pescatore, 'Les objectifs de la Communauté européenne comme principes d'interprétation dans la jurisprudence de la Cour de justice' (1972) vol 2 Miscellanea W.J. Ganshof van der Meersch 328; Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 6 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.
[2269] Dara Hallinan et al, 'Neurodata and Neuroprivacy: Data Protection Outdated?' (2014) Vol 12 Iss 1 Surveillance and Society 68 <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata/neurodata4> accessed 8 February 2024.
[2270] Marcello Ienca, Gianclaudio Malgieri, 'Mental data protection and the GDPR' (2022) Vol 9 Iss 1 Journal of Law and the Biosciences 1, 6.

provision by means of different interpretation methods. Literal (textual) interpretation is the prevailing method of interpretation if the provision to be interpreted is clear and precise.[2271] The wording in Article 9 (1) GDPR clearly points to an exhaustive enumeration of special personal data. Typical words from the legal jargon ('for instance', 'such as', 'inter alia' etc.) used to indicate non-exhaustiveness are absent. According to settled case law,[2272] the literal meaning of a provision cannot be called into question by means of contextual or teleological interpretation if provision is clear and precise.[2273] Thus, the re-interpretation of Article 9 (1) GDPR through judicial action performed by the CJEU is not an option. Having established that new or revised legislation is unavoidable, I now elaborate how this could be done. Before doing so, I briefly reflect on the rationale for regulating special data. To avoid confusion, I use the term 'special data' to refer to data that are, in fact, listed and thus currently protected under the GDPR and 'sensitive data' for data that are currently *not specifically protected* under the GDPR (although they arguably should be).

According to the CJEU, the rationale to ensure enhanced protection for special data stems from their particular sensitivity. Processing of special data is likely to constitute a particularly serious interference with the fundamental rights to privacy and data protection.[2274] Recital 51 GDPR stresses the particularly sensitive nature of such data. According to AG Rantos, the object is to prevent significant risks for data subjects arising from the processing of special data, regardless of any subjective element such as the controller's *intention*. Thus, intentions do *not* play a role when determining whether personal data constitutes special data or not.[2275] In the view of SAs, specific protection for special data is needed because misuse may have more severe consequences for data subjects than misuse of 'regular' personal data.[2276] This is underscored by Recital 51 GDPR, which states that 'processing [of sensitive personal data] could create significant risks to the fundamental rights and freedoms'. Nevertheless, the approach to provide specific protection for certain categories of personal data is not undisputed.[2277]

In what I call the 'context objection', Bygrave claims that the sensitivity of personal data is context-dependent.[2278] In the 'use objection', Moerel and Prins argue that the sensitivity of personal data

[2271] Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 6 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.
[2272] Case C-220/03 *BCE* [2005] ECR I-10595 para 3; Case C-263/06 *Carboni e derivati* [2008] ECR I-1077 para 48; Case C-48/07 *Les Vergers du Vieux Tauves* [2008] ECR I-10627 para 44.
[2273] Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 7 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.
[2274] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 para 70; Case C-184/20, *OT* [2022] ECR I-601, para 126; Case C-136/17, GC and Others [2019] ECR I-773 para 44; Recital 51 GDPR.
[2275] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 paras 69-70; see also Opinion of AG Rantos para 41.
[2276] Art 29 Working Party, 'Advice paper on special categories of data ('sensitive data')' (20 April 2011) at 4.
[2277] Ludmila Georgieva, Christopher Kuner Commentary of Article 9 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 370.
[2278] Lee A. Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014) 165.

essentially depends on the specific use of personal data.[2279] In their view, the regime for special categories of personal data is no longer meaningful because it is becoming less and less clear which data are sensitive and that the focus should be on the use of data when determining sensitivity of processing.[2280] One of the examples they provide is the case of an email address, which in itself is not sensitive data, but in combination with a password becomes highly sensitive because many individuals use the same email and password to access different websites.[2281] Similarly, regulatory guidance stresses the importance of a more flexible approach to sensitive personal data because the context plays an important role in determining the sensitivity of a certain processing activity.[2282]

The 'context' and 'use' objections are valid, but they are not new. Already traveaux préparatoire relating to the DPD drafted in the 1990s point to the context and use objections.[2283] More importantly, the GDPR explicitly requires one to take the context into account when it comes to the processing of special data. Recital 51 GDPR states that special data merits specific protection because the *context* of their processing may create significant risks for data subjects. The reference to 'context' in this recital was added at an advanced stage of the legislative procedure and was not included in the European Commission's initial proposal.[2284] Thus, the legislator made a deliberate choice to recognise context as a relevant factor when it comes to the processing of special data. This is precisely what the CJEU did when ruling that also personal data which *indirectly* reveal special data are covered by Article 9 GDPR.[2285] In this case, it was possible to derive information with respect to the sex life or sexual orientation of the data subject from 'non-sensitive' personal data published on the Internet, i.e. name-specific data relating to the spouse, cohabitee or partner of that data subject.[2286] This ruling addresses the context and use objections: arguably non-sensitive personal data might become sensitive depending on its specific use and context.

According to US scholar Solove, the current approach with respect to special data is a dead end, and the only viable solution is to focus on use, harm and risk.[2287] According to his 'dead-end' objection,

[2279] Lokke Moerel, Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016) p 11 and 56 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 8 February 2024.
[2280] Ibid 11.
[2281] Ibid 56.
[2282] However, note that EU Supervisory Authorities do not seem to be fully aligned in this point; see Art 29 Working Party, 'Advice paper on special categories of data ('sensitive data')' (20 April 2011) at 9-10.
[2283] 'It is generally accepted that the right to privacy is endangered, *not* by the *contents* of personal data, *but* by the *context* in which the processing of personal data takes place.' Commission, 'Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data' COM (90) 314 final, explanatory memorandum p 35 <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/COMPLETETRAVEAU(ENGLISH)DPDIRECTIVE.pdf#page=1P> accessed 8 February 2024.
[2284] See Recital 41 at page 24 < https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf > accessed 8 February 2024.
[2285] Case C-184/20, *OT* [2022] ECR I-601.
[2286] Case C-184/20, *OT* [2022] ECR I-601 paras 117-128.
[2287] Daniel J Solove, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2024) Vol 11 No 4 Northwestern University Law Review 1081, 1083 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198> accessed 8 February 2024.

the special data categories are arbitrary and based on blurry lines. Moreover, in Solove's view, nearly all personal data are special due to the capabilities of powerful ML algorithms. Processing of non-sensitive personal data by means of ML can generate inferences about special data, which means that most controllers are processing vast amounts of special data in violation of the law.[2288]

Solove's dead-end objection completely ignores the rationale of EU law[2289] to specifically protect special data, which involve both prevention of harm *and* risks. According to the CJEU, a heightened standard of protection for special data is needed because this processing is likely to constitute a particularly serious interference with the fundamental rights to privacy and data protection.[2290] Obviously, interferences relate to both harm and risks. According to AG Rantos, the objective is to prevent *significant risks* for data subjects arising from the processing of special data.[2291] The connotation on risks for data subjects is also stressed in Recital 51 GDPR, which states that 'processing [of special data] could create significant risks to the fundamental rights and freedoms'. Thus, Article 9 GDPR proactively prevents harms *and* risks by prohibiting the processing of special data, unless an exception applies. Thus, contrary to what Solove claims in the dead-end objection, the prevention of harm and risks for data subjects *is* covered by the rationale to specifically protect special data.[2292] In addition, substantive fairness as introduced in Section 6.2 provides additional protection against harm and risk, as it focusses on whether the outcome of processing is fair. Therefore, what is left from Solove's 'dead-end' objection is the call to focus on the use, which ultimately boils down to the 'context' and 'use' objections. Moreover, Solove exaggerates when claiming that nearly all personal data is sensitive simply because inferences by means of ML *are possible*. He presumes that almost all controllers engage in such processing and oversimplifies processing performed by means of ML. Arguably, mainly controllers that have the technological know-how and sufficient financial resources engage in such processing, but not 'most organisations' as claimed in Solove's dead-end objection.[2293] Only controllers that *in fact* infer special data by means of ML need to comply with Article 9 GDPR. Solove's dead-end objection mentions powerful ML algorithms several times, but he ignores new types of highly sensitive personal data (e.g. emotion data, mental and neurodata) that can be generated by means of the various AI disciplines discussed in this thesis. Instead, Solove mentions rather trivial

[2288] Daniel J Solove, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2024) Vol 11 No 4 Northwestern University Law Review 1081, 1083, 1084 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198> accessed 8 February 2024.
[2289] Although he is a US scholar, Solove extensively discusses EU law in his contribution relating to the dead-end objection. The GDPR is mentioned 68 times, and Solove admits that the approach to regulating sensitive data stems from the EU. It can, therefore, also be expected that the EU's rationale to regulate sensitive data is acknowledged and discussed.
[2290] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 para 70; Case C-184/20, *OT* [2022] ECR I-601, para 126; Case C-136/17, GC and Others [2019] ECR I-773 para 44; Recital 51 GDPR.
[2291] Case C-252/21, *Meta Platforms Inc.* [2022] ECR I-704, Opinion of AG Rantos para 41.
[2292] Case C-252/21 *Meta Platforms Inc.* [2023] ECR I-537 para 70; Case C-184/20, *OT* [2022] ECR I-601, para 126; Case C-136/17, GC and Others [2019] ECR I-773 para 44; Case C-252/21, *Meta Platforms Inc.* [2022] ECR I-704, Opinion of AG Rantos para 41; Recital 51 GDPR.
[2293] Daniel J Solove, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2024) Vol 11 No 4 Northwestern University Law Review 1081, 1084 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198> accessed 8 February 2024.

examples, for example inferences concerning political beliefs or opinions, sexual orientation, ethnicity, health status and race derived from Facebook likes.[2294]

There are basically two possible approaches for new or revised legislation concerning the processing of special personal data. The first approach is to enumerate specific categories of special personal data ('current approach'). The second approach is to make the sensitivity of a certain processing dependent on the context and specific use of personal data ('contextual approach'). Obviously, both approaches have their (dis)advantages.

The contextual approach has the main advantage that it is quite flexible, as sensitivity depends on the use and context, not on the content of the personal data processed. For example, processing health data by insurance companies for the benefit of data subjects would not be considered sensitive, whereas processing health data to exclude data subjects from insurance coverage would be. In addition, the contextual approach would allow employers to launch initiatives to improve diversity and inclusion within the company. For example, employers could use unsupervised ML to detect correlations and patterns in data relating to the current workforce, which might be helpful to improve their businesses. The current approach makes such initiatives difficult when considering that none of the exceptions to the processing of sensitive data listed in Article 9 (2) GDPR is applicable in this case.
The main advantage of the contextual approach, i.e. flexibility, is simultaneously also a disadvantage. In my view, this approach gives controllers too much flexibility when considering the power imbalance between controllers and data subjects. Ultimately, it is the controller that determines the use of personal data by defining the purpose of processing. Controllers can define purposes with enough specificity and can demonstrate that such purposes are legitimate, meaning any purpose is valid under the GDPR.[2295] Hence, relying on the sensitive use of personal data is not suitable to actually prevent risks and harms for data subjects because controllers determine the use of personal data. They have considerable freedom when doing so and can be creative in defining it as a 'non-sensitive' use. In addition, it is rather difficult to determine precisely which types of use should be regarded as particularly harmful or risky. It is even more difficult to anticipate and foresee all imaginable harmful uses that might emerge in the future. This approach is questionable from the perspective of legal certainty, which notably constitutes one of the GDPR's legislative aims.[2296]

[2294] Daniel J Solove, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2024) Vol 11 No 4 Northwestern University Law Review 1081, 1099-1109 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198> accessed 8 February 2024.
[2295] Asia Biega, Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' (2021) Technology and Regulation 44, 49 <https://arxiv.org/abs/2101.06203> accessed 8 February 2024.
[2296] Recitals 7 and 13 GDPR.

The current approach is more convincing from the perspective of legal certainty, because the GDPR lists all types of special data in Article 9, and some are even defined.[2297] Additionally, it is more suitable because it starts from a general prohibition of processing special data. Controllers need to be able to rely on one of the exceptions in Article 9 (2) GDPR. The current approach is based on the rationale that there are specific types of personal data with an inherently sensitive nature as stressed by Recital 51 GDPR.[2298] When considering the inherently sensitive nature of mental data, neurodata and emotion data generated by AI, it should not play a role in which context or for which purpose such data are processed. *Mental data* refers to the processing of information relating to the mental states of individuals. Mental states comprise all conscious and non-conscious mental representations, events, processes and propositional attitudes, including thoughts, beliefs, emotions and moods, as well as the underlying psychological mechanisms (collectively referred to as 'mental states').[2299] Mental data are perceived to form the core of an individual's private sphere[2300] and are therefore of a particularly sensitive nature. *Neurodata* provide unique insights into people[2301] and their behaviour.[2302] Scholars have argued that neurodata are a particularly sensitive class of data due to their direct link with mental processes[2303] and the strong link to the individual's personhood.[2304] Also, *emotion data* have a strong link to personhood. Information regarding emotions is of sensitive and intimate nature[2305] because there is an inherent relationship between emotions and personhood[2306] and privacy is considered fundamental to the maintenance of human dignity and the boundary to one's personhood.[2307] Thus, neurodata, mental data and emotion data are of inherently sensitive nature and merit

[2297] Genetic data in Article 4 (13), biometric data in Article 4 (14) and health data in Article 4 (15) GDPR.
[2298] The following reasoning contained in preparatory documents for the DPD, on which Article 9 GDPR is built, holds still true. 'Certain categories of data which, by virtue of their *contents* – quite *irrespective* of the *context* in which they are *processed* – carry the risk of infringing the data subject's right to privacy' COM (90) 314 final, explanatory memorandum p 35 <https://resources.law.cam.ac.uk/cipil/travaux/data_protection/COMPLETETRAVEAU(ENGLISH)DPDIRECTIVE.pdf#page=1P> accessed 8 February 2024
[2299] Jan-Christoph Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination' in Andreas von Arnauld, Kerstin von der Decken, Mart Susi (eds) *The Cambridge Handbook of New Human Rights* (Cambridge University Press 2020) 30; Marcello Ienca, Gianclaudio Malgieri, 'Mental data protection and the GDPR' (2022) Vol 9 Iss 1 Journal of Law and the Biosciences 1, 4.
[2300] Dara Hallinan et al, 'Neurodata and Neuroprivacy: Data Protection Outdated?' (2014) Vol 12 Iss 1 Surveillance and Society 68 <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/neurodata/neurodata4> accessed 8 February 2024.
[2301] Neurodata are of highly personalised nature and allows for identification ('brain fingerprinting').
[2302] Brent J. Lance et al, 'Brain-Computer Interface Technologies in the Coming Decades' (2012) Vol 100 Proceedings of the IEE 1587.
[2303] Marcello Ienca, Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotech- nology' (2017) Vol 13 Iss 1 Life Science, Society and Policy 1, 14; Marcello Ienca, Karolina Ignatiadis, 'Artificial Intelligence in Clinical Neuroscience: Methodological and Ethical Challenges' (2020) Vol 11 Iss 2 AJOB Neuroscience 77-87; Rafael Yuste et al, 'Four ethical priorities for neurotechnolgies and AI' (2017) Vol 551 Nature 159-163.
[2304] Marcello Ienca, Roberto Andorno, 'Towards New Human Rights in the Age of Neuroscience and Neurotech- nology' (2017) Vol 13 Iss 1 Life Science, Society and Policy 1, 14.
[2305] Andrew McStay, 'Emotion AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy' (2020) Vol 7 Iss 7 Big Data & Society 1, 4.
[2306] Giovanni Stanghellini, René Rosfort, *Emotions and Personhood: Exploring Fragility – Making Sense of Vulnerability* (OUP 2013) 149.
[2307] William S Brown, 'Technology, Workplace Privacy and Personhood' (1996) Vol 15 Journal of Business Ethics 1237, 1243.

specific protection. It is therefore justifiable to maintain a 'sui generis' regime[2308] for such highly sensitive personal data. Letting it entirely up to the controllers to determine whether the envisaged use qualifies as sensitive, as in the contextual approach, is not a suitable solution.

To adjust the level of protection for special data to the harm or risk of harm as suggested in the dead-end objection seems unworkable in practice. Harms and risks are highly subjective, as they depend on the specific data subject concerned by the processing. What may constitute harm for one data subject might be different for another data subject. The same applies to the corresponding risks. Definitions of specific types of harm relating to the processing of special data are arguably too abstract to actually work in practice.[2309] By analogy, proving harm caused by the processing of personal data is inherently difficult. This is underscored by at least nine cases pending at the CJEU[2310] (at the time of writing beginning 2023) which address the compensation of non-material damages caused by GDPR infringements. According to a petition submitted to the Commission, the legislator failed to sufficiently specify when non-material damages exist and to name examples within the GDPR's recitals.[2311] This omission makes it rather difficult for data subjects to claim compensation for non-material damages because they carry the burden of proof. In its response to the petition, the Commission outlined that Recitals 75, 85 and 146 GDPR provide indications for the concept of non-material damages, and that this concept must be further clarified by national courts.[2312] Notably, Recitals 75 and 85 GDPR only mention examples of possible harms relating to *personal data breaches* as defined in Article 4 (12) GDPR. In addition, AG Campos Sánchez-Bordona seems to recognise the difficulty in determining exactly what constitutes harm and what not. He is 'in no doubt that there is a *fine line* between *mere upset* (which is not eligible for compensation) and *genuine* non-material damage (which is eligible for compensation)'. Likewise, he is aware of 'how complicated it is to *delimit*, in the *abstract*, the two categories and apply them to a particular dispute'.[2313] Arguably, it is exactly for these reasons that the legislator omitted to name examples of harm eligible for the compensation of non-material damages. Thus, the approach to adjust the level of protection for special data to the harm or risk of harm as suggested in the dead-end objection is unworkable in practice. Even the author of the dead-end objection admits that regulating use, harm and risk is a difficult road, fraught with complexity.[2314]

[2308] Koops suggests having sui generis regimes for types of data that have certain effects when they are processed see Bert-Jaap Koops, 'The trouble with European data protection law' (2014) Vol 4 No 4 International Data Privacy Law 250, 260.
[2309] Paul Ohm, 'Sensitive Information' (2015) Vol 88 Southern California Law Review 1125, 1147.
[2310] Cases C-340/21 *Natsionalna agentsia za prihodite*; C-300/21 *UI* [2022] ECR I-756*;* C-741/21 *Juris*; C-687/21 *Saturn Electro;* C-667/21 *Krankenversicherung Nordrhein;* C-189/22 *Scalable Capital;* C-182/22 *Scalable Capital* C-456/22 *Gemeinde Ummendorf*; C-590/22 *PS.*
[2311] Petition No 0386/2021 see <https://www.europarl.europa.eu/doceo/document/PETI-CM-699118_EN.pdf> accessed 8 February 2024.
[2312] Ibid.
[2313] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona para 116.
[2314] Daniel J Solove, 'Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data' (2023) George Washingto University Law School Draft Research Paper 5 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198> accessed 8 February 2024.

Instead of regulating based on harm, I suggest focussing on the compensation of non-material harm caused by GDPR infringements. Proving this and obtaining compensation according to Article 82 GDPR is extremely difficult for data subjects. This could be overcome by establishing a typology for non-material damages based on the nature of the infringed provision. Article 83 GDPR, which empowers SAs to impose administrative fines on controllers, contains a similar typology. The legislator seems to have weighed GDPR infringements normatively by setting up two different maximum amounts for fines. Infringements of principles and data subject rights can lead to fines of up to twenty million euros or 4% of a controller's annual worldwide turnover, while infringements of other GDPR provisions can lead to fines of up to ten million euros or 2% of a controller's annual worldwide turnover. This distinction indicates that infringements of principles and data subject rights are considered *more serious* than infringements of other provisions.[2315] Thus, the legislator provided an indication concerning the seriousness on an infringement in an abstract sense: the more serious the infringement, the higher the fine.[2316]

The same mechanism might be used to establish a typology for non-material damages. This typology puts a price on the infringement of GDPR provisions. The amount of non-material damages to be awarded for infringements of principles and data subject rights will be higher than for other GDPR infringements. Setting up this typology and embedding it in the GDPR would enable data subjects to *effectively* enforce their right to the compensation of non-material damages.[2317] Arguably, this will also have a deterrent effect on controllers because it facilitates collective actions pursued by bodies representing data subjects in order to obtain the compensation of non-material damages.[2318]

In my view, the current approach is suitable to *prevent* harm and risks arising from the processing of special data. It contains many layers of protection. Processing of such data is prohibited, unless an exception applies. In addition, processing of special data must always be supported by a legal basis[2319] and comply with other provisions[2320] of the GDPR.[2321] The fairness principle and its components listed in Table 6.3 in Section 6.2.2 form a particularly helpful layer of protection. The fairness components vulnerability, autonomy, non-discrimination and detrimental effects protect data subjects from *possible* harm. The controller's obligation to perform a Data Protection Impact Assessment (DPIA) for processing that is likely to result in a high risk for data subjects could be seen as another layer of

[2315] Article 29 Working Party, 'Guidelines on the application of administrative fines for the purposes of Regulation 2016/679' (WP 253, 3 October 2017) 9.
[2316] European Data Protection Board, 'Guidelines on the calculation of administrative fines under the GDPR' (Guidelines 4/2022, 16 May 2022) 16.
[2317] Article 82 (1) GDPR.
[2318] Article 80 (1) GDPR.
[2319] According to Article 6 GDPR; see also European Data Protection Board, 'Guidelines 3/2019 on the processing of personal data through video devices' (29 January 2020) at 17.
[2320] Such as principles for processing and other rules of the GDPR; see Recital 51 GDPR.
[2321] Ludmila Georgieva, Christopher Kuner Commentary of Article 9 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 374, 376.

protection. According to Article 35 (3) GDPR, such a DPIA is mandatory if the controller processes special categories of personal data on a large scale. Actual harm can then be compensated.

However, the current approach also has disadvantages as it may lead to over or under protection of special data.[2322] Overprotection occurs for instance when the processing of special data is not particularly sensitive and is carried out for the benefit of the data subject. This holds true when health data are processed by insurance companies for the benefit of data subjects or when employers process special personal data to improve diversity and inclusion within the company. Typical examples of under protection are mental data, neurodata and emotion data (Section 4.9.3). These highly sensitive types of data are underprotected because they are not included in the exhaustive list of special data according to Article 9 GDPR.

To sum up, the current approach to specifically regulate special personal data with an inherently sensitive nature is at least better than the alternatives suggested in the 'use', 'context' and 'dead-end' objections. However, this approach is far from perfect and has its disadvantages; for instance, it may lead to over-regulation.

6.3.2 Solution: Introducing a dynamic list for special data

Section 4.8.3 concluded that the approach of enumerating special categories of personal data exhaustively is not fit for purpose to address the challenges caused by AI as it cannot keep up with technological developments. To solve this problem, I suggest a revision of Article 9 GDPR, which contains a dynamic list of special personal data. More specifically, I suggest that the European Commission be empowered to adopt delegated acts for the purpose of updating the list of special personal data where necessary due to technological developments. If new information technologies facilitate processing of new types of sensitive personal data, the Commission can proactively add such new categories to the list. Likewise, the Commission is also empowered to remove categories of personal data from that list when the inherently sensitive nature of such data ceases to exist, for example, due to societal changes. When doing so, the Commission should consider the rationale for the increased standard of protection for special data. The rationale is to prevent particularly serious interferences with the fundamental rights to privacy and data protection[2323] as well as corresponding significant risks for data subjects.[2324] In order to prevent over-regulation, it could be considered to also empower the Commission to add exceptions applicable to the processing of special data if corresponding scientific evidence is available.

[2322] Paul Ohm, 'Sensitive Information' (2015) Vol 88 Southern California Law Review 1125, 1146; Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life* (Stanford Law Books 2010) 89-102.
[2323] Case C-184/20, *OT* [2022] ECR I-601, para 126; Case C-136/17, GC and Others [2019] ECR I-773 para 44; Recital 51 GDPR.
[2324] Recital 51 GDPR.

EU consumer law follows a similar approach[2325] in the Unfair Commercial Practices Directive (UCPD)[2326] as introduced in Section 6.2.1. In its annex, the UCPD contains a list with commercial practices which are regarded as unfair. However, this list can only be modified by revising the Directive, which makes it less feasible to anticipate quickly-evolving technological change.[2327]

My suggested solution is comparable to the AI Act's compromise text[2328] concerning high-risk systems referred to in Article 6 (2) and Annex III. According to Article 7 (1), the Commission is empowered to add or modify use-cases of high-risk AI systems contained in Annex III.[2329] A similar approach has been adopted in the Digital Services Act ('DSA').[2330] Article 87 DSA empowers the Commission to adopt delegated acts, for example, by laying down the methodology for calculating the number of average monthly active users[2331] or by laying down rules concerning audits to be pursued under the DSA.[2332] In order to proactively counter the argument that the Commission should not be empowered to enact law, I suggest including a similar provision as contained in Article 87 (6) DSA. This provision foresees that delegated acts by the Commission only enter into force if neither the European Parliament nor the Council raise objections.

The proposed solution provides a basic layer of protection for special personal data, i.e. a default prohibition of processing, and is able to address technological developments. In addition, it comes with legal certainty for all the actors involved in the processing of personal data: the controllers, the data subjects, the supervisory authorities and, in litigious cases, the Courts. The components of the fairness principle outlined in Section 6.2.2 constitute the second layer of protection. In particular, the components vulnerability, autonomy, non-discrimination and detrimental effects protect data subjects from possible harm.

I acknowledge that the suggested solution is far from perfect. However, for now, it seems at least *better* than the alternatives suggested in the 'use' and 'dead-end' objections. There are certainly disadvantages, the risk of over-regulation in particular. For example, it can be doubted whether the Commission would be willing to also remove special categories from the list and not only add new

[2325] Although with a different rationale, i.e. consumer law.
[2326] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market OJ L 149/22 furtheron 'UCPD'.
[2327] In May 2022, the Commission launched a fitness check on EU consumer law, focussing on digital fairness. This fitness check determines whether additional legislative action is needed to ensure a high level of consumer protection in the digital environment. See <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en> accessed 8 February 2024.
[2328] On 2 February 2024, the Committee of the Permanent Representatives of the Governments of the Member States to the European Union unanimously approved the compromise text of the AI Act resulting from the trilogue negotiations see < https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf > accessed 8 February 2024.
[2329] Ibid.
[2330] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L277/1 'Digital Services Act' (DSA).
[2331] Article 33 (3) DSA.
[2332] Article 37 (7) DSA.

categories. It also remains to be seen how the approach taken in the DSA plays out in practice. Nonetheless, I think that the suggested solution is still better than the available alternatives.

6.3.3 Conclusion

The legal solution to solve the mental data problem[2333] consists of a revision of Article 9 GDPR. This revision should introduce a dynamic list of special personal data. This list overcomes the current problem related to the approach to exhaustively enumerate special categories of personal data. The current approach is not fit for purpose to address the challenges caused by AI as it does not keep up with technological developments. In my suggested solution, the European Commission is empowered to adopt delegated acts to update the list of special personal data where needed in light of technological developments. This solution is flexible enough to address this and comes with legal certainty for all actors involved.

6.4 Confidentiality – the communication surveillance problem

The communication surveillance problem (Type 3)
ML, NLP and AC facilitate the surveillance of both human-machine and interpersonal communication. Major tech companies that offer human-machine communication services, such as virtual assistants, may easily intercept and otherwise process such communication. Providers of these services do not fall under the strict regime of Article 5 (1) ePD, which regulates the confidentiality of communications. This creates a significant gap in legal protection and outlines that the ePD is not fit for purpose to ensure the confidentiality of both interpersonal and human-machine communication.

6.4.1 Setting the scene

AI and people's interactions with it do not fit neatly into paradigms of communication theory that have focussed on human–human communication.[2334] The same can be said about the legal protection with respect to the confidentiality of human-machine communication. The AI discipline natural language processing (NLP) provides powerful means to analyse voice and speech data obtained by means of human-machine communications, in particular when combined with classification techniques adopted in the AI discipline machine learning (ML). With NLP and ML, rather sensitive information can be derived from human speech and other acoustic elements in recorded audio. In addition to the linguistic content of speech, a speaker's voice characteristics and manner of expression may contain a rich array of personal information, including clues with regard to the speaker's biometric identity, personality, physical traits, geographical origin, level of intoxication and sleepiness,

[2333] In addition to other legal problems that are inextricably linked to it (emotion data, location data and neurodata problems).
[2334] Andrea L Guzman, Seth C Lewis, 'Artificial intelligence and communication: A Human-Machine Communication agenda' (2020) Vol 22 Iss 1 New Media & Society 70-86.

age, gender, health condition and even an individual's socioeconomic status.[2335] In addition, speech-based emotion recognition systems powered by the AI discipline affective computing (AC) measure and quantify emotions of a person by observing speech signals of this person.[2336] Research has demonstrated specific associations between emotions such as fear, anger, sadness, joy and features of speech such as pitch, voice level and speech rate.[2337] Amazon's patented technology enabling the virtual assistant Alexa to recognise the user's emotional state derived from the user's voice constitutes a practical example of this (see Section 4.9.3).[2338] Likewise, tech companies may intercept interpersonal communication. For example, a former Apple employee revealed that he had listened to hundreds of Siri recordings every day, including unintended recordings, for the purpose of quality control.[2339] These recordings concerned sensitive interpersonal communications such as discussions between doctors and patients, business deals, seemingly criminal acts and sexual encounters.[2340] This is not an exception, and press coverage points to similar practices at Google[2341] and Amazon[2342] (see Section 4.9.3). In addition, both human-machine and interpersonal communications might be intercepted in the context of virtual assistant services for the purpose of serving targeted ads.[2343]

The protection gap regarding the confidentiality of human-machine communication and interpersonal communication captured in the context of virtual assistant services can only be solved by means of new or revised legislation. The literal interpretation of Article 5 (1) ePD that regulates the confidentiality of communications is clear: The provision does not apply to providers of virtual assistant services such as Amazon, Google and Apple given that these services do not constitute an electronic communication service (ECS) as defined in European Electronic Communications Code (EECC).[2344] The new definition of an ECS covers three types of services: (i) Internet access services, (ii)

[2335] 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) 242.
[2336] Chi-Chun Lee et al, 'Speech in Affective Computing' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 171.
[2337] Christina Sobn and Murray Alpert, 'Emotion in Speech: The Acoustic Attributes of Fear, Anger, Sandess, and Joy' (1999) Vol 28 No 4 Journal of Psycholinguistic Research, 347.
[2338] Huafeng Jin, Shuo Wang 'Voice-Based Determination of Physical and Emotional Characteristics of Users' US Patent Number US 10096319 B1 (Assignee: Amazon Technologies, Inc.) October 2018 <https://patentimages.storage.googleapis.com/f6/a2/36/d99e36720ad953/US10096319.pdf> accessed 8 February 2024.
[2339] Alex Hern, 'Apple contractors regularly hear confidential details on Siri recordings' *The Guardian* (London, 26 July 2019) < https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings > accessed 8 February 2024.
[2340] Alex Hern, 'Apple contractors regularly hear confidential details on Siri recordings' *The Guardian* (London, 26 July 2019) < https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings > accessed 8 February 2024.
[2341] Tom Simonite, 'Who's Listening When You Talk to Your Google Assistant?' *Wired* (New York, 10 July 2019) <https://www.wired.com/story/whos-listening-talk-google-assistant/> accessed 8 February 2024.
[2342] Alex Hern, 'Amazon staff listen to customers' Alexa recordings, report says' *The Guardian* (London, 11 April 2019) <https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says> accessed 8 February 2024.
[2343] Joseph Cox, 'Marketing Company Claims That It Actually Is Listening to Your Phone and Smart Speakers to Target Ads' *404 Media* (United States, 14 December 2023) <Marketing Company Claims That It Actually Is Listening to Your Phone and Smart Speakers to Target Ads (404media.co)> accessed 8 February 2024.
[2344] Directive (EU) 2018/1972 of the European Parliament establishing the European Electronic Communications Network OJ L 321/36 further on 'EECC'.

interpersonal communications services and (iii) services consisting wholly or mainly in the conveyance of signals.[2345] It also includes over-the-top (OTT) services such as VoIP[2346] solutions, messaging services and web-based email services, which are functionally equivalent to traditional voice telephony and text message services.[2347] With regard to requirement (i), it is clear that virtual assistant services do not constitute Internet access services.

Concerning requirement (ii), an interpersonal communication service is defined as a 'service normally provided for remuneration that enables *direct interpersonal and interactive exchange of information* via *electronic communications networks* between a *finite number of persons*, whereby the persons initiating or participating in the communication determine the recipient(s) and do not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service'.[2348] Recital 17 EECC clarifies what is meant with interpersonal communication: communications between *natural persons*. Communications involving legal persons fall within the definition only to a limited extent, for instance if natural persons act on behalf of those legal persons.[2349] Thus, human-machine communications fall outside the scope of interpersonal communication services as defined in Article 2 (5) EECC.

Concerning requirement (iii), all that matters concerning the conveyance of signals is that a service provider is *responsible* vis-à-vis the end-users for *transmission* of the *signal* which ensures that they are supplied with the service to which they have subscribed.[2350] In the case of web-based services, it is the Internet Access Providers (IAPs) and the *operators* of the *various networks* of which the *open web* is based that convey the signals necessary for the functioning of web-based services.[2351] Providers of web-based services can participate in the conveyance of signals, for example, by means of uploading data packets to the Internet or by splitting messages into data packets. According to the CJEU, however, this is not sufficient to be regarded as an ECS consisting 'wholly or mainly in the conveyance of signals on electronic communications networks'.[2352]

Thus, none of the three types of services (i-iii) contained in the definition of an ECS align with human-machine communication services, such as virtual assistants. As outlined in Section 6.3.1, literal (textual) interpretation is the prevailing method of interpretation if the provision to be interpreted is clear

[2345] Article 2 (4) EECC.
[2346] VoIP solutions, for example, enable individuals to call via computer without the call being routed on to a number in the regular telephony numbering plan.
[2347] Recital 15 EECC.
[2348] Article 2 (5) EECC, emphasis added.
[2349] It seems unclear what the phrase 'or are at least involved on one side of the communication' contained in Recital 15 precisely means.
[2350] Case C-475/12, *UPC* [2014] ECR I-285 para 43.
[2351] Case C-193/18, *Google LLC* [2019] ECR I-498 para 36.
[2352] Case C-193/18, *Google LLC* [2019] ECR I-498 para 36.

and precise.[2353] The definition of an ECS according to Article 2 (4) EECC is clear and the three types of services covered by it are defined further in case law,[2354] the EECC[2355] or elsewhere.[2356] According to settled case law,[2357] the literal meaning of a provision cannot be called into question by means of contextual or teleological interpretation if the provision is clear and precise.[2358] Thus, re-interpretation of the notion ECS and the three types of services covered by it through judicial action performed by the CJEU is not an option. Having established that the communication surveillance problem can only be solved by means of new or revised legislation, I now discuss how such legislation might look.

To be clear, and as explained in Section 4.9, providers of human-machine communication services need to adhere to the GDPR when processing personal data. Thus, only because providers of human-machine communication services fall outside the scope of the ePD does not lead to a complete lacuna in legal protection. However, the provisions of the GDPR are less strict than Article 5 (1) ePD. As outlined in Section 4.9.3, human-machine communications deserve the same level of confidentiality as interpersonal communications. This is due to the sensitivity of such communications, as explained in the first paragraph of this section.

6.4.2 Solution: Regulating human-machine communication

The proposed ePrivacy Regulation,[2359] which is still subject to political negotiations, seems well suited to solve this problem. The proposed ePrivacy Regulation sets rules regarding the protection of the fundamental right to privacy and particularly the confidentiality of communications.[2360] Unfortunately, neither the initial proposal nor the subsequent amendments regulate the confidentiality of human-machine communication. The initial proposal clarifies that the ePrivacy Regulation also applies to the transmission of machine-to-machine communications to ensure full protection of the right to privacy and confidentiality of communications.[2361] The proposal completely ignores human-machine communications and therefore, the communication surveillance problem essentially remains in the initial proposal for the ePrivacy Regulation. Instead of providing an analysis of the initial proposal and subsequent amendments, I propose specific provisions that can fill the current protection gap.

[2353] Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 6 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.
[2354] Case C-193/18, *Google LLC* [2019] ECR I-498 para 36; Case C-475/12, *UPC* [2014] ECR I-285 para 43;
[2355] Interpersonal communications service is defined in Article 2 (5) EECC.
[2356] Internet access service is defined in point (2) of the second paragraph of Article 2 Regulation (EU) 2015/2120.
[2357] Case C-220/03 *BCE* [2005] ECR I-10595 para 3; Case C-263/06 *Carboni e derivati* [2008] ECR I-1077 para 48; Case C-48/07 *Les Vergers du Vieux Tauves* [2008] ECR I-10627 para 44.
[2358] Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 7 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.
[2359] Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM (2017) 10 final 'Proposal ePrivacy Regulation'
[2360] Article 1 Proposal ePrivacy Regulation.
[2361] Recital 12 Proposal ePrivacy Regulation.

First, the future ePrivacy Regulation should clarify that the confidentiality of communication also applies to human-machine communication and that processing of this is only allowed in specific circumstances. Therefore, I suggest including the following or similar provision:

Article y Confidentiality of human-machine communications

(1) Human-machine communications shall be confidential. Any interference with human-machine communications, such as listening, tapping, storing, monitoring, scanning, intercepting or other kinds of interception and surveillance that amount to the processing of human-machine communications, by persons other than end-users, shall be prohibited, except on the following grounds:

(a) Processing is strictly necessary for the sole purpose of facilitating human-machine communication explicitly initiated by the end user; or

(b) The end user has explicitly consented to the processing for one or more explicit purposes.

(2) The prohibition enshrined in paragraph 1 also applies to communication between natural persons captured in the context of human-machine communication.

Paragraph 1 of this proposed article sets the general rule that surveillance of human-machine communication and any other kind of processing is prohibited unless specifically permitted in the ePrivacy Regulation. According to my proposal, processing of human-machine communication is first and foremost permitted if this is strictly necessary for the sole purpose of facilitating human-machine communication expressly initiated by the end user. The term 'strictly necessary' is used to limit this processing. A corresponding recital should clarify that purposes such as quality control, advertisement, emotion detection, drawing inferences from captured recordings of human-machine communications are not 'strictly necessary' to facilitate human-machine communication. In my view, such processing should be subject to consent from the end user according to lit b of paragraph 1. To stipulate in a recital that advertisement is not strictly necessary to facilitate human-machine communication might be superfluous at first sight. Nonetheless, I suggest including this purpose as 'not strictly necessary' because companies are rather innovative when interpreting 'necessity'.[2362] In addition, and as explained in Section 5.5.1, the technology for targeted advertisement facilitated by virtual assistant services is readily available, for example, Amazon's US patent 'Keyword Determinations from Voice Data'.[2363] Drawing inferences from recorded human-machine communication by means of ML and NLP may lead to profiling of the end user and reveal a rich array of personal information, including clues with respect to the speaker's biometric identity, personality, physical traits, geographical origin,

[2362] Think, for example, about Meta, which claims that targeted advertisement is strictly necessary for the performance of the contract between Meta and the Facebook user see Case C-446/21.

[2363] 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.

level of intoxication and sleepiness, age, gender, health condition and even an individual's socioeconomic status.[2364]

Likewise, processing human-machine communication for the purpose of emotion detection should require the consent of the end user, mainly due to the sensitive nature of data derived by AC (see Section 4.8.3). As indicated in Section 6.4, emotion detection systems for virtual assistants already exist. For example, Amazon's patented technology enables Alexa to recognise the user's emotional state derived from the user's voice.[2365] Other purposes such as improvement of services and quality control, should also be subject to the consent of the end user because all recordings might contain highly sensitive information. A former Apple employee revealed that he had listened to hundreds of Siri recordings every day for the purpose of quality control. These recordings concerned sensitive interpersonal communications such as discussions between doctors and patients, business deals, seemingly criminal acts and sexual encounters.[2366] This is not an exception, and press coverage points to similar practices at Google[2367] and Amazon (see Section 4.9.3).[2368]

The term 'explicitly initiated' included in lit a) contained in the first paragraph of proposed Article *y* prevents accidental recordings and other kinds of unsolicited processing of human-machine communication. Accidental recordings are common in virtual assistant services[2369] and occur when virtual assistants activate, transmit and/or record audio from their environment when the wake word is *not* spoken.[2370] Such recordings are caused by accidental triggers, i.e. sounds that wrongfully trigger virtual assistants, and they occur within the whole range of virtual assistants available on the market, including Amazon Alexa, Google Assistant and Siri. Researchers conducted a comprehensive analysis of accidental triggers in eleven smart speakers from eight different manufacturers and have found hundreds of such accidental triggers. The researchers automated the process for finding accidental triggers and measured their prevalence using everyday media such as TV shows, news and other kinds

[2364] 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) 242.
[2365] Huafeng Jin, Shuo Wang 'Voice-Based Determination of Physical and Emotional Characteristics of Users' US Patent Number US 10096319 B1 (Assignee: Amazon Technologies, Inc.) October 2018 <https://patentimages.storage.googleapis.com/f6/a2/36/d99e36720ad953/US10096319.pdf> accessed 8 February 2024.
[2366] Alex Hern, 'Apple contractors regularly hear confidential details on Siri recordings' *The Guardian* (London, 26 July 2019) < https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings > accessed 8 February 2024.
[2367] Tom Simonite, 'Who's Listening When You Talk to Your Google Assistant?' *Wired* (New York, 10 July 2019) <https://www.wired.com/story/whos-listening-talk-google-assistant/> accessed 8 February 2024.
[2368] Alex Hern, 'Amazon staff listen to customers' Alexa recordings, report says' *The Guardian* (London, 11 April 2019) <https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says> accessed 8 February 2024.
[2369] Nathan Malkin et al, 'Privacy Attitudes of Smart Speaker Users' (2019) Iss 4 Proceedings on Privacy Enhancing Technologies 250, 252.
[2370] Daniel J Dubois et al, 'When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers' (2020) Iss 4 Proceedings on Privacy Enhancing Technologies 255-276.

of audio datasets.[2371] Accidental recordings are problematic because conversations and other audio captured are sent over the Internet and subsequently stored on remote servers, [2372] often in the cloud.[2373] Incidents[2374] reveal that accidental recordings potentially include sensitive data and might be shared with third parties.[2375] An Alexa user listened to four years of his Alexa archive and found thousands of fragments of his life, including sensitive conversations such as medication-related family discussions.[2376]

Paragraph 2 of this proposed article is necessary because processing in the context of virtual assistants and similar services captures not only human-machine communications, but also interpersonal communications. Many of the examples mentioned in the previous paragraph in fact relate to recorded communications between natural persons, such as members of the household, visitors etc. When virtual assistant services are used by means of a smartphone app, basically every communication between the end user and any other natural person might be recorded, intentionally or accidentally. These recordings might be sensitive and include conversations between doctors and patients, business partners, criminals and sex partners.[2377] Therefore, communications between natural persons also should be confidential.

For the sake of legal certainty, I also suggest including a (broad) definition of human-machine communication in the ePrivacy Regulation. This definition could be worded as follows:

Article x (00) lit (z)
Human-machine communication means any information, irrespective of its form or content, relating to human-machine interactions facilitated via electronic communications networks.

[2371] Lea Schönherr et al, 'Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers' (2020) at 1 <https://arxiv.org/pdf/2008.00508.pdf> accessed 8 February 2024.
[2372] Daniel J Dubois et al, 'When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers' (2020) Iss 4 Proceedings on Privacy Enhancing Technologies 255-276.
[2373] Lea Schönherr et al, 'Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers' (2020) at 2 <https://arxiv.org/pdf/2008.00508.pdf> accessed 8 February 2024.
[2374] Tim Verheyden et al, 'Hey Google, are you listening?' *VRTB* (Brussels 10 July 2019) <https://www.vrt.be/vrtnws/en/2019/07/10/google-employees-are-eavesdropping-even-in-flemish-living-rooms/ > accessed 8 February 2024; Artem Russakovskii, 'Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7 [Update x2]' (2017) <https://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247/> accessed 8 February 2024.
[2375] Daniel J Dubois et al, 'When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers' (2020) Iss 4 Proceedings on Privacy Enhancing Technologies 255.
[2376] Geoffrey A Fowler, 'Alexa has been eavesdropping on you this whole time' *The Washington Post* (Washington, 6 May 2019) <https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/> accessed 8 February 2024.
[2377] Alex Hern, 'Apple contractors regularly hear confidential details on Siri recordings' *The Guardian* (London, 26 July 2019) <https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings> accessed 8 February 2024; Alex Hern, 'Apple contractors regularly hear confidential details on Siri recordings' *The Guardian* (London, 26 July 2019) < https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings > accessed 8 February 2024; Tom Simonite, 'Who's Listening When You Talk to Your Google Assistant?' *Wired* (New York, 10 July 2019) <https://www.wired.com/story/whos-listening-talk-google-assistant/> accessed 8 February 2024; Alex Hern, 'Amazon staff listen to customers' Alexa recordings, report says' *The Guardian* (London, 11 April 2019) <https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says> accessed 8 February 2024.

The proposed definition is intentionally drafted broadly and is suited to cover all kinds of human-machine communication, including virtual assistant services, smart homes services and any possible future means of human-machine communication. Because it covers information regardless of its form or content, it applies to communication in the form of speech, text, video and any other means of current and future communication. In addition, I have refrained from including the requirement of remuneration of services that facilitate human-machine communication. Making the protection of such communication dependent on remuneration, like in the case of information society services,[2378] is the wrong approach, in particular when considering that individuals often tend to use services that are 'free of charge', while in fact 'paying' with their personal data. The apps for virtual assistant services offered by the major actors in the field, namely, Apple, Amazon and Google can all be downloaded for smartphones, free of charge.[2379] Users of these virtual assistant services might need to purchase hardware in case they wish to have dedicated 'smart speakers'[2380] at home, but the virtual assistant service itself remains free of charge. Therefore, the remuneration requirement would prevent legal protection for human-machine communications.

Additionally, and for the sake of legal certainty, the material scope of the initially proposed ePrivacy Regulation[2381] should be extended as follows (underlined text):

This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services, <u>human-machine communications</u> and to information related to the terminal equipment of end-users.

The suggested (extended) scope of the ePrivacy Regulation makes clear that this piece of legislation applies to human-machine communications regardless of whether the provider facilitating such communication qualifies as an ECS. This closes the current gap of protection. Notably, within the initial proposal, the same approach has been taken in terms of information relating to the terminal equipment of end-users.[2382]

[2378] Article 1 (1) Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services ('Information Society Services Directive'); Case C-62/19 *Star Taxi App SRL* [2020] ECR I-980 paras 41-48; Case C-390/18 *X* [2019] ECR I-1112 paras 39-49.
[2379] See <https://smartgeekhome.com/how-much-does-alexa-cost/>; <https://www.makeuseof.com/tag/what-is-google-assistant/>; <https://appstorechronicle.com/what-does-siri-cost> accessed 8 February 2024.
[2380] Parker Hall, 'The Best Smart Speakers With Alexa, Google Assistant, and Siri' *Wired* (New York, 27 September 2022) <https://www.wired.com/story/best-smart-speakers/> accessed 8 February 2024.
[2381] Article 2 Proposal ePrivacy Regulation.
[2382] The material scope stipulated in Article 2 Proposal ePrivacy Regulation explicitly mentions 'information related to the terminal equipment of end-users', which is a novum compared to the current scope defined in Article 1 ePD.

6.4.3 Conclusion

In this section, I have outlined that the legal solution to solve the communication surveillance problem consists of two new provisions in the future ePrivacy Regulation. The first new provision regulates the confidentiality of human-machine communication. According to this provision, the surveillance of human-machine communication is prohibited unless it is specifically permitted, i.e. if processing of human-machine communication is strictly necessary to facilitate such communication or if the user has explicitly provided consent. The second proposed provision defines human-machine communication broadly. For the sake of legal certainty, I also suggest extending the scope of the future ePrivacy Regulation by specifically including human-machine communication. Together, these provisions solve the current gap of protection regarding the confidentiality of human-machine communication.

6.5 Right of access – the trade secrets problem

The trade secrets problem (Type 2)
Trade secret protection under the TSD covers AI itself, as well as output generated by the AI system, including personal data relating to emotional states and life expectancy predictions. When data subjects invoke their right to obtain a copy of personal data undergoing processing according to Article 15 (3) GDPR, controllers are likely to argue that disclosure of the output generated by the AI system infringes their trade secrets and restrict access to such personal data in accordance with Article 15 (4) GDPR. Consequently, data subjects cannot enforce their right to obtain a copy of their personal data.

6.5.1 Setting the scene

The right of access is arguably the most important data subject right. The CJEU repeatedly stressed the relevance of this right as a prerequisite to other data protection rights.[2383] Article 15 (3) GDPR, which forms part[2384] of this highly important data subject right, empowers the data subject to obtain a copy of the personal data undergoing processing. As mentioned in Section 3.3.4.1, the concept of a 'copy' is not defined in the GDPR. The CJEU ruled that a 'copy' refers to the 'faithful reproduction or transcription' of an original. A purely general description of the data undergoing processing or a reference to categories of personal data does not correspond to that definition.[2385] In addition, the right to obtain a copy not only includes personal data collected by the controller, but also information

[2383] Case C-579/21, *Pankki S* [2023] ECR I-501 paras 56-58; Case C-487/21, *F.F.* [2022] ECR I-1000 paras 34-35; Case C-434/16, *Nowak* [2017] ECR I-994 para 57; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44; Case C-553/07 *Rijkeboer* [2009] ECR I-03889, para 51.
[2384] Case C-487/21, *F.F.* [2022] ECR I-1000 para 30.
[2385] Case C-487/21, *F.F.* [2022] ECR I-1000 para 21.

resulting from the processing of personal data, for example, a credit score.[2386] Both the CJEU and AG Pitruzella hesitated to clarify what is meant with 'faithful'. Dictionaries describe this notion as 'true and accurate; not changing anything'[2387] and 'true or not changing any of the details, facts, style, etc. of the original'.[2388] The copy must enable the data subject to effectively exercise its right of access in full knowledge of all personal data undergoing processing, including personal data *generated* by the *controller*.[2389] This is only possible if data subjects receive a faithful reproduction in intelligible form of the personal data requested, and *not only* a list with the categories of personal data, as in the case of Article 15 (1) lit b GDPR.

Copies empower data subjects to achieve the aims of the right of access, which includes to 'be aware of, and verify the lawfulness of processing'[2390] and to obtain 'the rectification, erasure or blocking' [2391] of personal data. For example, enforcing the right to rectification necessitates assessing the accuracy of any given piece of personal data. Such an assessment, however, is only possible if the data subject has access to a copy of the actual personal data processed by the controller. Being aware of the mere category of personal data undergoing processing is insufficient for this assessment, because categories are too imprecise. As an example, to assess whether the controller spells the data subject's name correctly requires actual access to the data subject's name and obviously, the mere category 'name' is insufficient. The same applies to personal data generated by means of AI, such as the specific emotional state detected by the AI system or topics of interests ascribed to a data subject inferred by means of ML (pattern detection) or other outcomes of profiling.

Article 15 (4) GDPR states that the right to obtain a copy of the personal data processed should not adversely affect the rights and freedoms of others, which includes personal data generated by AI that fall under within the broad scope of protection under the TSD.[2392] Rights and interests must be balanced against one another. According to the CJEU, a 'fair balance' must be struck between the various fundamental rights protected by the EU legal order and any restriction on those rights must comply with the principle of proportionality.[2393] The trade secrets problem will also not be solved when the controller provides the data subject with redacted documents, as regulatory guidance suggests.[2394] As

[2386] Case C-487/21, *F.F.* [2022] ECR I-1000, para 26.
[2387] See <https://www.oxfordlearnersdictionaries.com/definition/english/faithful?q=faithful> accessed 8 February 2024.
[2388] See < https://dictionary.cambridge.org/dictionary/english/faithful > accessed 8 February 2024.
[2389] Case C-487/21, *F.F.* [2022] ECR I-1000 paras 26, 39; see also the opinion of AG Pitruzella paras 45, 70.
[2390] Recital 63 GDPR.
[2391] Case C-487/21, *F.F.* [2022] ECR I-1000 para 21; see also the opinion of AG Pitruzella paras 45, 70; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44.
[2392] Paul B de Laat, 'Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?' (2022) Vol 24 Iss 1 Ethics and Information Technology 1, 16.
[2393] Case C-275/06 *Promusicae* [2008] ECR I-00271 paras 65, 68.
[2394] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 163.

personal data themselves may constitute trade secrets, the controller could redact them, which is not helpful for the data subject and detrimental to the objectives[2395] of Article 15 GDPR.

As outlined in Section 5.6.2, the rule of non-prevalence constitutes the starting point for the balancing exercise. Based on CJEU case law, the outcome of the balancing exercise might essentially favour both the data subject's fundamental right to data protection and commercial interests pursued by the controller. I refer to trade secrets as commercial interests because commercial value constitutes one of the requirements when assessing whether information qualifies as a trade secret under Article 2 (1) TSD. Case law of the CJEU indicates that the protection of IP rights may prevail over the protection of personal data.[2396] The CJEU considered that the obligation to communicate personal data, for the purpose of ensuring effective protection of copyrights, of private persons in civil proceedings is eligible to strike a fair balance between the protection of IP rights and the fundamental right to data protection.[2397] Also, AG Pikamäe stresses that the legislator clearly did not contemplate sacrificing the fundamental right to intellectual property for the benefit of the fundamental right to data protection or the other way around. Rather, the legislator intended a fair balance between these two rights.[2398] However, the CJEU clarified that a fair balance requires particular consideration of the interests of the data subject. In the words of the CJEU, this fair balance 'may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life'.[2399] It is thus not excluded that the CJEU favours the data subject's fundamental right to data protection when balancing it with the controller's commercial interest in the form of a trade secret.

According to the CJEU, the balancing of opposing rights and interests, i.e. IP rights/trade secrets versus the fundamental right to data protection, depends on the *specific circumstances of the case*.[2400] Obviously, this conclusion is not satisfactory, nor does it provide legal certainty. I think it is questionable whether 'fair balancing' is the proper solution here. When considering the highly important role of the right to obtain a copy of the personal data processed and the consequences arising from the restriction of this right, in particular for other data subject rights, the trade secrets problem must be solved differently. I now discuss what this solution could look like.

[2395] Case C-487/21, *F.F.* [2022] ECR I-1000 paras 33-35.
[2396] Case C-597/19 *Telenet BVBA* [2021] ECR I-492 para 132; Case C-580/13 *Stadtsparkasse Magdeburg* [2015] ECR I-485 paras 28-41; C-461/10 *Bonnier Audio AB* [2012].
[2397] See Case C-264/19 *YouTube LLC* [2020] ECR I-542 paras 37-38; C-461/10 *Bonnier Audio AB* [2012] paras 57-60;
[2398] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 55.
[2399] Case C-131/12, *Google Spain* [2014] ECR I-317 para 81.
[2400] Case C-597/19 *Telenet BVBA* [2021] ECR I-492 para 111; Case C-13/16 *Rīgas* [2017] ECR I-336 para 31.

6.5.2 Solution: Introducing a new exception in the TSD

Many concerns have been raised with respect to the clash of trade secrets and the right of access in the context of AI.[2401] This is mainly due to the breadth of trade secrets: Any detail of algorithmic processing may be declared as a trade secret by the controller, including personal data generated by AI.[2402] Recital 2 TSD acknowledges that personal data might fall within the scope of information covered as trade secrets by mentioning 'information on customers'. In this very specific case of obtaining a copy of personal data under the right of access, I suggest eliminating the balancing exercise described in Section 6.5.1 and partially restrict trade secret protection. Perhaps the term 'restricting' is not completely accurate. Rather, my approach is to avoid that controllers exploit trade secret protection when data subjects exercise their right to obtain a copy of personal data undergoing processing. I use the term 'exploit' because, in my view, providing data subjects with a copy of their personal data is unlikely to harm the interests of the controller and the ability to compete.

As outlined in Section 5.6, three cumulative criteria must be met to trigger trade secret protection under the TSD. To qualify as trade secret according to Article 2 TSD, the information must be *secret*, have *commercial value* due to its secrecy and shall be subject to *reasonable steps to keep it secret*. It has been suggested to interpret the notion of commercial value as simply referring to the trade secret holder's ability to compete.[2403] However, I deem this interpretation too narrow when consulting the recitals of the TSD as the trade secret holder's ability to compete is simply one of the various ways how interests may be harmed. Protected information or knowledge has commercial value in the sense of the TSD, for example, when its unlawful acquisition, use or disclosure is likely to *harm the interests of the person lawfully controlling it*, in that it undermines that person's business or financial interests, strategic position or ability to compete.[2404] Misappropriation of trade secrets could also lead to costs for internal investigations, increased costs for protective measures and costs for prosecuting and litigating.[2405]

The acquisition, use and disclosure of trade secrets can either be lawful or unlawful under the TSD. I doubt that it is possible to speak of an unlawful disclosure of a trade secret in the context of a data subject's access request to receive a copy of the personal data undergoing processing. Article 3 (2)

[2401] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 608; Gianclaudio Malgieri, 'Trade Secrets v. Personal Data: A Possible Solution for Balancing Rights' (2016) Vol 6 No 2 International Data Privacy Law 102, 113-114; Paul B de Laat, 'Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?' (2022) Vol 24 Iss 1 Ethics and Information Technology 1, 9.
[2402] Paul B de Laat, 'Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?' (2022) Vol 24 Iss 1 Ethics and Information Technology 1, 9.
[2403] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 415.
[2404] Jens Schovsbo, 'The Directive on trade secrets and its background' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 14.
[2405] Baker McKenzie, 'Study on Trade Secrets and Confidential Business Information in the Internal Market' (MARKT/2011/128/D) (2013), 129 <https://single-market-economy.ec.europa.eu/publications/study-trade-secrets-and-confidential-business-information-internal-market_en> accessed 8 February 2024.

TSD outlines that acquisition, use and disclosure of trade secrets is lawful if 'required or allowed by Union or national law'. In my view, Article 15 (3) GDPR should be considered as a provision which requires the trade secret holder (controller) to lawfully disclose a copy of personal data undergoing processing. This interpretation however is not explicitly affirmed by the corresponding recital. Recital 18 TSD states, in a general manner, that 'the acquisition, use or disclosure of trade secrets, *whenever imposed* or *permitted* by law, should be treated as lawful for the purposes of this Directive'. Examples mentioned in Recital 18 do not refer to rights of data subjects, but focus on the rights of workers, their representatives and acquisitions or disclosures of trade secrets taking place in the context of statutory audits performed in accordance with Union or national law. However, the word 'particularly' hints to a non-exhaustive interpretation. Therefore, it seems reasonable to interpret that Article 3 (2) TSD also applies to the controller's obligation to disclose a trade secret (in the form of a copy of personal data), as required by Article 15 (3) GDPR. Consequently, this disclosure is lawful. From a systematic point of view, this also excludes ex-ante liability for misappropriation of the trade secret.[2406] Controllers might argue that such disclosure harms its interest protected by the TSD and refer to Article 15 (4) GDPR. Hence, the ultimate question is whether disclosing a copy of personal data undergoing processing to the data subject is likely to undermine the controller's business or financial interests, strategic position or ability to compete.[2407] In my view, this is not the case for four reasons.

First, the right to obtain a copy of personal data undergoing processing is an individual, non-transferable right. Only the data subject or a third party on the data subject's behalf can invoke it. In addition, the controller must identify the data subject when responding to a request and confirm the identity of the data subject in case of doubt[2408] to minimise the risk of unlawful disclosure. This limits the possible harm for the controller as personal data will be disclosed solely to the data subject (or its representative) making the request.

Second, after having obtained a copy of the personal data undergoing processing, it seems unlikely that the data subject will use this information in a way that undermines the controller's business or financial interests, strategic position or ability to compete. More specifically, data subjects will hardly make their copies of personal data available to the public or to other controllers, for example, to competitors because of privacy considerations. Thus, the risk of subsequent disclosure of personal data in ways that harm the interests of the controllers, in particular their position to compete, seems to be small.[2409] In cases in which data subjects use their right to obtain a copy of personal data in an

[2406] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 250.
[2407] Recital 14 TSD.
[2408] Article 12 (6) GDPR.
[2409] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 313.

abusive manner, controllers may regard such requests as manifestly unfounded. Controllers may refuse to comply with such requests or charge a reasonable fee.[2410]

Third, personal data does not have commercial value per se and does not automatically undermine a controller's business or financial interests when disclosed to the data subject. One single piece of personal data may qualify as a trade secret, but will hardly have a commercial value. It is mostly the composition of various pieces of personal data, in particular in the form of profiles, that constitute commercial value.[2411] There is no established approach to measuring the economic value of data, arguably because this very much depends on the content and the context and because it is difficult to quantify the benefits of data.[2412] Nevertheless, there are three common approaches to measure the monetary value of personal data from a firm's perspective, considering (i) the stock value of the firm, (ii) the revenues of the firm or (iii) the price of personal data records on the market.[2413] The conceptual challenges linked to each approach (every approach has its drawbacks)[2414] also come with various practical challenges. For example, markets for data and datasets are underdeveloped, and there is also no universal standard for categorising data into 'types' for statistical purposes.[2415] Hence, due to the challenges for measuring the value of personal data, it is difficult for controllers to substantiate that the disclosure of personal data copies to the data subject indeed harms their business and financial interests. In addition, the disclosure of individual personal data, even if generated by AI, arguably does not affect the trade secret holder's ability to compete. Likewise, it does not involve a disclosure to competitors. In addition, the relative value of individuals' data is typically rather low.[2416]

Fourth, providing data subjects with a copy of their personal data does not facilitate reverse engineering that may unlock trade secrets and consequently harm the controller's interests. Reverse engineering originates from mechanical engineering but is now increasingly used in the context of digital technologies.[2417] It is a technique whereby a product is being analysed in order to understand how it was designed and how it operates.[2418] In the context of IT systems, reverse engineering may simply

[2410] Case C-307/22, *FT* [2023] ECR I-315, Opinion AG Emiliou paras 32-35; European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 188-191.
[2411] Marc van Lieshout, 'The value of personal data' in Jan Camenisch et al (eds) *Privacy and Identity 2014 IFIP AICT vol. 457* (Springer 2015) 29; Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 313.
[2412] John Mitchell et al, 'Going Digital Toolkit Note: Measuring the economic value of data' OECD Document DSTI/CDEP/GD(2021)2/FINAL at 8, 10, 22 <https://one.oecd.org/document/DSTI/CDEP/GD(2021)2/FINAL/en/pdf> accessed 8 February 2024.
[2413] Marc van Lieshout, 'The value of personal data' in Jan Camenisch et al (eds) *Privacy and Identity 2014 IFIP AICT vol. 457* (Springer 2015) 29.
[2414] Gianclaudio Malgieri, Bart Custers, 'Pricing privacy – the right to know the value of your personal data' (2017) Vol 34 Iss 2 Computer Law & Security Review 289-303.
[2415] John Mitchell et al, 'Going Digital Toolkit Note: Measuring the economic value of data' OECD Document DSTI/CDEP/GD(2021)2/FINAL at 15 <https://one.oecd.org/document/DSTI/CDEP/GD(2021)2/FINAL/en/pdf> accessed 8 February 2024.
[2416] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 313.
[2417] Frank Apunkt Schneider, Günther Friesinger, 'Technology v Technocracy' in Günther Friesinger and Jana Herwig (eds) *The Art of Reverse Engineering* (transcript Verlag 2014) 10.
[2418] Noam Shemtov, Beyond the Code: Protection of Non-Textual Features of Software (Oxford University Press 2017) 71.

be described as 'the process of analysing a system to create representations of the system at a higher level of abstraction'.[2419] Therefore, reverse engineering starts with the final product and analyses backwards in order to determine the methods, components and logic used to generate the final product.[2420] A simple copy of personal data however prevents reverse engineering as it does not facilitate any access to software artefacts. The goal of reverse engineering is to derive information from available software artefacts and to translate it into abstract representations. Software artefacts are requirements, design, code, test case, manual pages etc.[2421] Providing a copy of personal data does not facilitate access to the system that generated the personal data nor does it facilitate access to the system's internal components expressed in source code format[2422] or other system artefacts. In addition, the TSD indicates that reverse engineering requires access to the *product* or *object* in which the trade secret is embodied.[2423] However, this is impossible when simply a copy of personal data is disclosed.

The risks related to reverse engineering are different, however, when a part of the algorithm would need to be disclosed to the data subject for complying with Article 15 (1) lit h GDPR (meaningful information about the logic involved in ADM). In a case pending at the CJEU, the technical expert appointed by the referring court suggested that at least a part of the algorithm needs to be disclosed to comprehend the logic involved in ADM[2424] (see Section 5.6.2). Although it seems unlikely that the CJEU follows the expert's opinion, such information is more likely to indeed harm the controller's business or financial interests, strategic position or ability to compete. Disclosing a part of the algorithm, together with additional information,[2425] allows one to analyse the system used to understand how it was designed and how it operates[2426] which ultimately unlocks the trade secret of the controller. If successful, reverse engineering facilitates the generation of a new program which is functionally equivalent to or even better than the program which was subject to reverse engineering.[2427] Obviously, this undermines the controller's business or financial interests, strategic position or ability to compete. However, the outcome is different when only a copy of personal data is provided.

[2419] Gerardo Canfora, Massimiliano Di Penta, 'New Frontiers of Reverse Engineering' (2007) Future of Software Engineering (FOSE '07) 326-341.
[2420] Noam Shemtov, Beyond the Code: Protection of Non-Textual Features of Software (Oxford University Press 2017) 71.
[2421] Gerardo Canfora, Massimiliano Di Penta, 'New Frontiers of Reverse Engineering' (2007) Future of Software Engineering (FOSE '07) 326, 327.
[2422] Noam Shemtov, Beyond the Code: Protection of Non-Textual Features of Software (Oxford University Press 2017) 71.
[2423] Article 3 (1) lit b TSD; Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 537.
[2424] Case C-203/22 *Dun & Bradstreet Austria* see page 12 <https://www.ris.bka.gv.at/Dokumente/Lvwg/LVWGT_WI_20220211_VGW_101_042_791_2020_44_00/LVWGT_WI_20220211_VGW_101_042_791_2020_44_00.pdf> accessed 8 February 2024.
[2425] E.g. information such as the concrete factors and mathematical formula used, the concrete value assigned to the data subject, the disclosure of the intervals within which different data on the same factor are assigned to the same value; see Case C-202/22 *Dun & Bradstreet Austria*.
[2426] Noam Shemtov, Beyond the Code: Protection of Non-Textual Features of Software (Oxford University Press 2017) 71.
[2427] Andrew Johnson-Laird, 'Software Reverse Engineering in the Real World' (1994) Vol 19 Iss 3 University of Dayton Law Review 843, 846.

Based on these arguments, providing data subjects with a copy of their personal data seems unlikely to harm the controller's business or financial interests, strategic position or ability to compete. It could harm the interests of the controller, but it does not harm the rights or interests specifically protected by the TSD. Therefore, there is no need for a balancing exercise as outlined in Section 6.5.1. Instead, a solution is needed which allows data subjects to effectively enforce their right to obtain a copy of their personal data. Currently, controllers can buttress their (arguable) trade secrets protection.[2428] Already in 2011, Facebook denied a data subject access to his personal data because such disclosures 'would adversely affect trade secrets'.[2429] As I have outlined in this section, these claims are unjustified regarding obtaining a copy of personal data undergoing processing. Empowering data subjects to effectively enforce their right to obtain a copy of their personal data must entail the elimination of the power imbalance between the data subject and the controller. In the current situation, it is the controller who decides whether to provide a copy, and the data subject can only influence the controller's decision by means of costly, lengthy and burdensome litigation. My suggested solution aims to overcome the current issues by extending the exceptions to trade secrets protection currently enshrined in Article 5 TSD as follows:

New exception in Article 5 TSD:

e) for exercising the right to obtain a copy of the personal data undergoing processing as set out in Article 15 (3) of Regulation (EU) 2016/679

The proposed solution solves the trade secrets problem by clarifying that trade secrets protection under the TSD does not apply when data subjects enforce their right to obtain a copy of their personal data undergoing processing enshrined in Article 15 (3) GDPR. This solution is needed because the right of access is a precondition for the enforcement of other data subject rights.[2430] It allows data subjects to verify the lawfulness[2431] of processing and empowers them to request controllers to rectify, erase or block their personal data.[2432] As outlined in Section 6.5, an actual copy of the personal data is the only way for data subjects to obtain rectification of inaccurate personal data. The right to rectification will become more important in the future considering the developments in AI. These developments facilitate the generation of vast amounts of personal data in the form of predictions, profiles, emotion data and any other types of inferred personal data. As outlined in Sections 4.3.1, 4.7.1 and 5.7.2, such personal data are likely to be sometimes inaccurate. This can only be rectified when data

[2428] Paul B de Laat, 'Algorithmic decision-making employing profiling: will trade secrecy protection render the right to explanation toothless?' (2022) Vol 24 Iss 1 Ethics and Information Technology 1, 14.
[2429] See <http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf> accessed 8 February 2024.
[2430] Case C-434/16, *Nowak* [2017] ECR I-994 para 57; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44; Case C-553/07 *Rijkeboer* [2009] ECR I-03889, para 51.
[2431] Recital 63 GDPR.
[2432] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44.

subjects obtain a copy of the personal data processed, for example, the exact emotional state detected by the AI system or the precise topics of interests ascribed to a data subject. By extending the exceptions in Article 5 TSD, five legislative aims of the GDPR will be achieved, namely, ensuring a high level of protection in the EU,[2433] providing data subjects with control concerning the processing of their personal data,[2434] enhancing legal certainty,[2435] strengthening the data subject's rights and the effective protection of personal data.[2436] Simultaneously, it does not necessarily negatively affect the controller's commercial interests protected by the TSD, nor does it hinder the free flow of personal data between the Member States, which is another legislative goal of the GDPR.[2437]

6.5.3 Conclusion

In this section, I have outlined that the legal solution to solve the trade secrets problem consists of introducing a new provision in Article 5 TSD. This new provision, in the form of an exception, clarifies that trade secrets protection under the TSD does not apply when data subjects enforce their right of access according to Article 15 (3) GDPR. This exception strengthens the position of data subjects. It enables subjects to enforce their data subject rights regarding personal data generated by means of AI. Such an exception is justified because providing data subjects with a copy of their own personal data seems unlikely to harm the controller's business or financial interests, strategic position or ability to compete.

6.6 Right to rectification – the verifiability standard problem

The verifiability standard problem (Type 3)

Data subjects need to meet the objective verifiability standard to have output generated by ML and AC powered systems rectified. Output generated by means of ML may constitute unverifiable personal data. Emotion data are by nature highly subjective. Therefore, data subjects cannot provide evidence that meets the objective verifiability standard. Thus, the right to rectification is not fit for purpose to protect the fundamental right to data protection, as this standard hinders data subjects from exercising their right.

6.6.1 Setting the scene

The right to rectification enables the data subject to request the controller to rectify inaccurate personal data and to have incomplete personal data completed.[2438] As the name of the right indicates,

[2433] Recitals 6 and 10 GDPR; Case C-534/20, *Leistritz AG* [2022] ECR I-594 para 26; Case C-645/19 [2021] *Facebook Ireland* ECR I-483 para 45; Case C-511/18, *La Quadrature du Net* [2020] ECR I-791 para 106; Case C-131/12, *Google Spain* [2014] ECR I-317 para 66; Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 44; Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[2434] Recitals 7 GDPR.
[2435] Recitals 7 and 13 GDPR.
[2436] Recital 11 GDPR.
[2437] Recitals 3 and 6 GDPR.
[2438] Article 16 GDPR.

rectification implicitly relies upon the notion of verification in the sense that something may demonstrably be shown to be inaccurate or incomplete.[2439] The CJEU seems to put the emphasis on *factual* evidence, ruling that facts in particular are susceptible to provable evidence.[2440] This task is straightforward when personal data are verifiable (such as a name, date of birth, email address or the weight of an individual).[2441] Nonetheless, predictions produced by ML, such as life expectancy, score value ratings and career perspectives, are essentially educated guesses based on large amounts of data.[2442] Such data are neither factual nor counter-factual data. Predictions may prove to be wrong or true, but in essence they are simply probabilistic and not objectively verifiable,[2443] mainly because they relate to the future and lack 'truth' as a baseline for comparison.[2444] Also, other types of personal data generated by AI such as emotion data are not objectively verifiable due to the subjective perception of emotion. Emotions are subjectively verifiable: emotion data can uniquely be verified by the individual experiencing the emotional state.[2445] Thus, due to the unverifiable or subjective nature of personal data generated by means of AI, it is impossible for data subjects to provide factual data meeting the objective verifiability standard. Consequently, they cannot enforce their right to rectification for personal data which is likely to be inaccurate (Sections 4.3.1, 4.7.1 and 5.7.2).

The right to rectification according to Article 16 GDPR is an underexplored provision in both academia and regulatory guidance. The same can be said about case law on this from the CJEU. There are only three rulings[2446] on the matter which explicitly deal with the right (under the DPD). Only one case relating to the right to rectification is pending at the CJEU.[2447] Nevertheless, I reckon that the right to rectification will have a more prominent role in the future due to developments in AI and the nature of the personal data generated by it.

Let me start with the scope of the right to rectification in the context of personal data generated by means of AI. There are no cases yet at the CJEU which specifically relate to the verifiability standard problem. Regulatory guidance suggests interpreting the scope of the right to rectification broadly,

[2439] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 548.
[2440] Case C-460/20, *TU* [2022] ECR I-962 para 66.
[2441] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 548.
[2442] 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.
[2443] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 302.
[2444] Diana Dimitrova, 'The rise of the personal data quality principle: is it legal and does it have an impact on the right to rectification?' (2021) Vol 12 No 3 European Journal of Law and Technology 21.
[2445] Jennifer Healey, 'Physiological Sensing of Emotion' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 213, 214.
[2446] Case C-434/16, *Nowak* [2017] ECR I-994; Joined Cases C-141/12 & C-372/12, *YS, M and S v Minister voor Immigratie, Integratie en Asiel* [2014] ECR I-2081; Case C-553/07 *Rijkeboer* [2009] ECR I-03889.
[2447] Case C-247/23, *VP*.

including both derived and inferred personal data.[2448] According to EU supervisory authorities, the right to rectification not only applies to 'input data' but also to 'output data'.[2449] In this context, input data means the personal data used by the AI system to generate the output, for example, bank statements, income, zip-code of an individual or the facial expressions of an individual recorded during an automated video assessment. The output data are the prediction with respect to the individual (e.g. non-reliable borrower) or the individual's emotional state detected by the AI system (e.g. anger). Both types of output constitute personal data as they concern information relating to an identified or identifiable natural person. It is therefore clear that the right to rectification applies to both types of output generated by AI.

There are views which suggest limiting the right to rectification to factual data. AG Sharpston takes the view that 'only information relating to *facts* about an individual can be personal data.'[2450] Such facts may be expressed in different forms, for example a person's weight might be expressed objectively in kilos or in subjective terms such as 'underweight' or 'obese'.[2451] Guidelines of the EDPS bluntly state that the right to rectification 'only applies to *objective and factual data*, not to subjective statements (which, by definition, cannot be factually wrong).'[2452] By referring to CJEU case law, legal scholars Wachter and Mittelstad suggest that inferred personal data are being excluded from the scope of the right to rectification.[2453] Implicitly, AG Pikamäe also seems to take this view concerning the automated establishment of a credit score performed by a credit rating agency. In his view, data subjects may enforce their right to rectification 'if the *personal data used to carry out the scoring* should prove to be inaccurate'.[2454] This limits the right to rectification to the input, i.e. to the personal data used to established the credit score. Simultaneously, it excludes the output in the form of the established credit score (inferred personal data).

When these views are applied to predictions generated by ML or emotion data generated by means of AC, none of them could be rectified. To be considered a non-reliable borrower is simply a probabilistic prediction which cannot be verified currently as it relates to the future. Thus, it does not constitute factual data. Likewise, the emotional state detected by the AI system is simply subjective and thus cannot constitute factual data. Obviously, this outcome is undesirable and, in my view, simply wrong, because the text of Article 16 GDPR does not at all suggest such a limitation. Article 16 GDPR applies to the 'rectification of inaccurate personal data' and it does not play a role whether such

[2448] Art 29 Working Party 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', (WP251rev.01, 6 February 2018) at 8-9.
[2449] Ibid at 17-18.
[2450] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081, Opinion of AG Sharpston para 56.
[2451] Ibid para 57.
[2452] European Data Protection Supervisor, 'Guidelines on the Rights of Individuals with regard to the Processing of Personal Data' (25 February 2014) at 18.
[2453] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 550.
[2454] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 50, emphasis added.

personal data constitutes factual data, inferred data, input data or output data *as long as is personal data*, i.e. information relating to an identified or identifiable natural person. In addition, there is nothing in the preparatory documents of the GDPR, which indicates the legislator's intention to limit this right to factual data. In addition, such a limitation would be contradictory to the CJEU's contextual and teleological approach to interpret data subject rights.[2455] As a result, both the prediction as a 'non-reliable borrower' and the emotional state detected by the AI system do fall within the scope of the right to rectification.

It could be argued that inferred personal data by means of AI such as the classification as a non-reliable borrower and detected emotional states constitute opinions (i.e. judgements, thoughts or beliefs about someone[2456]) cannot be rectified. In fact, similar claims about opinions have been made with respect to the accuracy principle. According to Herbst and Dienst, since opinions are not directly related to an objectively provable or disprovable reality about individuals, they cannot be labelled as accurate or inaccurate and thus lie beyond the scope of the accuracy principle.[2457] According to their view, personal data in the form of opinions are simply not the type of information to which the accuracy principle de facto can apply.[2458] When transposing this view to the right to rectification, personal data in the form of opinions cannot be rectified if the personal data does not constitute an objectively provable or disprovable reality about the data subject (a fact)[2459]. Arguably, this applies to the non-reliable borrower prediction and emotional states detected by the AI system. Due to their unverifiable and/or subjective nature, this output in the form of opinions does not constitute an objectively provable or disprovable reality (i.e. a fact) about the data subjects concerned. Consequently, it cannot be rectified.

Wachter and Mittelstad, by referring to CJEU case law, argue that inferred personal data cannot be rectified under data protection law as it constitutes *opinions* and/or *assessments*.[2460] This view is based on a non-contextual reading of the CJEU's case law and assumes that opinions and/or assessments are not rectifiable under Article 16 GDPR. This assumption is wrong. Opinions and/or assessments relating to a particular data subject constitute personal data according to the CJEU. In the words of the CJEU, the concept of personal data 'encompasses all kinds of information, not only *objective* but also *subjective*, in the form of *opinions* and *assessments*, provided that it "relates" to the data

[2455] Case C-434/16, *Nowak* [2017] ECR I-994 paras 53, 54.
[2456] See <https://dictionary.cambridge.org/dictionary/english/opinion> accessed 8 February 2024.
[2457] Tobias Herbst, 'Art. 5 Grundsäze für die Verarbeitung personenbezogener Daten' in Jürgen Kühling and Benedikt Buchner (eds) DatenschutzGrundverordnung/BDSG (2nd edn Beck 2018) 229, para 60; Sebastian Dienst, 'Lawful Processing of Personal Data in Companies under the GDPR' in Daniel Rücker and Tobias Kugler (eds) New European General Data Protection Regulation: A Practitioner's Guide (Beck/Hart/Nomos 2018) 68, para 326.
[2458] See also Dara Hallinan, Frederik Zuiderveen Borgesius 'Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle' (2020) Vol 10 No 1 IDPL 1, 5.
[2459] Case C-460/20, *TU* [2022] ECR I-962 para 68.
[2460] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 550.

subject'.[2461] This condition is satisfied if the information, by reason of its content, purpose or effect, is linked to a particular person.[2462] According to the CJEU, personal data in the form of assessments or opinions fall under the scope of the right to rectification. The data subject to whom the assessment or opinion relates has, at least in principle, a right to rectification because opinions and assessment qualify as personal data.[2463]

The right to rectification is not absolute and not intended to enable data subjects to object and change unfavourable opinions and assessments relating to them. Obviously, the right to rectification should not result in situations in which a candidate in a professional examination may correct his answers in an exam retroactively.[2464] Neither should a person involved in an immigration case be able to rectify the content of a legal analysis.[2465] This contextual and normative limitation is justified and necessary in order to avoid an interpretation of the right to rectification that is excessively broad or 'over-inclusive'.[2466] To add another example, if a controller's employee classifies a data subject as a complete idiot, the data subject cannot use Article 16 GDPR to change this opinion. This would by contrary to the freedom of expression and information according to Article 11 EUCFR. This statement arguably amounts to a value judgement which is not susceptible to proof according to the CJEU.[2467] In common language usage, value judgements are 'a personal opinion about whether something is good or bad' based on 'on personal opinion rather than facts'.[2468] However, the data subject could correct the incorrect representation of this opinion and point out why the subject is not an idiot, for example, by adding a supplementary statement as foreseen by the second sentence of Article 16 GDPR.

Thus, opinions and assessments regarding a specific data subject do fall under Article 16 GDPR. This conclusion also holds true when personal data inferred by means of AI are seen as opinions and assessments. It seems likely that the CJEU will rely on a specific type of teleological interpretation, i.e. functional interpretation 'effet utile'.[2469] If personal data in the form of opinions or assessments established by humans are subject to the right to rectification, the same must apply to opinions and assessments established by machines. Nonetheless, qualifying personal data generated by AI as opinions or assessments might be premature or simply wrong. As outlined in Section 4.7.1, inferences generated by machines are *not* based on human reasoning. Whereas humans have been conditioned to look for

[2461] Case C-434/16, *Nowak* [2017] ECR I-994 para 34. Emphasis added.
[2462] Ibid para 35.
[2463] Ibid para 46.
[2464] Case C-434/16, *Nowak* [2017] ECR I-994, para 54.
[2465] Joined Cases C-141/12 & C-372/12, *YS, M and S v Minister voor Immigratie, Integratie en Asiel* [2014] ECR I-2081, para 45.
[2466] Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 27 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.
[2467] Case C-460/20, *TU* [2022] ECR I-962 para 66.
[2468] See < https://dictionary.cambridge.org/dictionary/english/value-judgment > accessed 8 February 2024.
[2469] Koen Lenaerts, José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) European University Institute Working Paper AEL 2013/9 at 25 <https://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1&isAllowed=y> accessed 8 February 2024.

causes (why), AI focusses on correlations and probabilities (what).[2470] As indicated in Section 4.3.1, current AI systems have been called to be clueless[2471] to understand cause and effect and to be devoid of common sense.[2472] It seems that humans are much better at this than machines.[2473] Common sense reasoning still constitutes a challenge in AI applications.[2474] AI is unable to think in a manner on par with human thinking[2475] which is underscored by the shortcomings in the AI discipline of automated reasoning (Section 2.2.5). Personal data generated by AI systems cannot qualify as opinions and/or assessments when considering that such systems do not adopt human reasoning and lack common sense capabilities. The correct qualification for personal data generated by AI systems is 'personal data inferred by automated means'.

It is crucial for data subjects that personal data generated by AI systems fall under the right to rectification, in particular when considering that such data are highly scalable and riskier than personal data derived by humans. Actions taken based on probabilistic predictions and correlations may have real impact on human interests[2476] (e.g., to receive a loan or to be employed). This holds particularly true when such predictions or correlations are essentially considered as *facts*, although such personal data generated by ML are simply probabilistic and relate to future conduct that has not yet happened. As outlined in Sections 4.3.1, 4.7.1 and 5.7.2, output generated by AI can be problematic in terms of accuracy. Personal data inferred by AI are not based on human reasoning, and AI is currently subject to severe reasoning deficiencies, in particular regarding common sense reasoning (see also Sections 2.2.5, 4.3.1, 4.4.1 and 4.7.1). Personal data generated by AI can be shared with third parties on a large scale (e.g. advertisers and other service providers).

After having discussed these views that interpret the scope of the right to rectification too narrowly, I also want to mention a view that interprets the right to rectification too broadly. Dimirova suggests that the right to rectification should be seen as a tool 'having the potential to rectify algorithm model issues', meaning that this right can also be invoked to correct the quality of the data processing

[2470] Viktor Mayer-Schönberger; Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Houghton Mifflin Harcourt 2013) 14, 18.
[2471] Brian Bergstein, 'What AI still can't do' MIT Technology Review (Cambridge 31 January 2020) <https://www.technologyreview.com/2020/01/31/304844/ai-common-sense-reads-human-language-ai2/> accessed 8 February 2024.
[2472] Cade Metz, 'Paul Allen Wants to Teach Machines Common Sense' *The New York Times* (New York, 28 February 2018) < https://www.nytimes.com/2018/02/28/technology/paul-allen-ai-common-sense.html > accessed 09 November 2019.
[2473] Davide Castelvecchi, 'AI pioneer: The dangers of abuse are very real' *Nature* (London, 4 April 2019) < https://www.nature.com/articles/d41586-019-00505-2> accessed 8 February 2024.
[2474] Shoham Yoav et al, 'The AI Index 2018 Annual Report' (AI Index Steering Committee Stanford University 2018) 64 <https://hai.stanford.edu/sites/default/files/2020-10/AI_Index_2018_Annual_Report.pdf > accessed 8 February 2024.
[2475] Lance Eliot, 'AI Ethics And The Quagmire Of Whether You Have A Legal Right To Know Of AI Inferences About You, Including Those Via AI-Based Self-Driving Cars' *Forbes* (New York, 25 May 2022) < https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/lanceeliot/2022/05/25/ai-ethics-and-the-quagmire-of-whether-you-have-a-legal-right-to-know-of-ai-inferences-about-you-including-those-via-ai-based-self-driving-cars/amp/> accessed 8 February 2024.
[2476] Brent Daniel Mittelstadt et al, 'The ethics of algorithms: Mapping the debate' (2016) Vol 3 Iss 2 Big Data & Society 1, 5; Solon Barocas, 'Data Mining and the Discourse on Discrimination' (2014) <https://dataethics.github.io/proceedings/DataMiningandtheDiscourseOnDiscrimination.pdf> accessed 8 February 2024.

model.[2477] Obviously, when assessing the accuracy of personal data generated by AI, the model upon which the personal data are based also must be considered in order to ensure a comprehensive assessment. This is because the quality of the information, i.e. the personal data generated by AI, is affected by the quality of the AI system used.[2478] In my view, the right to rectification should not be interpreted so broadly as to empower data subjects to request the rectification of models deployed by an AI system. In itself, AI models do not constitute personal data. They process (and are trained with) personal data. Models cannot be 'information relating to an identified or identifiable natural person' simply because they operate and are trained with personal data from many data subjects. Thus, the right to rectification should be limited to input and output data. Extending this right to the rectification of models deployed by AI systems is not needed from a conceptual point of view. It is the accuracy principle, together with the accountability principle further substantiated in Article 24 (1) GDPR, that obliges controllers to ensure that the AI system generates accurate output. Controllers must 'implement appropriate and effective measures to ensure and demonstrate' that processing of personal data occurs in accordance with the rules laid down in the GDPR.[2479]

After having established the proper scope of the right to rectification in the context of AI, the question remains how data subjects may enforce their right to rectification concerning inferred personal data that by nature is either unverifiable or subjective. I now discuss possible solutions.

6.6.2 Solution: Amending the right to rectification

The problems surrounding the rectification of personal data generated by means of AI have not gone unnoticed. The scholars Wachter and Mittelstadt have claimed that inferences increasingly determine how data subjects are being viewed and evaluated, and that the GDPR attributes only limited rights regarding inferences to data subjects.[2480] They suggest closing this gap and proposing the 'right to reasonable inferences'. This right should apply to 'high-risk' inferences that cause damage to privacy or reputation or have low verifiability in the sense of being predictive or opinion-based while being used for 'important decisions'.[2481] The suggested right has an ex-ante and ex-post component. This right obliges controllers, ex-ante, to establish whether an inference is reasonable, by disclosing to the data subject (i) why certain data are normatively acceptable bases to draw inferences, (ii) why these inferences are normatively acceptable and relevant for the chosen processing purpose or type of automated decision and (iii) whether the data and methods used to draw the inferences are accurate and

[2477] Diana Dimitrova, 'The rise of the personal data quality principle: is it legal and does it have an impact on the right to rectification?' (2021) Vol 12 No 3 European Journal of Law and Technology 28.
[2478] See Lee A Bygrave, who discusses information quality in the context of information systems 'Ensuring Right Information on the Right Person(s)' (1996) University of Oslo, Institute for Private Law <https://www.jus.uio.no/ifp/om/organisasjon/afin/forskning/notatserien/1996/4_96.html> accessed 8 February 2024.
[2479] Art. 24 (1), Recital 74 GDPR.
[2480] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 611 and 613.
[2481] Ibid 611, 613.

statistically reliable. Then, an ex-post component allows data subjects to challenge unreasonable inferences which could support the right to contest ADM as enshrined in Article 22 (3) GDPR.[2482] The ex-post component relates to the verifiability problem discussed here. It allows data subjects to raise objections on the ground that the inference or its source data is irrelevant, unreliable or non-verifiable and, concerning unverifiable and subjective inferences, to provide supplementary information to convince the controller to change its assessment.[2483] According to Wachter and Mittelstadt, the right to reasonable inferences 'would embed an answer to the verifiability question in law' and thus strengthen data protection rights, including the right to rectification which arguably already offers 'a remedy for non-verifiable and subjective inferences and opinions'.[2484] I assume that these statements refer to the ex-ante component of the right which obliges controllers to inform data subjects whether the data and methods used to draw the inferences are accurate and statistically reliable. If the controller cannot demonstrate this, data subjects can enforce their right to rectification because they can establish that the inference is not accurate.

The proposed right to reasonable inferences is an important contribution to the field and contains several valid points and suggestions. However, it is beyond the scope of this thesis to analyse this broad right in depth. I therefore restrict myself to assess whether the right to reasonable inferences solves the verifiability standard problem. In essence, it does not solve the problem because controllers are likely to claim that the methods used to draw the inferences are accurate and statistically reliable. If not, controllers would incriminate themselves and indicate non-compliance with the accuracy principle which could lead to both regulatory and private enforcement. In addition, controllers need results from reliable practices. To state not using accurate and statistically reliable methods would be of no use for controllers. Consequently, data subjects may not receive information that empowers them to effectively enforce their right to rectification concerning unverifiable or subjective personal data generated by AI. It will arguably become even more difficult for data subjects to enforce this right because controllers, when confronted with a rectification request, can simply claim that the methods used to draw the inferences are accurate and statistically reliable and refer to the information already disclosed in the context of the right to reasonable inferences. The suggested scope of the right contains several ambiguous terms, such as 'high-risk' inferences causing 'damage to privacy or reputation' and 'important decisions'. I opine that this right, when implemented as suggested, would lead to similar problems as those occurring in the context to the right not to be subject to ADM (see Section 5.11). In addition, data subjects should be able to enforce their right to rectification irrespective whether the personal data are used for 'important decisions'. This holds particularly true when considering the extensive data sharing which takes place in the context of IoT solutions which leverage

[2482] Sandra Wachter, Brent Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) No 2 Columbia Business Law Review 494, 613.
[2483] Ibid 494, 619.
[2484] Ibid.

data captured using Internet of Things devices. IoT is defined as the cyber-physical ecosystem of interconnected physical and potentially virtual sensors and actuators.[2485] If shared with other controllers, inaccurate personal data may cause harm to data subjects because it is disclosed and subsequently used by third parties.

Another solution for the verifiability standard problem is proposed by Ausloos, Veale and Mahieu. They suggest construing the right to rectification as an addendum rather than a replacement of data. In contentious cases, neither the data subject nor the controller should act as 'the arbiter of truth'. Rather, when the controller has 'good reasons' to disagree with the data subject with respect to a requested rectification, the best solution is to ensure that both views co-exist in the data processing system and to oblige the controller to consider both the suggested rectification and the original data.[2486] The data subject has a right to provide 'a supplementary statement' as enshrined in the second sentence of Article 16 GDPR. However, it is unclear what specific obligations such a supplementary statement imposes on the controller,[2487] also when consulting regulatory guidance.[2488] Thus, the right to have incomplete personal data completed does not prove to be particularly helpful in the context of AI because it does not solve the problem of inaccurate data. Furthermore, the proposed solution does not effectively protect the data subject. The data subject has no means to control how the controller shares the 'original data' of which the accuracy the data subject contests. Third, the controller's 'good reasons' to disagree with the requested rectification seem to be too vague and gives the controller significant leeway. Conclusively, the suggested solution does not really solve the problem, as potentially inaccurate personal data will be further processed by the controller, including the risk of subsequent sharing with third parties.

The solution I have in mind is more straightforward. In essence, I suggest slightly broadening the right to rectification concerning the processing of personal data generated by automated means and empower data subjects to easily contest the accuracy of such personal data. When the data subject contests the accuracy of such personal data, the controller shall either cease processing or rectify the personal data as requested by the data subject, unless it can demonstrate that the controller's interest prevail. I therefore suggest adding a second paragraph to Article 16 GDPR, worded as follows:

[2485] European Union Agency for Network and Information Security, 'Good Practices for Security of Internet of Things' (2018) 45 <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/@@download/fullReport> accessed 8 February 2024.
[2486] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 302.
[2487] Diana Dimitrova, 'The rise of the personal data quality principle: is it legal and does it have an impact on the right to rectification?' (2021) Vol 12 No 3 European Journal of Law and Technology 27.
[2488] Which simply states that Article 16 GDPR contains a right for the data subject to complement the personal data with additional information see Art 29 Working Party 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679', (WP251rev.01, 6 February 2018) at 18.

> *(2) The data subject shall have the right to contest the accuracy of personal data generated by automated means, including to obtain the rectification of such personal data. The controller shall cease the processing and, if requested by the data subject, rectify the personal data, unless the controller demonstrates that its interest to process the personal data in the contested form and for the specified purpose override the interests, rights and freedoms of the data subject.*

First, I propose to use the term 'generated by automated means' to overcome discussions whether personal data are inferred or observed, as is the case concerning the right to data portability (see Section 5.9). Furthermore, the term 'automated' means is widely used in the GDPR[2489] and is broad enough to capture any kind of processing facilitated by means of AI. At the same time, the term 'automated' means limits the extended scope of the right to rectification by excluding personal data inferred or generated by humans such as opinions and conclusions with respect to the data subject. This avoids creating regulatory overreach and limits the right for data subjects to (i) exercise influence (control) over personal data generated by means of AI and other automated means, (ii) concerns related to the accuracy of such personal data and (iii) possible harm for data subjects caused by the automated processing of personal data, like the rationale concerning Article 22 GDPR.[2490]

The right of data subjects to contest the accuracy of personal data generated by automated means allows them to exercise effective control over the processing of such data. Data subjects may request the rectification of such personal data without having to provide evidence that meets the objective verifiability standard. As pointed out in Sections 6.6.1 and 5.7.3, this might be impossible due to the unverifiable and subjective nature of the personal data generated by AI. Reversing the burden of proof and demanding the controller to provide evidence that the personal data meets the objective verifiability standard 'does the trick'. The proposed solution imposes the duty on the controller to demonstrate why its interest to process personal in the contested form prevails over the interests, rights and freedoms of the data subject. Thus, the controller bears the burden of proof to demonstrate that its interests prevail when the controller intends to process the personal data contested by the data subject. The proposed solution intentionally excludes specific requirements to which data subjects must adhere when exercising this right. This allows data subjects to effectively enforce this right, which is needed when considering that personal data generated by AI may be unverifiable or subjective. It protects data subjects from harms arising due to the processing of personal data of which the accuracy cannot be verified due to the lack of truth as a baseline for comparison, as is the case with predictions. When data subjects contest the accuracy of predictions, controllers need to cease processing and, if

[2489] Articles 2 (1), 4 (2), 20 (1) lit b, 21 (5) and Recitals 15, 68 GDPR.
[2490] Isak Mendoza, Lee A Bygrave, 'The Right Not to be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou et al (eds) *EU Internet Law: Regulation and Enforcement* (Springer International 2017) 83-84; Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 526.

requested by the data subject, rectify the prediction. A controller may only continue with processing the prediction if it can demonstrate that its interests prevail. This might be quite challenging and requires the controller to carefully assess the interests at hand. The proposed solution resembles the concept of the right to object according to Article 21 (1) GDPR in which the controller has to prove that it has compelling legitimate grounds to processing.[2491] If the nature of personal data generated by AI is highly subjective, as is the case with detected emotional states, the data subject may easily contest the accuracy and ask the controller to rectify the detected emotional state as perceived by the data subject.

If a controller cannot demonstrate that its interests to process the personal data for the specified purpose prevail, it must ultimately erase such personal data in accordance with Article 17 (1) lit a GDPR. In this case, processing the personal data is no longer necessary for the specified purpose when the controller cannot demonstrate prevailing interests. This provides effective protection[2492] for the data subject because personal data of which the nature is unverifiable or subjective may only be processed if the controller's interests indeed prevail, and in all other cases such personal data must be either rectified or erased after the data subject has contested the accuracy.

It might be argued that the proposed solution is overly broad and reinforces the data subjects' interests too strongly. However, I think this is not the case. In my view, if controllers engage in speculative processing of personal data of which the nature is unverifiable or subjective, data subjects need a powerful counterweight to contest to such processing. This solution does not prohibit such processing from the outset, as data subjects need to enforce their right to create an impact on the controller. In addition, this solution does not intervene with the controller's fundamental right to have a business or the controller's freedom of contract. It simply obliges controllers to assess their own interests and the data subject's fundamental rights, freedoms and interests when engaging in arguably speculative processing that relates to unverifiable or subjective personal data. If the controller's interests do not prevail, it can no longer process such data. The decision of whom to hire or accept as a client remains in full discretion of the controller and there is no impact on the freedom of contract. The latter is covered by the freedom to conduct a business according to Article 16 EUCFR (as confirmed by the CJEU)[2493] and grants the controller legal freedom to enter a contract and decide on its content.[2494]

[2491] Gabriela Zanfir-Fortuna, Commentary of Article 21 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 517.
[2492] Case C-645/19 [2021] *Facebook Ireland* ECR I-483 para 45; Case C-319/20, *Meta Platforms Ireland Limited* [2022] ECR I-322 para 73.
[2493] Case C-426/11, *Alemo-Herron* [2013] ECR I-521 para 32; Case C-283/11, *Sky Österreich* [2013] ECR-28 paras 42, 43.
[2494] Olha O Cherednychenko, 'Fundamental Freedoms, Fundamental Rights, and the Many Faces of Freedom of Contract in the EU' in Mads Andenas, Tarjei Bekkedal, Luca Pantaleo (eds) *The Reach of Free Movement* (Springer 2017) 273, 276.

The proposed solution does not negatively affect the accomplishment of an economic union and economic progress, which is one of the legislative goals of the GDPR.[2495] It restricts the processing of personal data generated by automated means when data subjects enforce their right to contest the accuracy of such data or to have it rectified. If the proposed solution has an economic impact at all, it seems likely to be minimal when considering that the majority of data subjects do not invoke their rights granted by the GDPR. According to empirical research conducted in the Netherlands, 83% of the participants reported to not have taken any action to enforce their data subject rights.[2496] Unfortunately, the study does not specifically outline the practical use of the right to rectification. When referring to the practical use of other data subject rights (object 8%, access 5%, erasure 4%), one can expect similarly low figures for the right to rectification.[2497] If there is economic impact for the controllers and the economic union, it will be minimal. The low practical usage of data subject rights does not imply that these rights are superfluous. They empower data subjects to effectively influence the processing of personal data. To couple the justification of such rights with practical usage is ill-founded and would make many enforceable rights, for example, those enshrined in consumer law, superfluous.

The proposed solution is well aligned with a couple of legislative aims envisaged by the GDPR. It ensures a consistent and high level of protection of natural persons,[2498] and strengthens the data subject right's effectiveness.[2499] Likewise, the solution provides the same level of legally enforceable data subject rights[2500] by avoiding difficulties concerning procedural autonomy as discussed in Section 5.7.1. The rectification of unverifiable or subjective personal data generated by automated means depends not on objectively verifiable evidence but on the balancing of the interests at hand.

6.6.3 Conclusion

In this section, I have outlined that the legal solution to solve the verifiability standard problem consists of amending the right to rectification. I suggest adding an additional paragraph in Article 16 GDPR. This paragraph broadens the right to rectification regarding the processing of personal data generated by automated means and empowers data subjects to easily contest the accuracy of such personal data. When data subjects contest the accuracy, the controller shall either cease processing or rectify the personal data as requested by the data subject, unless it can demonstrate that the controller's

[2495] Recital 2 GDPR.
[2496] Joanna Strycharz, Jef Ausloos, Natali Helberger, 'Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR' (2020) Vol 6 Iss 3 European Data Protection Law Review 407, 414-415.
[2497] See Table 4: Joanna Strycharz, Jef Ausloos, Natali Helberger, 'Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR' (2020) Vol 6 Iss 3 European Data Protection Law Review 407, 417.
[2498] Recital 10 GDPR; Case C-534/20, *Leistritz AG* [2022] ECR I-594 para 26; Case C-645/19 [2021] *Facebook Ireland* ECR I-483 para 45; Case C-511/18, *La Quadrature du Net* [2020] ECR I-791 para 106; Case C-131/12, *Google Spain* [2014] ECR I-317 para 66; Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 44.
[2499] Recital 11 GDPR.
[2500] Recital 13 GDPR.

interest prevail. This new paragraph solves the verifiability standard because data subjects are not required to provide objectively verifiable evidence when they intend to rectify unverifiable and subjective personal data generated by AI.

6.7 Automated decision-making – cumulativeness problem

The cumulativeness problem (Type 3)

The cumulative and vague requirements in Article 22 GDPR render it inapplicable to many decisions enabled, taken by or generated with the support of AI. Therefore, Article 22 GDPR is not fit for purpose to effectively protect data subjects from the particular risks associated with the automated processing of personal data, which is the main rationale of this provision according to the CJEU.

6.7.1 Setting the scene

As outlined in Section 3.3.4.6, Article 22 (1) GDPR rests on three cumulative conditions: (i) a decision is made that is (ii) based solely on automated processing or profiling and (iii) has either legal effects or similarly significant effects for the data subject concerned.[2501] Most output generated by AI, i.e. ML predictions such as future behaviour, potential interests or characteristics of data subjects, do not necessarily constitute decisions in the sense of requirement (i). The same can be said about output produced by an AI system that intends to detect the emotional state of an individual, combining ML with other AI disciplines (AC, CV and NLP). Requirement (ii) excludes AI systems that 'only' provide decisional support for decision-making from the scope of Article 22 GDPR.[2502] In fact, a limited degree of human involvement is sufficient to render Article 22 GDPR inapplicable.[2503] For example, the Amsterdam Court of Appeal considers a personal conversation as sufficient to satisfy the requirement of actual human intervention.[2504] Also, requirement (iii) seems difficult to satisfy considering that AI systems used for ADM utilise relatively obscure logic and come with covert consequences.[2505] Thus, due to the cumulative requirements which must be met simultaneously, this right is often not applicable. It therefore protects data subjects ineffectively from decisions enabled, generated or supported by AI. This starkly contrasts with the rationale of the provision as identified by the CJEU, which is *effective protection* against the risks associated with the *automated* processing of personal

[2501] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 43; Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 532.
[2502] Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Autmated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 253.
[2503] Sebastião Barros Vale, Gabriela Zanfir-Fortuna, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities' (2022) 8 <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf> accessed 8 February 2024.
[2504] Amsterdam Court of Appeal 4 April 2023, ECLI:NL:GHAMS:2023:793 para 3.25.
[2505] Lee A. Bygrave, Commentary of Article 22 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary – 2021 Update* (OUP 2021) 100.

data, including profiling.[2506] Despite CJEU's broad interpretation[2507] of the notion of a decision, the cumulativeness problem is not solved. The other two cumulative conditions (ii) and (iii) must still be met *simultaneously*. Often, processing is not 'solely automated' as required by condition (ii), and the required effects foreseen by condition (iii) remain vague.

Article 22 GDPR is heavily debated in academia, mostly focussing on the question whether the GDPR contains a right to explanation[2508] of ADM as indicated in Sections 4.4.1 and 5.6.2.[2509] Binns and Veale[2510] discuss particular challenges with respect to conditions (i) to (iii) that arise when human intervention and/or a decision's significance is layered by stages or by particular decision outcomes. These challenges include, for example, the difficulty to locate the decision itself and whether the significance should be interpreted in terms of potential or realised effects.[2511] Brkan compares Article 22 GDPR with a Swiss cheese with giant holes in it due to the limitations and exceptions enshrined in this provision.[2512] Bygrave uses a different metaphor for pointing to the issues of Article 22 (1) GDPR. If one of the three requirements is not met, the house of cards collapses and the provision does not apply in its entirety.[2513] This metaphor underscores the essence of the cumulativeness problem. I now discuss how this problem could be solved.

6.7.2 Solution: Redrafting the right not to be subject to ADM

In essence, there are three approaches to solve the cumulativeness problem. The first is to consider Article 22 GDPR a regulatory failure and focus on other means enshrined in the GDPR to counter the challenges and risks of ADM. The fairness and accountability principle, data protection by design and default, data protection impact assessments and certifications could be suitable instruments for this. In particular, data protection impact assessments ('DPIAs') according to Article 35 GDPR could be helpful because they demand controllers to consider the rights, freedoms and interests of data subjects rather than focussing on the degree of automation involved in ADM.[2514] However, to leave

[2506] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 57, 60.
[2507] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 44-46; Opinion AG Pikamäe paras 37, 38, 42, 43.
[2508] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 75-101; Sandra Wachter, Brent Mittelstadt, Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) Vol 7 Iss 2 IDPL 76-99; Giancludio Malgieri, Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Makig Exists in the General Data Protection Regulation' (2017) Vol 7 Iss 4 IDPL 243-265.
[2509] For an overview, see Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' (2019) Vol 27 Iss 2 International Journal of Law and Information Technology 91, 110-119.
[2510] Reuben Binns, Michael Veale, 'Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR' (2021) Vol 11 No 4 International Data Privacy Law 319, 332.
[2511] Reuben Binns, Michael Veale, 'Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR' (2021) Vol 11 No 4 International Data Privacy Law 319, 332.
[2512] Maja Brkan, 'Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond' (2019) Vol 27 Iss 2 International Journal of Law and Information Technology 91, 97.
[2513] Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Autmated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 253.
[2514] Reuben Binns, Michael Veale, Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR' (2021) Vol 11 No 4 International Data Privacy Law 319, 331.

the task to mitigate possible risks for data subjects related to ADM to controllers is insufficient. Apart from formalistic bureaucratic overkill and a lack of substantive change,[2515] it is fairly predictable that controllers will seize the opportunity to claim that AI systems and ADM generated by it are not really 'risky'.[2516] Ultimately, controllers are responsible for processing of personal data and need to perform risk assessments, such as DPIAs. Hence, the first approach is not suitable to actually solve the cumulativeness problem.

The second approach is to find the solution beyond data protection law, such as EU consumer law. In May 2022, the European Commission launched a fitness check on EU consumer law focussing on digital fairness. This fitness check determines whether additional legislative action is needed to ensure a high level of consumer protection in the digital environment.[2517] The Commission stressed the risks for consumers associated with the digital transformation, specifically difficulties for consumers to make informed choices and safeguard their interests.[2518] More specifically, the Commission points to commercial practices that distort consumers decision-making processes and abuse their behavioural biases by means of personalisation and profiling. It specifically links these practices with the processing of personal data: 'underlying data collection and processing combined with analysis of consumers behaviour and their cognitive biases can be used to influence consumers to take decisions that are detrimental to their best interests'.[2519]

In the digital economy, personal data constitute an integral part of products, services and transactions. In this context, personal data may be seen as an economic asset (e.g., use of a service in exchange for personal data), part of the service (e.g. virtual assistants and IoT services), means to determine the conditions of the service (e.g. personalisation) or as a means to influence consumer's decision-making process (e.g. exploiting consumer behavioural biases).[2520] EU consumer law and policy aims to ensure a high level of consumer protection, in particular with regard to the health, safety and *economic interests of consumers*.[2521] An important aspect of this is to avoid possible exploitations of the consumer as the economically weaker party.[2522] Thus, the scope and objectives of EU consumer and data protection law are different. Nonetheless, these two areas of law might complement each other.[2523]

[2515] Lilian Edwards, Michael Veale, 'Slave to the Algorithm: Why a 'Right to Explanation' is Probably not the Remedy You are Looking for' (2017) Vol 16 Iss 1 Duke Law & Technology Review 19, 77-80.
[2516] Reuben Binns, Michael Veale, 'Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR' (2021) Vol 11 No 4 International Data Privacy Law 319, 331.
[2517] See < https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13413-Digital-fairness-fitness-check-on-EU-consumer-law_en > accessed 8 February 2024.
[2518] Commission, 'New Consumer Agenda' COM (2020) 696 final at 10 < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0696&from=EN > accessed 8 February 2024.
[2519] Ibid.
[2520] Natali Helberger et al, 'The perfect match? a closer look at the relationship between eu consumer law and data protection law' Vol 54 Iss 5 Common Market Law Review 1427, 1430-1431.
[2521] Article 169 TFEU.
[2522] Stephen Weatherill, *EU Consumer Law and Policy* (2nd edn Elgar Publishers 2013) 310.
[2523] Natali Helberger et al, 'The perfect match? a closer look at the relationship between eu consumer law and data protection law' Vol 54 Iss 5 Common Market Law Review 1427, 1464.

EU data protection law governs the processing of personal data by means of AI and EU consumer law protects the economic interests of consumers. Using personal data generated by AI (e.g., emotion data) to distort a consumer's decision-making capacity may be prohibited under EU consumer law. Consider a trader that exploits a consumer's emotional state by manipulating the consumer into the conclusion of a contract that is detrimental to its economic interest. This specific use of personal data potentially constitutes a prohibited unfair commercial practice under the current and future EU consumer law framework. EU consumer law protects the economic interests of data subjects acting in the capacity of a consumer by prohibiting unfair commercial practices that rely on the use of personal data generated through AI. However, this is a complementary protection to the protection provided by Article 22 GDPR, which does not primarily protect the data subject's economic interests. Rather, Article 22 GDPR aims to effectively protect individuals against the particular risks associated with the automated processing of personal data, including profiling.[2524] It also envisages to let data subjects exercise influence over ADM, to reduce concerns over the quality of ADM,[2525] and to uphold human dignity by ensuring that humans maintain the primary role in constituting themselves.[2526] This is emphasised by Recital 4 GDPR, which states that 'the processing of personal data should be designed to serve mankind'. Hence, the cumulativeness problem cannot be simply solved by current or future EU consumer law.

Another relevant area of law to address the cumulativeness problem is the AI Act. In 2021, the EU Commission proposed[2527] the AI Act. After multiple amendments and trilogue negotiations, the AI Act's compromise text[2528] was published in February 2024. The latter tries to achieve the ambitious aim to be a far-reaching regulation envisaging a high level of protection for Union values, fundamental rights and principles. At the same time, it focusses on new rules relating to placing on the market, putting into service and use of AI systems, promotes innovation and aims to improve the functioning of the internal market.[2529] Thus, it is regulation covering aspects of product safety and fundamental rights. Due to its scope, [2530] the AI Act's compromise text does not specifically regulate risks for data subjects arising from the processing of personal data in the context of ADM. This does not mean that the AI Act is not beneficial for individuals and the society, but it simply does not address the specific

[2524] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 57, 60.
[2525] Recital 71 GDPR.
[2526] Isak Mendoza, Lee A Bygrave, 'The Right Not to be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou et al (eds) *EU Internet Law: Regulation and Enforcement* (Springer International 2017) 83-84; Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 249.
[2527] AI Act proposal adopted by the Commission COM (2021) 206 final <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN> accessed 8 February 2024.
[2528] AI Act compromise text resulting from the trilogue negotiations see <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 8 February 2024.
[2529] Article 1 and Recitals 1, 5, 28 AI Act compromise text <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 8 February 2024.
[2530] Ibid, Article 2 (5a) states that the AI Act shall not affect the GDPR nor the ePD.

risks relating to the processing of personal data. For this, secondary law on the fundamental right to data protection remains the proper regulatory instrument.

Interestingly, Article 68 c of the AI Act's compromise text introduces a 'right to explanation of individual decision-making.'[2531] Reading this provision leads to a deja vu: the wording is very similar to Article 22 GDPR, with some variations. Article 68 c (1) compromise text reads as follows: '*Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2, and which produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety and fundamental rights shall have the right to request from the deployer clear and meaningful explanations on the role of the AI system in the decision-making procedure and the main elements of the decision taken.*' This points clearly to the academic discussions on the existence of a right to explanation for ADM under the GDPR.[2532] In the AI Act, the emphasis lies on meaningful *explanation*, as opposed to meaningful *information* under the GDPR. The notion of 'main elements' of the decision seems to be a new concept. Article 68 c (3) of the AI Act's compromise text states that this right '*shall only apply to the extent that the right referred to in paragraph 1 is not already provided for under Union legislation*.' Undoubtedly, this paragraph refers to Article 22 GDPR and will lead to tricky demarcation issues, blended with legal uncertainty. What seems clear, however, is that the AI Act aims to provide *complementary* protection from ADM. Hence, the second approach to finding a solution beyond data protection law is unsuitable to solve the cumulativeness problem.

The third approach is to redraft Article 22 GDPR. In my view, this is the most suitable solution. In fact, some scholars already suggested to 'radically' redraft Article 22 or 'let it die'.[2533] These scholars suggested to redraft paragraph 1 of Article 22 GDPR as follows:

The data subject shall ~~have the right not to~~ **not** be subject to a decision based ~~solely~~ on automated processing **without meaningful human intervention**, including profiling, which produces ~~legal effects concerning him or her or similarly significantly affects~~ **a significant effect on** him or her.

This suggestion is a good starting point, but in my view not suited to solve the cumulativeness problem. Whereas paragraph 1 gets rid of requirement (ii) 'based solely on automated processing or profiling', it introduces a new requirement, i.e. 'without meaningful human intervention'. Debates will

[2531] Article 68 c AI Act compromise text <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf> accessed 8 February 2024.
[2532] See references contained in the last paragraph of Section 3.3.4.6 for an overview.
[2533] Paul De Hert, Guillermo Lazcoz, 'Radical rewriting of Article 22 GDPR on machine decisions in the AI era' *European Law Blog* (13 October 2021) <https://europeanlawblog.eu/2021/10/13/radical-rewriting-of-article-22-gdpr-on-machine-decisions-in-the-ai-era/> accessed 8 February 2024.

arise which requirements must be met to qualify as meaningful human intervention, similar to the discussions in Sections 5.11.2 and 5.11.3. Also, this new requirement comes with some ambiguity which is likely to be buttressed by controllers. In addition, it is not entirely clear whether the requirement of a 'significant effect' for the data subject must materialise or also includes potentially significant effects. Whether the reference 'including profiling' should be understood as 'involving profiling' or rather as an alternative baseline criteria for application (either ADM or profiling)[2534] remains unclear. In sum, the ambiguities with respect to the cumulative requirements that must be met to render Article 22 GDPR applicable remain to a large extent.

I suggest redrafting Article 22 GDPR as follows:

Harmful profiling and automated inferences

1. *The data subject shall not be subject to profiling or automated inferences which potentially harm its interests, rights and freedoms. Controllers must assume harm if profiling or automated inferences is intended to be used for decision-making regarding that data subject.*
2. *Paragraph 1 shall not apply if such profiling or automated inferences:*
   a) *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
   b) *is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
   c) *is based on the data subject's explicit consent.*
3. *The data subject shall have the right to obtain the controller's assessment which is required to comply with paragraph 1.*
4. *In the cases referred to in points a) and c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.*
5. *Profiling and automated inferences referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

Paragraph 1 entails two cumulative requirements: (i) profiling *or* automated inferences and (ii) possible harm to the data subject's interests, rights and freedoms. As indicated in Section 3.3.4.6 and confirmed by the CJEU, [2535] Article 22 GDPR constitutes a prohibition which is subject to the

[2534] Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 252.
[2535] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 52, 64; Opinion AG Pikamäe para 31.

exceptions listed in paragraph 2. The nature of this provision should be clarified by a corresponding recital to avoid another discussion in academia.

The term profiling in requirement (i) is defined in Article 4 (4) GDPR. The core element of this definition is 'to evaluate certain personal aspects' relating to the data subject. Evaluation includes efforts to 'analyse' or 'predict' aspects with respect to data subjects, for example, their economic situation, personal preferences, interests, reliability and behaviour. In addition, profiling refers to any form of automated processing of personal data to evaluate data subjects. The wording 'in particular' is typically used to indicate non-exhaustiveness. Thus, the examples of specific personal aspects mentioned in the definition are not exhaustive. The definition of profiling is broad enough to capture personal data generated by AI systems, for example, to establish probabilistic predictions (ML) or to detect the data subject's emotional state (AC) based on behaviour (e.g. facial expressions). Profiling also covers any kind of score attributed to a data subject. Think about an insurance company that ascribes a risk score to a data subject as a 'risky driver'. A dating app which attributes an 'attractiveness' score to the data subject to suggest a match with individuals having a similar score is another example.

I have added automated inferences as an additional requirement triggering this provision. In everyday use, inferences are defined as 'a *guess* that you make or an opinion that you form based on the information you have'[2536] or 'something that you *can find* out indirectly from what you already know'.[2537] Both definitions point to the predictive nature of inferences. Although profiling arguably covers most types of automated inferences, some AI systems may be beyond the scope of profiling. Think about speech-based emotion recognition systems as introduced in Section 2.2.4.2 and the real-world examples mentioned in Sections 4.7.1 and 4.9.3. Amazon's patented technology enables Alexa to detect the user's emotional state derived from the user's voice.[2538] Spotify's patented voice assistant[2539] recognises when a user sounds sad and then offers encouragement by 'cheering' the user.[2540] A bank used a speech-based emotion recognition system to predict the emotional states of customers calling the bank's customer support.[2541] In these examples, emotional states are inferred from speech recorded or

[2536] See < https://dictionary.cambridge.org/dictionary/english/inference?q=inferences > accessed 8 February 2024.
[2537] See < https://www.oxfordlearnersdictionaries.com/definition/english/inference?q=inference > accessed 8 February 2024.
[2538] Huafeng Jin, Shuo Wang 'Voice-Based Determination of Physical and Emotional Characteristics of Users' US Patent Number US 10096319 B1 (Assignee: Amazon Technologies, Inc.) October 2018 <https://patentimages.storage.googleapis.com/f6/a2/36/d99e36720ad953/US10096319.pdf> accessed 8 February 2024.
[2539] Daniel Bromand et al, 'Systems and Methods for Enhancing Responsiveness to Utterances Having Detectable Emotion' US Patent Number US 10566010 B2 (Assignee: Spotify AB) February 2020 11 < https://patentimages.storage.googleapis.com/2a/9d/2d/926b58a2bd956f/US10566010.pdf >, accessed 8 February 2024.
[2540] Josh Mandell, 'Spotify Patents A Voice Assistant That Can Read Your Emotions' *Forbes* (New York, 12 March 2020) <https://www.forbes.com/sites/joshmandell/2020/03/12/spotify-patents-a-voice-assistant--that-can-read-your-emotions/> accessed 8 February 2024.
[2541] Sebastião Barros Vale, Gabriela Zanfir-Fortuna, 'Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities' (2022) 48 <https://fpf.org/wp-content/uploads/2022/05/FPF-ADM-Report-R2-singles.pdf> accessed 8 February 2024.

streamed in daily life environments. Arguably, uttered speech and the emotional state derived from this is not necessarily behaviour or a 'personal aspect' as referred to in the definition of profiling. The detected emotional state constitutes an automated inference, as it is a guess based on information (recorded speech) the controller already has. It seems possible that new forms of automated inferences will arise in the future that do not fit the definition of profiling.

Requirement (ii) is intentionally phrased broadly to address some of the problems caused by AI. The term 'potentially' makes clear that not only realised harm is covered by Article 22 but also potential harm. This is needed due to the probability & inaccuracy (Section 4.3.1), common sense and rebuttal (Section 4.7.1), as well as the verification (Section 4.6.2) problems. These problems show that personal data generated by AI may harm the data subject's interest, rights or freedoms. Personal data generated by AI that is inaccurate, contradictory to common sense or cannot be verified due to its probabilistic nature is likely to harm the data subject's interest, rights or freedoms.

For example, ML generates uncertain knowledge such as predictions and correlations that are probabilistic. This may lead to inaccurate evaluations and representations of data subjects because ML often generalises. The use of probabilistic information in the context of a controller's decision-making process can have adverse and detrimental effects for data subjects. Predictions facilitated by ML, such as negative score values, may prevent the data subject from obtaining a loan for buying a house or a mobile subscription. This occurred in a case pending at the CJEU. Due to a poor score value ascribed to the data subject, the mobile network operator denied to prolong a mobile contract subscription with a rather low monthly fee of 10 €.[2542] The AC-powered HireVue software analyses the emotions a candidate portrays during the video assessment[2543] and automatically assigns the candidate with an average rating (score) and recommendation whether the candidate should be employed. It clearly harms the data subject's interest to find employment if the recruiter relies on inaccurate emotion data. Notably, AC technology is also used in sectors other than human resources, including marketing, customer service, healthcare, insurance, retail, autonomous driving, education and gaming.[2544]

Harm may be less obvious for output created by the AI system that merely constitutes the product of probability-based analytic processes (and thus inferred data as outlined in Section 4.4.1 and 4.4.3). Think about ML models that apply dimensionality reduction according to Section 2.2.1.2 on easily

[2542] Case C-203/22 *Dun & Bradstreet Austria* p 2 <https://www.ris.bka.gv.at/Dokumente/Lvwg/LVWGT_WI_20220211_VGW_101_042_791_2020_44_00/LVWGT_WI_20220211_VGW_101_042_791_2020_44_00.pdf> accessed 8 February 2024.
[2543] Nathan Mondragon, Clemens Aicholzer, Kiki Leutner, 'The Next Generation of Assessments' (HireVue 2019) <http://hrlens.org/wp-content/uploads/2019/11/The-Next-Generation-of-Assessments-HireVue-White-Paper.pdf> accessed 8 February 2024.
[2544] Cem Dilmegani, 'Top 24 Affective Computing (Emotion AI) Use Cases in 2023' <https://research.aimultiple.com/affective-computing-applications/> accessed 8 February 2024; Deepanshu Gahlaut, 'Top Emotion AI Companies to Watch out for in 2023' <https://deepanshugahlaut.medium.com/top-emotion-ai-companies-to-watch-out-for-in-2023-db925868fd9f> accessed 8 February 2024.

accessible digital records of behaviour, for example Facebook likes. These models predict the data subject's personality traits[2545] and could be used by a provider of a dating app. When implemented in the dating app, these personality traits could influence 'potential matches' and thus limit the data subject's freedom to choose between possible dating partners.

For these reasons, paragraph 1 of my proposal introduces a *rebuttable presumption* that profiling or automated inferences intended to be used for decision-making harm the data subject's interests, rights and freedoms. If controllers intend to engage in AI-powered processing, they may rebut this assumption and document the corresponding assessment mentioned in paragraph 3 accordingly. The rebuttable presumption of harm contained in paragraph 1 of my proposal is inspired by the EU Commission's proposal for an Artificial Intelligence Liability Directive.[2546] This proposal contains rebuttable presumptions, that are seen as the least interventionist tools because they balance the interests of claimants and defendants. Rebuttable presumptions are common in national liability systems of EU Member States.[2547]

When read together with paragraph 3, requirement (ii) enshrines a two-part human-in-the-loop approach for two reasons. First, it places human involvement at the very start of the processing chain according to the principle of data protection by design and default.[2548] It reinforces this principle which obliges controllers to assess the risks for the data subject's rights and freedoms posed by the envisaged processing and implement the data protection principles enshrined in Article 5 GDPR. In particular, the fairness (as suggested in Section 6.2.2) and accuracy principle will play an important role in this context. Second, a context-driven assessment which takes the interests, rights and freedoms of a particular data subject concerned into consideration is required. For example, profiling or automated inferences in the context of targeted advertisement are less likely to be harmful than profiling or automated inferences that influence the decision-making pursued in a recruitment context. Potential harm is subjective and will always depend on the context and the data subject concerned. A human assessment is needed due to the reasoning and common sense deficiencies in the AI discipline AR. The balancing problem explained in Section 4.2.1 shows that autonomous AI systems cannot balance the fundamental rights and freedoms of the parties involved due to the reasoning and cognitive deficiencies in the AI discipline AR.

[2545] Michal Kosinski, David Stillwell, Thore Graepel, 'Private traits and attributes are predictable from digital records of human behaviour' (2013) Vol 110 No 15 PNAS, 5802.
[2546] 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 <https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf> accessed 8 February 2024.
[2547] AI Liability Directive Proposal at 6 <https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf> accessed 8 February 2024.
[2548] Article 25 GDPR.

Paragraph 3 enables the data subject to obtain the assessment performed by the controller as required by paragraph 1. This assessment outlines why the controller reached the conclusion that profiling or automated inferences are unlikely to harm the data subject's interests, rights and freedoms. When the data subject is not convinced by this assessment, it can exert real influence concerning such processing. Based on the information contained in this assessment, the data subject can enforce its rights provided by the GDPR, namely:

- Lodging a complaint with the competent supervisory authority (Article 77 GDPR)
- Enforcing the right to an effective judicial remedy against the controller (Article 79 GDPR)
- Mandating a representative to exercise its rights (Article 80 GDPR)

The suggested redrafting of Article 22 GDPR arguably achieves what is currently envisaged by this provision. It aims to *effectively protect data subjects* against the particular risks associated with the automated processing of personal data, including profiling.[2549] It also supports data subjects to exercise influence over profiling and decision-making, to reduce concerns over its quality[2550] and to uphold human dignity by ensuring that humans keep the primary role in constituting themselves.[2551] The latter is emphasised by Recital 4 GDPR, which states that 'the processing of personal data should be designed to serve mankind' and requirement (ii) reflects this aim.

The redrafted version significantly broadens this right. By removing the requirement that decision-making involving profiling must be fully automated, it also applies to decisions which are *influenced* by AI. This addresses the problem that personal data generated by AI may create harm for the data subject, in particular when it is subsequently shared with and used by other parties. For example, a poor score value generated by a credit rating agency may prevent data subjects from obtaining a mobile subscription. A low attractivity score in a dating app might suggest potential dating partners that do not match the data subject's expectations and thus limit the data subject's freedom to choose between possible dating partners. The suggested redrafting renders Article 22 GDPR applicable regardless of whether the decisions taken regarding the data subjects are fully automated. The example of the score value used by the mobile network operator for the decision whether or not to prolong a mobile subscription would thus fall under the prohibition of Article 22 GDPR. The revised text of Article 22 GDPR also clarifies that potential harm is sufficient to trigger the protection granted by this right (i.e. the prohibition). Instead of providing data subjects with a procedural safeguard such as the current right to contest to ADM (see Section 5.11.3), it empowers the data subject to obtain the assessment performed by the controller as required by paragraph 1. This information enables the data

[2549] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 57, 60.
[2550] Recital 71 GDPR.
[2551] Isak Mendoza, Lee A Bygrave, 'The Right Not to be Subject to Automated Decisions Based on Profiling' in Tatiana-Eleni Synodinou et al (eds) *EU Internet Law: Regulation and Enforcement* (Springer International 2017) 83-84; Lee A Bygrave, 'Minding the machine v2.0: The EU General Data Protection Regulation and Automated Decision Making' in Karen Yeung and Martin Lodge (eds) *Algorithmic Regulation* (OUP 2019) 249.

subject to exert real influence over such processing and facilitates the enforcement of the data subject's rights enshrined in the GDPR.

6.7.3 Conclusion

In this section, I have argued that the legal solution to solve the cumulativeness problem consists of amending the right not to be subject to ADM. The proposed wording focusses on profiling and automated inferences that potentially harm the data subject's rights, interests or freedoms rather than on 'automated decision-making'. The proposed wording covers decisions which are influenced by profiling generated by AI. It also requires controllers to assess whether profiling, automated inferences and the intended decision-making potentially harm the data subject. Data subjects can obtain this assessment, which allows them to enforce their rights provided by the GDPR, lodging a complaint with an SA or initiating legal proceedings in particular.

6.8 Conclusions

This chapter aimed to answer Subquestion 5, i.e. how the incompatibilities of the current legal framework identified in Subquestions 3 and 4 should be addressed. Based on the selection criteria effectiveness, urgency and novelty, I have addressed six legal problems: the elusiveness, mental data, communication surveillance, trade secrets, verifiability standards and cumulativeness problems.

This chapter has focussed on legal solutions, although technological solutions[2552] should also be explored and developed. I argued that the incompatibilities of the current legal framework can be addressed by the following legal solutions: (i) new interpretations of existing provisions, (ii) amendments of existing provisions or (iii) the introduction of entirely new provisions. Table 6.4 provides an overview of which legal problem should be addressed by which type of legal solution.

Problem (type)	**AI Disciplines**	**Suggested Legal Solution (i, ii or iii)**
Elusiveness (2, 3)	ML, NLP, CV, AC, AR	New interpretation as substantive fairness (i)
Mental data (3)	ML, AC	Introducing dynamic list for special data (iii)
Comm. surveillance (3)	ML, NLP, AC	Regulating human-machine communication (iii)
Trade secrets (2,3)	ML, NLP, CV, AC, AR	Adding a new exception in the TSD (iii)
Verifiability standard (3)	ML, AC	Amending right to rectification (ii)
Cumulativeness (3)	ML, NLP, CV, AC, AR	Redrafting right not to be subject to ADM (ii)

Table 6.4 Outlining legal problems (type), AI disciplines concerned and suggested legal solutions.

[2552] As mentioned in Section 6.1 e.g. randomisation techniques, secure multiparty computation, homomorphic encryption, differential privacy, knowledge-infused learning.

The *elusiveness problem* should be addressed by a new interpretation of the fairness principle. The legal solution consists of interpreting the fairness principle as both procedural and *substantive* fairness. The provisions in the GDPR and the corresponding recitals already provide clarity with respect to procedural fairness. Substantive fairness as suggested here contains two major elements: fairness between the parties and fairness of the outcomes. Several components of substantive fairness should be considered, distributed among the two major elements of substantive fairness. These components are power inequalities/dominant positions, vulnerability, good faith, autonomy, non-manipulation, detrimental effects, accuracy and non-discrimination. To ultimately 'solve' the elusiveness problem, judicial action is needed. The CJEU should interpret fairness in EU data protection law as including both procedural and substantive fairness.

The proposed legal solution for the *mental data problem* consists of the introduction of a new dynamic list for special data. This solution overcomes the current problem that the approach to enumerate special data exhaustively is not fit for purpose to address the challenges caused by AI as it does not keep up with technological developments. In my suggested solution, the European Commission is empowered to adopt new delegated acts for the purpose to update the list of special data where needed due to technological developments. This solution is flexible and comes with legal certainty for all actors involved.

The proposed legal solution for the *communication surveillance problem* consists of two new provisions to be included in the future ePrivacy Regulation. The first new provision specifically regulates the confidentiality of human-machine communication. According to this provision, the surveillance of human-machine communication is prohibited unless it is specifically permitted, i.e. if processing of human-machine communication is strictly necessary to facilitate such communication or if the user has explicitly provided consent. The second new provision defines human-machine communication broadly. For the sake of legal certainty, the scope of the future ePrivacy Regulation should be extended by specifically including human-machine communication. Taken together, these provisions solve the current gap of protection regarding the confidentiality of human-machine communication.

The proposed legal solution for the *trade secrets problem* consists of a new exception to be included in Article 5 TSD. This new provision clarifies that trade secret protection under the TSD does not apply if data subjects enforce their right of access according to Article 15 (3) GDPR. This strengthens the position of data subjects. It enables them to enforce their data subject rights with regard to personal data generated by AI. This exception is justified because the right of access constitutes a conditio sine qua non for all other data subject rights. In addition, providing data subjects with a copy of their own personal data seems unlikely to harm the controller's interests specifically protected by the TSD. This protects a company's business and financial interests, strategic position and ability to compete.

The *verifiability standard problem* should be addressed by amending the right to rectification. I suggest adding an additional paragraph in Article 16 GDPR. This paragraph broadens the right to rectification regarding the processing of personal data generated by automated means and empowers data subjects to easily contest the accuracy of such personal data. When data subjects contest the accuracy, 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 prevail. This new paragraph solves the verifiability standard because data subjects are not required to provide objectively verifiable evidence when asking for the rectification of unverifiable and subjective personal data generated by AI.

The proposed legal solution for the *cumulativeness problem* consists of the redrafting of the right not to be subject to ADM. The proposed wording focusses on profiling and automated inferences instead of 'automated decision-making'. 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. The redrafted provision assumes harm if profiling or automated inferences is intended to be used for decision-making on the data subject concerned. Data subjects can obtain the assessment performed by the controller, which allows them to enforce their rights enshrined in the GDPR, in particular lodging a complaint with an SA or initiate legal proceedings. My proposed solution gets rid of the cumulativeness problem and enables data subjects to exercise real influence regarding profiling and automated inferences enabled by AI.