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

Häuselmann, A.N.

5 Legal problems: Rights

This chapter aims to answer Subquestion 4, namely, what legal problems arise or may arise when the enforceable rights enshrined in the current EU legal framework are applied to AI. Section 5.1 introduces the approach taken to assess the legal problems. Sections 5.2 through 5.5 elaborate on the fundamental right to privacy introduced in Section 3.1 and discuss four dimensions of privacy that are derived from the elements contained in the text of the fundamental right to privacy and the corresponding case law. These four dimensions are informational privacy (Section 5.2), bodily privacy (Section 5.3), mental privacy (Section 5.4) and communicational privacy (Section 5.5). Sections 5.6 through 5.11 do the same for the fundamental right to data protection as introduced in Section 3.2. I focus on the enforceable rights that data subjects have according to the GDPR because they implement the requirements enshrined in the fundamental right to data protection.[1448] Strong[1449] and effective data subject rights[1450] constitute a prerequisite for the protection of personal data. These enforceable rights are the right of access (Section 5.6), the right to rectification (Section 5.7), the right to erasure (Section 5.8), the right to data portability (Section 5.9), the right to object (Section 5.10) and the right not to be subject to automated decision-making (Section 5.11). Section 5.12 concludes.

Note that transparency requirements according to Articles 12-14 GDPR technically do not belong to the enforceable rights of data subjects although they are listed under data subject rights. Rather, these provisions are the manifestations of the transparency principle[1451] which I discussed in Section 4.4.

5.1 Approach

The approach for assessing legal problems related to the rights enshrined in the current legal framework is the same as introduced in Section 4.1. When referring to legal problems, three types of legal problems are distinguished, namely, Type 1 (legal provisions are violated), Type 2 (legal provisions cannot be enforced) and Type 3 (legal provisions are not fit for purpose to protect the fundamental right at stake). Type 3 legal problems are discussed from the perspective of *natural persons* as the primary subject of protection envisaged by fundamental rights. These types of legal problems are identified by means of the rationales and specific aims pursued by the current legal framework as outlined in Section 4.1 (see Table 4.2 therein). To determine which type of legal problem arises or may arise due to different AI disciplines, as outlined in Chapter 2, the AI disciplines are mapped with the enforceable rights contained in the current legal framework. For each right enshrined in the current

[1448] Case C-131/12, *Google Spain* [2014] ECR I-317 para 69; Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081, Opinion of AG Sharpston para 55.
[1449] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[1450] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[1451] Case C-487/21, *F.F.* [2022] ECR I-1000 para 37.

legal framework, I assess whether the enforceable right at hand creates Type 1, 2 or 3 legal problems. When doing so, I follow the order of the AI disciplines outlined in Chapter 2.

Before getting started, I shall explain the focus I have chosen with respect to the fundamental right to privacy. The latter states that everyone has the right to respect for his or her private life, home and communications.[1452] Due to the broad scope of the fundamental right to privacy, I focus on four dimensions[1453] of this right that are particularly relevant in the light of AI: informational, bodily, mental and communicational. These dimensions are derived from the elements contained in the text of the fundamental right to privacy and corresponding case law.[1454] Table 5.1 maps the elements of the right to privacy derived from the text and corresponding case law with the dimensions of privacy that are discussed in this chapter.

Element of the fundamental right to privacy	**Dimension**
private life	informational privacy
private life (physical integrity)	bodily privacy
private life (mental integrity)	mental privacy
correspondence/communications	communicational privacy

Table 5.1 Mapping elements contained in the text of the fundamental right to privacy in Article 8 ECHR and corresponding case law with dimensions of the right to privacy discussed in Section 3.1.

Let me explain why I have chosen to focus on these four dimensions of privacy. First, the right to privacy provides individuals with a form of informational self-determination,[1455] which is an extremely important dimension in the context of AI because the latter relies heavily on the processing of information. I discuss informational privacy in Section 5.2. Furthermore, physical and mental integrity, two elements falling under the term 'private life' as developed in corresponding case law [1456] are particularly relevant in the context of AI. I consider these two elements to be important because some AI disciplines such as affective computing and machine learning deal with body functions and characteristics (e.g., genetic codes, biometrics, physiological information) and aim to gain access to

[1452] Art 8 ECHR, Art 7 EUCFR.
[1453] Note that I refrain from elaborating on the elements 'family life' and 'home' contained in the text of the fundamental right to privacy because these elements do not seem to be particularly relevant in the context of AI. The element 'family life' essentially relates to the right to live together so that family relationships may develop normally and those members of the family may enjoy each other's company. See *Marckx v. Belgium* App no 6833/74 (ECtHR 13 June 1979) para 31; *Olsson v. Sweden* (No. 1) App no 10465/83 (ECtHR 24 March 1988) para 59. Possible interferences with the right to respect for one's home include examples such as police entry into a person's home, including searches and seizures, and displacements from home. See *Murray v. the United Kingdom* App no 14310/88 (ECtHR 28 October 1994) para 86; *Burlya and others v. Ukraine* App no 3289/10 (ECtHR 6 February 2019) para 166.
[1454] See also Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law.
[1455] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR 27 June 2017) para 137.
[1456] *Denisov v Ukraine* App no 76639/11 (ECtHR 25 September 2018) para 95, *S. and Marper v United Kingdom* App no 30562/04 and 30566/04 (ECtHR 4 December 2008) *Pretty v United Kingdom* App no 2346/02 (ECtHR 29 April 2002) para 63.

mental states of individuals (such as thoughts, feelings, emotional states). I discuss the element of physical integrity under the dimension of bodily privacy (Section 5.3) and the element of mental integrity under the dimension of mental privacy (Section 5.4). Finally, communication also constitutes an important element in the context of AI, as AI might interfere with the right to respect confidential communication because it computes communications in various forms, for example, by means of natural language processing and machine learning. I discuss the element of communication under the dimension of communicational privacy (Section 5.5).

5.2 Informational privacy

Informational privacy refers to the idea that data and images from individuals should not be automatically available to others[1457] and that individuals may 'exercise a substantial degree of control over that data and its use'.[1458] According to ECtHR case law, the right to privacy provides individuals with a form of informational self-determination[1459] which indicates that individuals should be able to exercise control with regard to the use of their information. Informational privacy should be understood as an overarching concept[1460] rather than a separate type or form of privacy.[1461] All AI disciplines as described in Chapter 2 process various types of information. In this section, I examine how these AI disciplines may lead to legal problems when applied to informational privacy.

5.2.1 Legal problems: Type 1

Research has shown that ML models can successfully identify markers of depression by analysing photographic data from Instagram accounts, and these models even outperformed general practitioner's average diagnostic success rate for depression.[1462] This implies that sensitive information about individuals can be inferred and disclosed to others beyond the individual's control, which contradicts their right to informational self-determination.[1463]

An ML-powered system that aims to analyse customer behaviour from large volumes of customer transaction data can make accurate predictions based on patterns and correlations identified in past customer behaviour.[1464] This could reveal information an individual arguably did not want to disclose.

[1457] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 8; Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law 438, 568.
[1458] Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Roger Clarke's Website, 24 July 2016) < http://www.rogerclarke.com/DV/Intro.html > accessed 8 February 2024.
[1459] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR 27 June 2017) para 137.
[1460] Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law 438, 568-569.
[1461] Bart Custers, *The Power of Knowledge* (Wolf Legal Publishers 2004) 145.
[1462] Andrew G Reece, Christopher M Danforth, 'Instagram photos reveal predictive markers of depression' (2017) Vol. 6 No. 15 EPJ Data Science, 1, 8.
[1463] *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no 931/13 (ECtHR 27 June 2017) para 137.
[1464] Ethem Alpaydin, *Machine Learning: The New AI* (3rd edn MIT Press 2016) 14.

A famous example is the so-called 'pregnancy prediction' score for female customers who paid with a credit card or used a loyalty card. Based on two dozen products used as proxies, the prediction model could identify pregnant customers when analysing their past shopping cart.[1465] ML approaches, for example clustering as described in Section 2.2.1.2, may infer an individual's home and work location from widely available location metadata in public data streams like Twitter.[1466] ML approaches can also infer even more sensitive information pertaining to health, religion and nightlife from location metadata through the reconstruction of a user's location history[1467] (see also Section 4.8.3). ML models that apply dimensionality reduction (see Section 2.2.1.2) on easily accessible digital records of behaviour, for example Facebook likes, may reveal and predict highly sensitive personal attributes such as sexual orientation, ethnicity, religious and political views and personality traits.[1468] Facebook users seem to have no control to prevent that such sensitive information will subsequently be revealed at the moment they click on the like button. In addition, arguably anonymised information could identify individuals when analysed by means of ML. According to a study which deployed ML approaches, 99.98% of the population of a US state could be uniquely re-identified in any dataset using fifteen demographic attributes.[1469] This study also demonstrates that identification can be estimated with high accuracy even when the anonymised dataset is heavily incomplete, which rejects claims that re-identification is not a practical risk.[1470]

Speech recordings, if analysed by AI, can reveal not only an individual's identity, but also gender, age, native language, emotional state[1471] and information related to individual's personality traits, degree of sleepiness or intoxication and physical and mental health, as well as socioeconomic status.[1472] Individuals are often unaware of being recorded and have limited means to control what information is inferred from their recorded speech through ML and NLP approaches. For example, Amazon has patented a version of its virtual assistant Alexa that (arguably) is able to detect whether a user is ill and then subsequently offer medicine.[1473] This raises the question whether a user wants to reveal such information in the first place and how effective control can be exercised when an individual does not

[1465] Viktor Mayer-Schönberger; Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Houghton Mifflin Harcourt 2013) 58.
[1466] Drakonakis Kostas et al, 'Please Forget Where I Was Last Summer: The Privacy Risks of Public Location (Meta) Data' (2019) 2 <https://arxiv.org/pdf/1901.00897.pdf> accessed 8 February 2024.
[1467] Ibid 1.
[1468] 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.
[1469] Luc Rocher, Julien M Hendrickx, Yves-Alexandre de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) Vol 10 Nature Communications 1.
[1470] Ibid 2.
[1471] Andreas Nautsch et al, 'Preserving privacy in speaker and speech characterisation' (2019) Vol 58 Computer Speech & Language 441, 444.
[1472] For more detailed information and related studies, see Jacob Leon Kröger, Otto Hans-Martin Lutz, Philip Raschke, 'Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference' in Michael Friedewald et al (eds) *Privacy and Identity management. Data for Better Living: AI and Privacy* (Springer 2020) 243.
[1473] James Cook, 'Amazon patents new Alexa feature that knows when you're ill and offers you medicine' *The Telegraph* (London 9 October 2018) < https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/> accessed 8 February 2024.

want to reveal such information. NLP approaches embedded in virtual assistants, such as Amazon Alexa or smart home applications (e.g., smart fridges and beds), provide the technical means to track and monitor individuals in an unprecedented manner. By deploying the most recent NLP and speech recognition techniques, virtual assistants such as Siri, Google Assistant and Amazon Alexa may effortlessly recognise when a person is praying and thus reveal rather sensitive information.

Behavioural inference systems that deploy CV and ML techniques in retail spaces allow fine-grained tracking of the shoppers' behaviour and characteristics.[1474] Possibilities for shoppers to truly avoid this is difficult, if possible, at all.[1475] CV allows one to identify people based on gait. Biometric information necessary for doing so may be captured in public spaces and from a distance.[1476] For example, the police in China can identify suspects by their gait and silhouette from up to 50 metres distance, even when a person's face is covered or pretends to have a limp or hunch.[1477] The same technology can be applied in semi-public spaces such as connected retail spaces for commercial purposes. In particular, when integrated into existing surveillance systems, face recognition (see Section 2.2.3.1) and automated face analysis (AFA) systems (see Section 2.2.4.1) pose serious risks to informational privacy since they do not require the awareness or cooperation of individuals involved. The same applies to situations where AFA systems make use of digital images uploaded on the Internet, e.g. on social media, as such processing may occur without any involvement or awareness by the individuals concerned.[1478]

This is not only a theoretical risk, as the Clearview AI case clearly underscores. The company Clearview AI Inc. collected, by means of web scraping techniques, images and relevant metadata available online and further processed such biometric data in its AFA system. The Italian supervisory authority imposed a fine on the company for the violation of several provisions of the GDPR.[1479] AFA systems may not only be deployed in public or semi-public spaces. Volvo plans to install on-board cameras in their cars that can be used for identifying the driver based on face recognition systems described in Section 2.2.3.1 to automatically set climate control and seating position according to the preferences of the driver.[1480] Surveillance systems in public spaces may identify individuals participating in

[1474] In-store tracking of shoppers that are being identified based on their observable characteristics such as height, colour, width as described in a patent of 7-Eleven Inc. <https://patents.google.com/patent/US11107226B2/en> accessed 8 February 2024.
[1475] Vasilios Mavroudis, Michael Veale 'Eavesdropping Whilst You're Shopping: Balancing Personalisation and Privacy in Connected Retail Spaces' (Living in the Internet of Things Conference, London, March 2018) 4 <https://ieeexplore.ieee.org/document/8379705> accessed 8 February 2024.
[1476] See Section 2.2.3 (CV).
[1477] Chiara Giordano, 'Chinese police use surveillance technology to identify people by their walking style' *The Independent* (London 26 February 2019) <https://www.independent.co.uk/news/world/asia/china-police-walking-gait-technology-surveillance-ai-suspect-a8797836.html> accessed 8 February 2024.
[1478] Council of Europe, Consultative Committee of Convention 108, 'Guidelines on Facial Recognition' (28 January 2021) at 3 <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> accessed 8 February 2024.
[1479] See <https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en> accessed 8 February 2024.
[1480] 'Volvo to install in-car cameras to watch over drivers' *CAR magazine* (London 20 March 2019) <https://www.carmagazine.co.uk/car-news/tech/volvo-driver-cameras/> accessed 8 February 2024.

political activities, for example, protests, by means of CV approaches such as gait recognition and/or facial recognition.

AC can be applied in various contexts such as recruitment, casinos, restaurants, retail, hospitality and call centres and is prone to violate an individual's right to informational privacy because it gains access to the emotions of the individual beyond their control. Candidates participating in video assessments that use software that analyses their emotions based on AC techniques can hardly determine themselves to what extent their emotional state is shared with the prospective employer. Likewise, users of virtual assistant Alexa cannot control whether Amazon will use technology that enables Alexa to recognise the user's emotional state derived from the user's voice[1481] and how such information is further processed. AC provides an unprecedented means to gain access to information related to the emotional state of individuals beyond their control. It seems difficult, if possible, at all, for individuals to determine themselves whether they want, in fact, to provide access to such information.

The control problem (Type 1)

The AI disciplines discussed in Chapter 2 undermine the right to informational privacy because individuals can hardly determine to reveal certain information or not. AI can infer such information anyway, beyond the individual's control, and therefore violates the right to informational privacy.

5.2.2 Legal problems: Type 2

No specific Type 2 legal problems arise when the AI disciplines introduced in Chapter 2 are applied to informational privacy. The fundamental right to privacy has been extensively enforced, which is underscored by the wealth of case law produced by both the ECtHR and the CJEU regarding the fundamental right to privacy. According to the HUDOC database maintained by the ECtHR, at least 12,323 cases dealt with the fundamental right to privacy within the last ten years.[1482] There are no indications that the enforcement of the fundamental right to privacy will decrease in the future because of AI.

5.2.3 Legal problems: Type 3

The broad scope of the fundamental right to privacy, along with the ECtHR's refusal to define the ambit of it,[1483] enabled the ECtHR to continuously respond to modern legal dilemmas and human

[1481] 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.
[1482] See HUDOC database accessed 8 February 2024.
[1483] Frederik Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting' (Doctoral thesis, Universiteit van Amsterdam 2015) 100 <https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5> accessed 8 February 2024.

rights challenges[1484] and adapt the protection to new circumstances and technological and societal developments.[1485] As introduced in Section 3.1.2, this dynamic approach to interpretation has been coined the 'living instrument doctrine'.[1486] This ensures that the fundamental right to privacy is interpreted and applied in the light of present-day conditions, thus considering, inter alia, technological developments and the issues to which these may raise.[1487] The living instrument doctrine also affects case law adopted by the CJEU.[1488] The ECtHR stressed that it will consider the extent to which 'intrusions into private life are made possible by new, more and more sophisticated technologies'[1489]. In my view, this statement addresses the technological developments facilitated by AI perfectly. Therefore, no specific Type 3 legal problems arise when AI is applied to the fundamental right to privacy.

5.3 Bodily privacy

Bodily privacy relates to the right to keep body functions and characteristics (e.g., genetic codes and biometrics) private. It specifically relates to the integrity of a person's body[1490] and physical access to it, but also encompasses the restriction and control of information about the body.[1491] Whereas traditional examples such as compulsory immunisation or blood transfusion without consent[1492] include physical and unsolicited harms to the body,[1493] examples in the context of AI shift the focus to information that is gained from a person's body and its functions without physically intruding the body, such as accessing the body by means of devices, for example, wearables that measure physiological signals. In this context, it is important to consider the distinction between informational and bodily privacy. Bodily privacy refers to access to the human body, and informational privacy relates to the observations that can be made by analysing the information gained from the human body. In other words, bodily privacy concerns the protection of the actual object of privacy which can be directly intruded, i.e. the body, and informational privacy concerns the protection of information that may be obtained by analysing the body, but not the body itself.[1494]

[1484] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 569, 570.
[1485] Frederik Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting' (Doctoral thesis, Universiteit van Amsterdam 2015) 100 <https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5> accessed 8 February 2024.
[1486] Alastair Mowbray, 'The Creativity of the European Court of Human Rights' (2005) Vol 5 Iss 1 Human Rights Law Review 57-59.
[1487] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 509.
[1488] Case C-400/10, *J. McB.* [2010] ECR I-582 para 53. See also Article 52 (3) EUCFR which states that the 'meaning and scope' of the rights contained in the EUCFR and ECHR shall be the same, provided that these rights 'correspond'. This holds true for Article 8 ECHR and Article 7 EUCFR.
[1489] *Köpke v Germany*, App No 420/07 (EctHR 05 October 2010) emphasis added.
[1490] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 7, 8.
[1491] Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law 438, 569.
[1492] Roger Clarke, 'What's Privacy' (Roger Clarke's Website, 7 August 2008) <http://www.rogerclarke.com/DV/Privacy.html> accessed 8 February 2024.
[1493] Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law 438, 498.
[1494] Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law 438, 555.

5.3.1 Legal problems: Type 1

Two AI disciplines are particularly relevant in the context of bodily privacy, namely, ML and AC. In what follows, I outline why these two AI disciplines cause legal problems regarding the right to bodily privacy.

Brain-computer interfaces (BCI), which are often powered by ML and DL,[1495] impact bodily privacy because they monitor physiological signals. Non-invasive BCIs, which are currently most widely used in BCI research, place sensors on the scalp to acquire electroencephalography (EEG) signals.[1496] EEG measures electrical impulses emitted by the brain.[1497] Companies develop consumer-directed wearable devices to record brain activity based on EEGs, leading to the analysis of information concerning brain activity on a large scale.[1498] BCI applications use different ML techniques for the classification of EEG signals.[1499] Neuroadaptive technologies combine AI with implantable BCIs which automatically adapt to the user's mindset without requiring explicit instructions.[1500] The company Neuralink develops a BCI system that aims to establish a direct link between the brain and everyday technology. The system records neural activity in the brain and as the user thinks about moving her arms or hands, the system decodes those intentions by means of ML and DL approaches. At a first stage, this technology is intended for individuals with paralysis and neurological disorders to regain independence by giving them the ability to control computers and mobile devices directly with their brains. Later, Neuralink intends to discover new, non-medical applications and make them available to the general population.[1501] This BCI system relies upon a small, wireless, battery-powered neural implant unseen from the outside of the body.[1502] Neuralink has already successfully implanted the device in the brains of a monkey and a pig. The company published a video showing the monkey that had been implanted with the neural device playing the video game Pong using only its mind.[1503] These approaches are invasive and physically access the body and therefore impact the physical integrity of the individuals concerned.

[1495] Mamunir Rashid et al, 'The classification of EEG Signal Using Different Machine Learning Techniques for BCI Application' in J.-H. Kim et al (Eds) *Robot Intelligence Technology and Applications* (Springer 2018) 207-221.
[1496] Hongchang Shan, 'Towards High Performance and Efficient Brain Computer Interface Character Speller: Convolutional Neural Network based Methods' Dissertation Universiteit Leiden 2020, 2.
[1497] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 7, 8.
[1498] Philipp Kellermayr, 'Big Neurodata: On the Responsible Use of Neurodata from Clinical and Consumer-Directed Neurotechnological Devices' (2018) 1, 2 <https://link.springer.com/article/10.1007/s12152-018-9371-x> accessed 8 February 2024.
[1499] Mamunir Rashid et al, 'The classification of EEG Signal Using Different Machine Learning Techniques for BCI Application' in J.-H. Kim et al (Eds) *Robot Intelligence Technology and Applications* (Springer 2018) 207-221.
[1500] Marcello Ienca, Gianclaudio Malgieri, 'Mental data protection and the GDPR' (2022) Vol 9 Iss 1 Journal of Law and the Biosciences 1, 4.
[1501] See the company's website <https://web.archive.org/web/20230331035227/https://neuralink.com/applications/> accessed 8 February 2024.
[1502] Emily Waltz, 'Elon Musk Announces Nuralink Advance Toward Syncing Our Brains With AI' *IEEE* (New York 28 August 2020) <https://spectrum.ieee.org/elon-musk-neuralink-advance-brains-ai> accessed 8 February 2024.
[1503] Rupert Neate, 'Elon Musk's brain chip firm Neuralink lines up clinical trials in humans' *The Guardian* (London 20 January 2022) <https://www.theguardian.com/technology/2022/jan/20/elon-musk-brain-chip-firm-neuralink-lines-up-clinical-trials-in-humans> accessed 8 February 2024.

Because measurable physiological changes such as changes in heart rate, galvanic skin response, muscle tension, breathing rate and electrical activity in the brain co-occur with emotions, AC technologies sense these changes and recognise emotion by detecting patterns that capture physiological responses.[1504] For example, a statistically significant increase in heart rate could be linked to the activation of the sympathetic nervous system, arguably due to the occurrence of anxiety.[1505] Therefore, AC is particularly relevant for bodily privacy. Because physiological signals cannot easily be controlled[1506] and are involuntary, they are considered to constitute a reliable method for emotion recognition.[1507] Wearables facilitate the monitoring of physiological signals in unprecedented ways and are therefore particularly suitable for emotion recognition. Such devices have the ability to detect signals from skin conductivity, skin temperature, heart rate and other emotion-related physiological parameters.[1508] Combined with ML approaches such as regression as explained in Section 2.2.1.1, wearables provide powerful means to develop emotion recognition systems.[1509] Emotion recognition systems based on physiological signals using wearables may monitor such signals in an unobtrusive manner.[1510] Research deploying ML approaches achieved high accuracy in detecting amusement and sadness by relying on an instrumented glove developed to acquire galvanic skin response signals and information about heart rate.[1511] Admittedly, the collection of bodily information through wearables and BCI as such is already problematic concerning bodily privacy. However, AI allows for inferences of bodily functions based on mere observations of the body. In this sense, AI can invade bodily integrity without touching the human body.

The two AI disciplines AC and ML (particularly DL) are highly dependent on physiological signals and body functions. In the case of body implants, physical access to the body is gained, which consequently violates the integrity of an individual's body. ML and AC technologies sense physiological signals by non-invasive means (e.g., wearables) and thus gain indirect access to the body through devices that measure physiological signals. Because bodily privacy encompasses the restriction and control of information about the body, non-invasive means also violate the right to bodily privacy since they monitor physiological signals such as changes in heart rate, galvanic skin response,

[1504] Jennifer Healey, 'Physiological Sensing of Emotion' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 204.
[1505] Francisco Lupiáñez-Villanueva et al, 'Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation' (2022) 98 <https://op.europa.eu/o/opportal-service/download-handler?identifier=606365bc-d58b-11ec-a95f-01aa75ed71a1&format=pdf&language=en&productionSystem=cellar&part=> accessed 8 February 2024.
[1506] Lin Shu et al, 'A Review of Emotion Recognition Using Physiological Signals' (2018) Vol 18 Iss 7 Sensors 2.
[1507] Juan Antonio Domínguez-Jiménez, 'A machine learning model for emotion recognition from physiological signals' (2020) Vol 55 Biomedical Signal Processing and Control 1.
[1508] Lin Shu et al, 'A Review of Emotion Recognition Using Physiological Signals' (2018) Vol 18 Iss 7 Sensors 32.
[1509] Değer Ayata, Yusuf Yaslan, Mustafa Kamasak, 'Emotion Recognition from Multimodal Physiological Signals for Emotion Aware Healthcare Systems' (2020) Vol 40 149-157.
[1510] Juan Antonio Domínguez-Jiménez et al, 'A machine learning model for emotion recognition from physiological signals' (2020) Vol 55 Biomedical Signal Processing and Control 1.
[1511] Ibid 1, 3.

breathing rate and electrical activity in the brain. AI systems deploy approaches in ML and DL in particular to make use of information derived from the human body and its functions.

The bodily information problem (Type 1)

ML, DL and AC are highly dependent on bodily information, including its functions, by gaining physical access to the body (e.g., implants) or by non-invasive means, e.g. wearables sensing physiological signals such galvanic skin response, and electrical activity in the brain. These technologies violate the right to bodily privacy, as they invade bodily integrity by allowing for inferences of bodily functions based on observed data, either by intervening with an individual's right to keep bodily functions and characteristics private or by gaining physical access to the body.

5.3.2 Legal problems: Type 2

No specific Type 2 legal problems arise when the AI disciplines introduced in Chapter 2 are applied to bodily privacy for the same reasons as outlined in Section 5.2.2. The fundamental right to privacy has been extensively enforced in the past ten years, [1512] and there are no indications that the enforcement of the fundamental right to privacy will decrease in the future due to AI.

5.3.3 Legal problems: Type 3

No specific Type 3 legal problems arise when AI is applied to the right to bodily privacy for the same reasons as outlined in Section 5.3.2. The broad scope of the fundamental right to privacy and the 'living instrument doctrine'[1513] ensure that this right keeps up with technological developments,[1514] including AI.

5.4 Mental privacy

Mental privacy refers to controlling access to the mind and thus to information about mental processes and states.[1515] As such, mental privacy has not yet been recognised as a specific element falling under the notion of private life as enshrined in the fundamental right to privacy. However, the right to mental privacy may be derived from existing ECtHR case law on the right to privacy, in particular from the notions *psychological*[1516] and *moral integrity*[1517] covered therein. According to ECtHR case law, the

[1512] See HUDOC database accessed 8 February 2024.
[1513] Alastair Mowbray, 'The Creativity of the European Court of Human Rights' (2005) Vol 5 Iss 1 Human Rights Law Review 57-59.
[1514] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 509.
[1515] Abel Wajnerman Paz, 'Is Mental Privacy a Component of Personal Identity?' (2021) Vol 15 Fronties in Human Neuroscience 2.
[1516] *Botta v Italy* App no 21439/93 (EctHR 24 February 1998) para 32, *Pretty v United Kingdom* App no 2346/02 (EctHR 29 April 2002) para 61; *Tysiąc v Poland* App no 5410/03 (EctHR 24 September 2007) para 107.
[1517] *Gladysheva v Russia* App no 7097/10 (EctHR 6 December 2011) para 93, *Bensaid v United Kingdom* App no 44599/98 (EctHR 6 February 2001) para 47.

term ‘private life’ also encompasses a person’s psychological[1518] and moral integrity.[1519] In its jurisprudence, the ECtHR did not define *moral integrity*, but this term seems to be related to both dignity and freedom from coercion with respect to choices with respect to one’s own decisions or as a sense of non-invasion by outside influences.[1520] The ECtHR regards mental health as a crucial part of private life associated with the aspect of moral integrity.[1521] Neither ECtHR case law nor scholarship thoroughly examine the term *‘psychological integrity’* in the context of the right to privacy.[1522] However, harm to reputation also constitutes harm to psychological integrity,[1523] or the suffering from maltreatment without physical marks such as deprival of sleep.[1524] Thus, psychological integrity does not necessitate the suffering from mental disorders in a clinical-pathological sense.[1525] Although ‘moral’ and ‘psychological’ integrity may have slightly diverging meanings, there are no indications that they fall outside the remit of the right to privacy considering that the ECtHR repeatedly emphasised the broad interpretation of private life.[1526] Therefore, it seems likely that a right to mental privacy could be derived from or at least developed within the ECtHR’ future jurisprudence with respect to the fundamental right to privacy and particularly the notion of private life.[1527] It seems plausible that the fundamental right to privacy protects mental privacy[1528] because this fundamental right is well equipped to cover all conceivable mental privacy interests that should enjoy legal protection.[1529] This holds particularly true when considering the ECtHR’s living instrument doctrine as explained in Section 3.1.2 which requires one to apply the right to privacy in the light of present-day conditions, taking into account, inter alia, technological developments and the issues these may raise.

Mental privacy has never been considered thoroughly because, traditionally, the mind has not been conceived as an entity vulnerable to external intrusions and therefore in need of legal protection.[1530]

[1518] *Botta v Italy* App no 21439/93 (EctHR 24 February 1998) para 32, *Pretty v United Kingdom* App no 2346/02 (EctHR 29 April 2002) para 61; *Tysiąc v Poland* App no 5410/03 (EctHR 24 September 2007) para 107.
[1519] *Gladysheva v Russia* App no 7097/10 (EctHR 6 December 2011) para 93, *Bensaid v United Kingdom* App no 44599/98 (EctHR 6 February 2001) para 47.
[1520] Jill Marshall, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff Publishers 2009) 168, 184.
[1521] *Bensaid v United Kingdom* App no 44599/98 (EctHR 6 February 2001) para 47; *Dolenec v Croatia* App no 25282/06 (EctHR 26 November 2009) para 165.
[1522] For an overview concerning relevant literature, see Footnote 57 on page 397 in Jan-Christoph Bublitz, ‘The Nascent Right to Psychological Integrity and Mental Self-Determination’ in Andreas van Arnauld, Kerstin von der Decken, Mart Susi (eds.), *The Cambridge Handbook of New Human Rights* (Cambridge University Press 2020).
[1523] *Kyriakides v Cyprus* App no 39058/05 (ECtHR 16 October 2008); *A. v Norway* App no 28070/06 (ECtHR 9 April 2009); *Axel Springer v Germany* App no 39954/08 (ECtHR 7 February 2012).
[1524] *Bati and others v Turkey* App nos 33097/96 and 57834/00 (ECtHR 3 June 2004).
[1525] Jan-Christoph Bublitz, ‘The Nascent Right to Psychological Integrity and Mental Self-Determination’ in Andreas van Arnauld, Kerstin von der Decken, Mart Susi (eds.), *The Cambridge Handbook of New Human Rights* (Cambridge University Press 2020) 396.
[1526] Ibid 395, 396.
[1527] Sjors Ligthart et al, ‘Forensic Brain-Reading and Mental Privacy in European Human Rights Law: Foundations and Challenges’ (2021) Vol 14 Neuroethics 191, 200 <https://link.springer.com/content/pdf/10.1007/s12152-020-09438-4.pdf> accessed 8 February 2024.
[1528] Thomas Douglas, Lisa Forsberg, ‘Three Rationales for a Legal Right to Mental Integrity’ in: Sjors Ligthart et al (eds) *Neurolaw Palgrave Studies in Law, Neuroscience, and Human Behavior* (Palgrave Macmillan 2021) 184.
[1529] Sjors Ligthart, ‘Freedom of thought in Europe: do advances in ‘brain-reading’ technology call for revision?’ (2020) Vol 7 Iss 1 Journal of law and the biosciences 4.
[1530] Jan Christoph Bublitz, Reinhard Merkel, ‘Crimes against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination’ (2014) Vol 8 Iss 1 Criminal Law and Philosophy 51, 61; Sjors Ligthart, ‘Freedom of

For the purpose of this thesis, I interpret mental privacy broadly referring to information related to 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 ('mental privacy').[1531] Given the broad scope of mental privacy, it also comprises privacy of thoughts and feelings, which refers to the right of individuals not to share their feelings and thoughts or to have them revealed. This type of privacy emphasises that individuals should be able to think or feel whatever they like.[1532]

In addition, the meaning of thought must be interpreted broadly to include emotional states because research demonstrates that emotion and cognition are interrelated phenomena and that good decision-making seems to require emotional capacities.[1533] Such a broad interpretation is also in line with case law adopted by the ECtHR regarding the freedom of thought enshrined in Article 9 ECHR, which interprets this notion broadly considering the comprehensiveness of the concept of thought.[1534] However, this right is a neglected human right[1535] and has never played a decisive role in legal practice which is why its scope and meaning remain vague.[1536] Also, it is arguable that the freedom of thought protected by Article 9 ECHR relates much more to the freedom of religion and conscience than thoughts per se. It is beyond of the scope of this thesis to elaborate on this in more detail, but freedom of thought might become more relevant in the future and even provide stronger legal protection for thoughts[1537] than the fundamental right to privacy because it does not allow any interference given its absolute character.[1538]

While the body may easily be subject to domination and control by others, mental states have until recently been beyond external constraints.[1539] Advances in AI and neuroscience are changing

thought in Europe: do advances in 'brain-reading' technology call for revision?' (2020) Vol 7 Iss 1 Journal of law and the biosciences 2.

[1531] 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.

[1532] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 19.

[1533] Jan Christoph Bublitz, Reinhard Merkel, 'Crimes against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination' (2014) Vol 8 Iss 1 Criminal Law and Philosophy 51, 64.

[1534] *Salonen v Finland* App no 27868/95 (ECtHR 2 July 1997).

[1535] Sjors Ligthart, 'Freedom of thought in Europe: do advances in 'brain-reading' technology call for revision?' (2020) Vol 7 Iss 1 Journal of law and the biosciences 3.

[1536] Jan Christoph Bublitz, Reinhard Merkel, 'Crimes against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination' (2014) Vol 8 Iss 1 Criminal Law and Philosophy 51; Leonard M Hammer, *The international human right to freedom of conscience: some suggestions for its development and application* (Ashgate 2001).

[1537] Sjors Ligthart et al, 'Forensic Brain-Reading and Mental Privacy in European Human Rights Law: Foundations and Challenges' (2021) Vol 14 Neuroethics 191, 200 <https://link.springer.com/content/pdf/10.1007/s12152-020-09438-4.pdf> accessed 8 February 2024.

[1538] Article 9 (1) EUCHR which does not allow for any interferences, as opposed to the right to the right to privacy according to Article 8 EUCHR.

[1539] Marcello Ienca, Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy' (2017) Vol 13 Life Sciences, Society and Policy 1 <https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1> accessed 8 February 2024.

traditional boundaries of the mind and yield information from the brain that enables to draw inferences about particular mental states of individuals and thus to some extent enable 'brain-reading'.[1540] Although the mind and mental states were insusceptible or irresistible to interference in the past, this seems no longer to be the case[1541] considering the progress in AI and neuroscience, in particular involving the AI disciplines ML (especially DL), CV as well as NLP and AC.

5.4.1 Legal problems: Type 1

Developments in AI raise legal problems regarding mental privacy, especially concerning the interpretation of neural activity patterns aiming to determine what an individual is thinking.[1542] These concerns partially overlap with the legal problems with respect to the processing of neurodata and mental data as discussed in Section 4.8.3. Brain-computer interfaces (BCIs) translate brain signals into computer commands and enable the communication between the human brain and devices.[1543] Such BCIs are often powered by ML and DL approaches.[1544] Measuring an individual's brain activity by means of electroencephalography (EEG) or functional magnetic resonance imaging (fMRI) in the form of BCI systems deploy ML and DL approaches and facilitate the drawing of inferences about particular mental properties, such as a person's emotions and memory.[1545]

Notably, the developments in neuro-AI may circumvent the cognitive process of filtering and selectively sharing information that humans typically perform to control the flow of information about them (e.g. thoughts and feelings). Thus, information that humans have considered and decided not to share may become available to entities[1546] anyway by interpreting neural activity and decoding it in order to determine those individual's thoughts, powered by ML and DL approaches as well as feature extraction techniques from the AI discipline CV[1547] that adaptively decode neurodata.[1548] Researchers have achieved to translate brain activity into text by means of ML and ANN approaches.[1549]

[1540] Sjors Ligthart, 'Freedom of thought in Europe: do advances in 'brain-reading' technology call for revision?' (2020) Vol 7 Iss 1 Journal of law and the biosciences 1, 2.
[1541] Thomas Douglas, Lisa Forsberg, 'Three Rationales for a Legal Right to Mental Integrity' in: Sjors Ligthart et al (eds) *Neurolaw Palgrave Studies in Law, Neuroscience, and Human Behavior* (Palgrave Macmillan 2021) 194.
[1542] Abel Wajnerman Paz, 'Is Mental Privacy a Component of Personal Identity?' (2021) Vol 15 Fronties in Human Neuroscience 2.
[1543] Hongchang Shan, 'Towards High Performance and Efficient Brain Computer Interface Character Speller: Convolutional Neural Network based Methods' Dissertation Universiteit Leiden 2020, 1.
[1544] Mamunir Rashid et al, 'The classification of EEG Signal Using Different Machine Learning Techniques for BCI Application' in J.-H. Kim et al (Eds) *Robot Intelligence Technology and Applications* (Springer 2018) 207-221.
[1545] Sjors Ligthart, 'Freedom of thought in Europe: do advances in 'brain-reading' technology call for revision?' (2020) Vol 7 Iss 1 Journal of law and the biosciences 1, 2.
[1546] Abel Wajnerman Paz, 'Is Mental Privacy a Component of Personal Identity?' (2021) Vol 15 Fronties in Human Neuroscience 2.
[1547] Mark Nixon, Alberto Aguado, *Feature Extraction & Image Processing for Computer Vision* (3rd edn Elsevier 2012).
[1548] Stephen Rainey et al, 'Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?' (2020) Journal of Law and the Biosciences 3 < https://academic.oup.com/jlb/advance-article/doi/10.1093/jlb/lsaa051/5864051?searchresult=1> accessed 8 February 2024.
[1549] Joseph G Makin, David A Moses, Edward F Chang, 'Machine translation of cortial activity to text with an encoder-decoder framework' (2020) Vol 23 Nature Neuroscience 575.

Developments in neurotechnology, powered by ML and DL approaches, have partially unlocked the human brain and made it readable under scientific lenses.[1550]

Whereas current applications of ML, DL and ANN in the context of neuroscience are being used in restricted scientific settings, such approaches will be used in a broader context in the future. It does not seem unlikely that the upcoming decades will see neurotechnology becoming pervasive and embedded in numerous aspects of human lives. Take, for example, a BCI system that records neural activity in the brain, and as the user thinks about moving an arm or a hand, the system decodes those intentions by means of ML and DL approaches. Whereas this system is initially intended to be used in a medical context, the provider of the system announced that it intends to discover new, non-medical applications allowing to control computers directly with the brain and make them available to the general population.[1551] In fact, there are already commercial brain-reading devices available to consumers,[1552] such as EEG sensor headsets for gaming, self-monitoring and entertainment.[1553] The right to privacy protects individuals from unwanted intrusions into their private lives, including intrusions into processes that occur solely inside one's brain, [1554] for instance thoughts that are not being communicated to others. These developments can violate mental privacy simply because they provide access to mental processes and states themselves as well as further information about mental states and information derived thereof.[1555] In addition to the infringement of mental privacy caused by the mere access to mental states and processes themselves (and information inferred thereof), the fact that individuals are unable to control access to mental processes and states violates mental privacy. Individuals are deprived of the opportunity to not share their feelings and thoughts or disclose them. Consequently, individuals are also unable to think or feel whatever they like.[1556]

Additionally, such approaches in AI may become increasingly effective in modulating the neural correlates of human psychology and behaviour.[1557] Neurotools such as BCIs allow interventions into

[1550] Marcello Ienca, Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy' (2017) Vol 13 Life Sciences, Society and Policy 5 <https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1> accessed 8 February 2024.
[1551] See the company's website <https://web.archive.org/web/20230331035227/https://neuralink.com/applications/> accessed 8 February 2024.
[1552] Sjors Ligthart, 'Freedom of thought in Europe: do advances in 'brain-reading' technology call for revision?' (2020) Vol 7 Iss 1 Journal of law and the biosciences 3.
[1553] Marcello Ienca, Pim Haselager, Ezekiel J Emanuel, 'Brain Leaks and Consumer Technology' (2018) Vol 36 Iss 9 Nature Biotechnology 805-815.
[1554] Jill Marshall, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff Publishers 2009) 3.
[1555] It might be argued that access to mental states and processes in fact refers to informational privacy as described in Section 5.2. However, I do see mental states and processes themselves as the source and thus object worthy of protection. Information about mental states such as concrete thoughts might then be protected under both mental and informational privacy.
[1556] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 19.
[1557] Marcello Ienca, Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy' (2017) Vol 13 Life Sciences, Society and Policy 5 <https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1> accessed 8 February 2024.

minds changing desires and beliefs without inflicting pain, harming bodily integrity or the need to indoctrinate persons over extended periods of time.[1558] Neuroenhancement, closed-loop brain interventions with on-chip ML[1559] and digital influences of the brain, such as nudging and other persuasive concepts, may allow interventions into minds and thus change desires and beliefs.[1560] Nudges are 'interventions that steer people in particular directions but that also allows them to go their own way'.[1561] Information about mental states and processes, including thoughts, provides powerful means to exhibit external influences, such as manipulation of individuals and their decision-making processes. As outlined in Section 4.3.3, manipulation perverts the way a person reaches decisions, forms preferences or adopts goals.[1562] It has been argued that case law does not provide hints as to whether mind-interventions such as manipulation of decision-making, fall within the ambit of mental integrity.[1563] In my view, manipulations violate what the ECtHR considers to constitute moral integrity.[1564] The latter covers non-invasion by outside influences.[1565] Therefore, I take the view that such manipulations may violate moral integrity which forms part of the broad concept of private life as elaborated by the ECtHR.

The AI discipline AC[1566] aims to detect emotional states and thus raises legal problems regarding mental privacy because it arguably renders emotional states and emotions machine-readable. AC violates mental privacy, simply because it detects and discloses emotions, moods and feelings of individuals.[1567] Systems that deploy AC and NLP approaches affecting mental privacy include automated border control systems aimed at detecting whether an individual lies, virtual assistants that detect the user's emotional state, video-based job assessments and wristbands that tell managers whether employees are unhappy.[1568] A notably EU funded automated border control system called

[1558] Jan Christoph Bublitz, Reinhard Merkel, 'Crimes against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination' (2014) Vol 8 Iss 1 Criminal Law and Philosophy 51, 61.
[1559] See Bingzhao Zhu, Uisub Shin, Masha Shoaran, 'Closed-Loop Neural Prostheses with On-Chip Intelligence: A Review and A Low-Latency Machine Learning Model for Brain State Detection' (2021) <https://www.epfl.ch/labs/inl/wp-content/uploads/2021/09/2109.058482.pdf> accessed 8 February 2024.
[1560] Sjors Ligthart, 'Freedom of thought in Europe: do advances in 'brain-reading' technology call for revision?' (2020) Vol 7 Iss 1 Journal of law and the biosciences 2.
[1561] Cass R Sunstein, 'The Ethics of Nudging' (2015) Vol 32 Yale Journal of Regulation 413, 417.
[1562] Joseph Raz, *The Morality of Freedom* (OUP 1986) 377; Cass R Sunstein, 'The Ethics of Nudging' (2015) Vol 32 Yale Journal of Regulation 413, 444.
[1563] Jan-Christoph Bublitz, 'The Nascent Right to Psychological Integrity and Mental Self-Determination' in Andreas van Arnauld, Kerstin von der Decken, Mart Susi (eds.), *The Cambridge Handbook of New Human Rights* (Cambridge University Press 2020) 397.
[1564] *Gladysheva v Russia* App no 7097/10 (ECtHR 6 December 2011) para 93, *Bensaid v United Kingdom* App no 44599/98 (ECtHR 6 February 2001) para 47.
[1565] Jill Marshall, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff Publishers 2009) 168, 184.
[1566] See the approaches in AC as discussed in Chapter 2.2.4.
[1567] It might be argued that access to emotions in fact refers to informational privacy as described in Section 5.2. However, given that emotions constitute srather sensitive information, I take the view that emotional states constitute a new object worthy of its own dedicated protection in the context of the right to privacy, namely under mental privacy.
[1568] For the latter, see Suzanne Bearne, 'A wristband that tells your boss if you are unhappy' *BBC* (London, 18 January 2021) <https://www-bbc-com.cdn.ampproject.org/c/s/www.bbc.com/news/amp/business-55637328> accessed 31 January 2021.

IBORDERCTRL 'analyses the micro-gestures of travellers to figure out if the interviewee is lying'.[1569] HireVue video interview software claims to be able to evaluate a candidate's employability, including personality traits, in under 30 minutes[1570] by means of on-demand video interviews where job candidates record responses to structured interview questions.[1571] The software detects and analyses the emotions a candidate portrays during the video assessment[1572] based on AC and AFA components. Amazon patented technology that enables its virtual assistant Alexa to recognise the users emotional state derived from the user's voice[1573] by combining AC and NLP approaches. Thus, systems that incorporate the discipline AC, sometimes[1574] combined with NLP, provide access to the emotional states and feelings of individuals.

The mere access to this sensitive information violates mental privacy. Furthermore, access to emotional states and feelings of individuals occurs beyond the control of the individuals concerned. AC deprives individuals of the opportunity not to share their feelings and emotional states because these disciplines may detect such information by non-invasive means anyway, such as by analysing facial expressions, gestures, physiological sensors and speech when combined with NLP. Individuals are also unable to feel whatever they like[1575] considering that their emotional states and feelings may be detected by non-invasive means and beyond their control. By means of revealing the emotional states of individuals, AC provides the necessary information needed to effectively manipulate decision-making of individuals, which arguably violates what the ECtHR considers to constitute moral integrity[1576] aiming to protect from undue external influences.[1577] Emotions play an important role in the elicitation of autonomous motivated behaviour.[1578] According to research in behavioural sciences, especially psychology, emotions constitute powerful, pervasive and predictable drivers of decision-making.[1579] Emotions can have significant effects on economic transactions and play a powerful role

[1569] European Commission, 'Smart lie-detection system to tighten EU's busy borders' (24 October 2018) < https://ec.europa.eu/research-and-innovation/en/projects/success-stories/all/smart-lie-detection-system-tighten-eus-busy-borders > accessed 8 February 2024.
[1570] 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.
[1571] See <https://www.hirevue.com/demo> accessed 8 February 2024.
[1572] 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.
[1573] Huafeng Jin, Shuo Wang 'Voice-Based Determination of Physical and Emotional Characteristics of Users' US Patent Number US 10096319 B1 (Assignee: Amayon Technologies, Inc.) October 2018 <https://patentimages.storage.googleapis.com/f6/a2/36/d99e36720ad953/US10096319.pdf> accessed 8 February 2024.
[1574] When emotional states are derived from speech.
[1575] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 19.
[1576] *Gladysheva v Russia* App no 7097/10 (ECtHR 6 December 2011) para 93, *Bensaid v United Kingdom* App no 44599/98 (ECtHR 6 February 2001) para 47.
[1577] Jill Marshall, *Personal Freedom through Human Rights Law? Autonomy, Identity and Integrity under the European Convention on Human Rights* (Martinus Nijhoff Publishers 2009) 168, 184.
[1578] 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.
[1579] Jennifer S Lerner et al, 'Emotion and Decision Making' (2015) Vol 66 Annual Review of Psychology 799, 802.

in everyday economic choices.[1580] The powerful insights that AC provides can be used to influence individuals, e.g. emotional states and feelings, which can violate mental privacy.

Although the mind and mental states were insusceptible or irresistible to interference, this seems no longer to be the case when considering the developments in AI, in particular BCI systems powered by ML, DL and CV,[1581] as well as approaches from the AI discipline AC (alone or combined with NLP).[1582] These AI disciplines may violate mental privacy in a yet unknown and unprecedented manner which constitutes a Type 1 legal problem simply because they enable mere access to mental states themselves as well as information that might be inferred or derived thereof. Furthermore, these disciplines violate mental privacy because individuals cannot control access to mental states and are deprived of the opportunity to not share such information. Consequently, individuals are also unable to think or feel whatever they like.[1583] Additionally, these developments in AI become increasingly relevant for the purpose of manipulating individuals, which arguably violates what, according to the ECtHR, constitutes moral integrity.[1584]

The mental information problem (Type 1)

Except for AR, all AI disciplines introduced in Chapter 2 facilitate access to mental states and information that might be inferred or derived thereof. Consequently, mental states and related information are no longer insusceptible or irresistible to interference. The AI disciplines ML, CV, NLP and AC are therefore prone to violate mental privacy.

5.4.2 Legal problems: Type 2

No specific Type 2 legal problems arise when the AI disciplines introduced in Chapter 2 are applied to mental privacy for the same reasons as outlined in Section 5.2.2. The fundamental right to privacy has been extensively enforced in the past ten years, [1585] and there are no indications that the enforcement of the fundamental right to privacy will decrease in the future due to AI.

[1580] Jennifer S Lerner, Deborah A Small, George Loewenstein, 'Heart Strings and Purse Strings' (2004) Vol 15 No 5 American Psychology Society 337-340.
[1581] Mark Nixon, Alberto Aguado, *Feature Extraction & Image Processing for Computer Vision* (3rd edn Elsevier 2012).
[1582] Thomas Douglas, Lisa Forsberg, 'Three Rationales for a Legal Right to Mental Integrity' in: Sjors Ligthart et al (eds) *Neurolaw Palgrave Studies in Law, Neuroscience, and Human Behavior* (Palgrave Macmillan 2021) 194.
[1583] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 19.
[1584] *Gladysheva v Russia* App no 7097/10 (ECtHR 6 December 2011) para 93, *Bensaid v United Kingdom* App no 44599/98 (ECtHR 6 February 2001) para 47.
[1585] See HUDOC database accessed 8 February 2024.

5.4.3 Legal problems: Type 3

If the broad interpretation of mental privacy[1586] in the context of AI does not hold true[1587] and the ECHR will not recognise mental privacy in such a broad way, it must be concluded that there is a Type 3 legal problem. In this case, the fundamental right to privacy, and particularly the broad concept of private life, is not fit for purpose to protect mental privacy. Nevertheless, and as outlined in Section 5.4, the broad scope of the fundamental right to privacy and the 'living instrument doctrine'[1588] are well equipped to ensure that the fundamental right to privacy keeps up with technological developments.[1589] I am therefore confident that the fundamental right to privacy will recognise and protect mental privacy considering the developments facilitated by AI that enable access to mental information.

Moreover, some interferences with mental privacy caused by AI may simultaneously also infringe bodily privacy (see Section 5.3.1). This might be the case with AC that detects emotions based on physiological signals or ML and DL approaches that use neuro implants to record neural activity and decode the intentions and thoughts of the individual concerned.

5.5 Communicational privacy

The right to communicational privacy as part of the fundamental right to privacy aims to avoid unsolicited interception of communication. Typical violations include eavesdropping or intercepting communication,[1590] including mere access to stored communication.[1591] Communication is to be understood broadly and includes telephone and wireless communication, as well as mail and email and, in line with the living instrument doctrine, future means of communication. Possible infringements also entail the interception of communication by means of bugs, microphones or other sensors.[1592] Communicational privacy is typified by an individual's interest in restricting access to communications or controlling the use of information communicated to third parties.[1593] According to ECtHR case law,

[1586] Sjors Ligthart et al, 'Forensic Brain-Reading and Mental Privacy in European Human Rights Law: Foundations and Challenges' (2021) Vol 14 Neuroethics 191, 200 <https://link.springer.com/content/pdf/10.1007/s12152-020-09438-4.pdf> accessed 8 February 2024; Abel Wajnerman Paz, 'Is Your Neural Data Part of Your Mind? Exploring the Conceptual Basis of Mental Privacy' (2022) Vol 32 Minds and Machines 395, 399.
[1587] For instance, Ienca and Andorno, which argue that the right to privacy is insufficient to protect mental privacy. See Marcello Ienca, Roberto Andorno, 'Towards new human rights in the age of neuroscience and neurotechnology. Life Sciences, Society and Policy' (2017) Vol 13 Life Sciences, Society and Policy 15 <https://lsspjournal.biomedcentral.com/articles/10.1186/s40504-017-0050-1> accessed 8 February 2024.
[1588] Alastair Mowbray, 'The Creativity of the European Court of Human Rights' (2005) Vol 5 Iss 1 Human Rights Law Review 57-59.
[1589] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 509.
[1590] Roger Clarke, 'What's Privacy?' (2006) <http://www.rogerclarke.com/DV/Intro.html > accessed 8 February 2024.
[1591] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 8.
[1592] Rachel L. Finn, David Wright, Michael Firedewald, 'Seven Types of Privacy' in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Springer 2013) 8.
[1593] Bert-Jaap Koops et al 'A Typology of Privacy' (2017) Vol. 38 Iss. 2 University of Pennsylvania Journal of International Law 438, 567.

the form and content of the communication are irrelevant to the question of interference.[1594] Moreover, the right to privacy aims to protect the confidentiality of communication in a wide range of situations and technologies. The living instrument doctrine explained in Section 3.1.2 enables the fundamental right to privacy to keep up with technological developments. This doctrine is also helpful for new methods of communication,[1595] arguably including methods involving AI. For example, I take the view that human-machine communication occurring in the context of virtual assistants and similar services as discussed in Section 4.9.3 is protected by the right to communicational privacy. The ECtHR anticipated new technological developments and emphasised that it will consider the extent to which 'intrusions into private life are made possible by new, more and more sophisticated technologies'[1596] (see also Section 5.5.3).

5.5.1 Legal problems: Type 1

Three AI disciplines are particularly relevant regarding communicational privacy. Speech-based emotion recognition systems that combine approaches from the AI disciplines ML and AC rely on the processing of personal communication, speech signals in particular. NLP requires the analysis of communication because it concerns the understanding and generation of natural language.

Approaches that implement AC and ML measure and quantify the emotions of individuals by observing the speech signals of these individuals. Supervised ML algorithms are at the heart of many emotion recognition efforts[1597] and methods applied to emotion recognition from speech also involve DL approaches.[1598] As explained in Section 2.2.4.2, effects of emotion tend to be present in acoustic signal features such as average pitch, pitch range and pitch changes, speech rate and articulation.[1599] ML maps the input, namely, the automatically derived acoustic features, to emotion labels that represent the characteristics for a given emotion category.[1600] For example, the detected acoustic feature of a high speech rate is typically associated with the emotional state of anger or fear.[1601] Virtual assistants as introduced in Section 4.9.1 deploy AC approaches to detect a user's emotional state, which allows them to modify their behaviour accordingly.[1602]

[1594] *A. v France* App no 14838/89 (ECtHR 23 November 1993) paras 35-37; *Frérot v France* App no 70204/01 (ECtHR 12 June 2007) para 54.
[1595] David Harris et al, *Law of the European Convention on Human Rights* (4th edn OUP 2018) 509.
[1596] *Köpke v Germany*, App No 420/07 (ECtHR 05 October 2010) emphasis added.
[1597] Chi-Chun Lee et al, 'Speech in Affective Computing' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 177.
[1598] Haytham M Fayek, Margaret Lech, Lawrence Cavedon, 'Evaluating deep learning architectures for Speech Emotion Recognition' (2017) Vol 92 Neural Networks 60.
[1599] Rosalind W Picard, *Affective Computing* (MIT Press 1997) 179, 180.
[1600] Chi-Chun Lee et al, 'Speech in Affective Computing' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 173, 177.
[1601] Rosalind W Picard, *Affective Computing* (MIT Press 1997) 179.
[1602] Giorgo Manfredi, Claudio Gribaudo, Virtual Assistant with real-time emotions, WIPO Patent WO 2008/049834 A2, Laurence Goasduff 'Emotion AI Will Personalize Interactions' (Gartner, 22 January 2018) <https://www.gartner.com/smarterwithgartner/emotion-ai-will-personalize-interactions/> accessed 8 February 2024.

For example, Amazon has been granted a patent for 'Voice-based determination of physical and emotional characteristics of users'. According to this patent, the system may detect emotions such as happiness, joy, anger, sorrow, sadness, fear, disgust, boredom and other emotional states based on analysis of acoustic features such as pitch or speech rate, as determined from the processing of the voice data. The patent specifically refers to the AI disciplines NLP and ML, including ANN approaches.[1603] Following the claims of this patent, virtual assistant Alexa is able to detect a user's emotional or physical state. This enables Alexa to intuitively suggest specific products based on the user's current emotional state or offer medicine if it detects a cough when a user makes a request.[1604] Spotify patented a virtual assistant that improves the way a machine processes and generates a response to a human's emotion based on an utterance (human vocalisation) from a user containing both a command and an emotion.[1605] The virtual assistant is designed for a 'media playback device' and can recognise when a user sounds sad and is able to offer encouragement by 'cheering' the user up.[1606] Apart from sadness, other detectable emotions enlisted in the patent are surprise, anger, fear, anxiety, disgust and joy.[1607] As mentioned in Section 2.2.4.1, these six 'basic emotions'[1608] are the most common ones used in emotion research.[1609] According to the patent, emotions are derived from a variety of cues associated with user's utterance. In the case of a command, such cues may be the tone, cadence, volume, pitch and pace of the user's speech.[1610] These cues resemble the acoustic signal features typically used in speech-based emotion recognition systems as outlined in Section 2.2.4.2. They are often related to prosody which considers the intonational and rhythmic aspects of language.[1611] Typical examples are pitch and energy of speech,[1612] including voice level and speech rate.[1613] Where the user's utterance

[1603] Huafeng Jin, Shuo Wang, 'Voice-based Determination of Physical and Emotional Characteristics of Users' US Patent Number US 10096319B1 (Assignee: Amazon Technologies, Inc.) October 2018 <https://patentimages.storage.googleapis.com/f6/a2/36/d99e36720ad953/US10096319.pdf>, accessed 8 February 2024.
[1604] James Cook, 'Amazon patents new Alexa feature that knows when you're ill and offers you medicine' *The Telegraph* (London 9 October 2018) < https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/> accessed 8 February 2024.
[1605] 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.
[1606] 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.
[1607] 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 12 < https://patentimages.storage.googleapis.com/2a/9d/2d/926b58a2bd956f/US10566010.pdf >, accessed 8 February 2024.
[1608] These six emotions refer to research conducted by psychologists in the early seventies that developed the methodology of 'basic emotions'; see Paul Ekman, Wallace v Friesen, 'Constants across cultures in the face and emotion' (1971) Vol 17 (2) Journal of Personality and Social Psychology 124.
[1609] Lisa Feldman Barrett et al. 'Emotional Expressions Reconsidered' (2019) Vol 20 (1) Psychological Science in the Public Interest 1, 4.
[1610] 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 12 < https://patentimages.storage.googleapis.com/2a/9d/2d/926b58a2bd956f/US10566010.pdf >, accessed 8 February 2024.
[1611] Daniel Jurafsky, James H Martin, *Speech and Language Processing* (2 edn, Pearson Education Limited 2014) 238.
[1612] Ricardo A. Calix, Leili Javadpour, Gerald M. Knapp, 'Detection of Affective States From Text and Speech For Real-Time Human-Computer Interaction' (2012) Vol 54 No 4 Human Factors and Ergonomics Society 530, 531.
[1613] 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.

contains no words from which a command can be extracted, (e.g. 'Ugh'), emotions are derived from the tone of this utterance.[1614]

Virtual assistants are not the only domain in which speech emotion recognition systems could be implemented. Speech emotion recognition may be used in various areas, such as call centres, smart devices or cars.[1615] In fact, they are already used in practice. A real-world application of AC aiming to derive emotional states from speech is Amazon's wearable 'Halo' that analyses voice tones to detect user emotions.[1616] A Hungarian bank used an AI system with the aim to detect and measure emotions of customers that called the bank's customer service.[1617] In order to identify customer dissatisfaction, the AI system deployed by the bank relied on acoustic signal features introduced in Section 2.2.4.2, namely, speed, volume and pitch of speech.[1618]

Speech-based emotion recognition systems combine approaches from the AI disciplines ML, AC and NLP. Because such systems are highly dependent on speech analysis, they violate communicational privacy. Speech falls under the term 'communication' according to the right to communicational privacy: the form and content of the communication is irrelevant to the question of interference.[1619] Individuals concerned cannot control the further use of such communication and might not even be aware of the fact that communication is analysed to detect their emotional state, let alone be aware of what information can be derived from analysing speech. Speech-based emotion recognition systems therefore violate communicational privacy, which leads to a Type 1 legal problem.

The speech analysis problem (Type 1)

By combining approaches from ML, AC and NLP, speech-based emotion recognition systems are highly dependent on the processing of communication (speech) to detect the emotional states of the individual concerned. These systems intercept, analyse and otherwise process communications in various contexts, including virtual assistants, call centres and cars. Individuals cannot control the further use of such communication. This violates communicational privacy.

[1614] 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 13 < https://patentimages.storage.googleapis.com/2a/9d/2d/926b58a2bd956f/US10566010.pdf >, accessed 8 February 2024.
[1615] See services of the company audeering: https://www.audeering.com/.
[1616] Alex Hern, 'Amazon's Halo wristband: the fitness tracker that listens to your mood' *The Guardian* (London, 28 August 2020) < https://www.theguardian.com/technology/2020/aug/28/amazons-halo-wristband-the-fitness-tracker-that-listens-to-your-mood > accessed 8 February 2024; Austin Carr, 'Amazon's New Wearable Will Know If I'm Angry. Is That Weird?' *Bloomberg* (New York, 31 August 2020) < https://www.bloomberg.com/news/newsletters/2020-08-31/amazon-s-halo-wearable-can-read-emotions-is-that-too-weird > accessed 8 February 2024.
[1617] 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.
[1618] Cesar Manso-Sayao, Summary of Hungarian SA Decision NAIH-85-3/2022 < https://gdprhub.eu/NAIH_(Hungary)_-_NAIH-85-3/2022 > accessed 8 February 2024.
[1619] *A. v France* App no 14838/89 (ECtHR 23 November 1993) paras 35-37; *Frérot v France* App no 70204/01 (ECtHR 12 June 2007) para 54.

NLP develops novel practical applications to facilitate the interactions between computers and humans,[1620] including the generation and understanding of natural language.[1621] Developments in the discipline NLP have led to the integration of AI technologies in daily life. Nowadays, individuals routinely communicate with virtual assistants[1622] such as Alexa, Siri or Google Assistant. Such interactions are expected to increase even more in the future.[1623] For example, car manufacturers already offer in-vehicle virtual assistants.[1624] A study concerning Amazon Alexa's ecosystem revealed that a user's activities can be reconstructed due to the large amount of data with timestamps.[1625]

Most of the virtual assistant's processing occurs on a remote server and every transaction and recording is kept by the company which provides the service.[1626] Contrary to what was claimed in the terms, a study revealed that Amazon Alexa records speech even if the wake word is not spoken: 91% of the study participants had instances of unintended voice recordings, i.e. recordings occurring without mentioning the wake word. Study participants reported that such unintended recordings contained sensitive conversations.[1627] This means that users do not have complete control over what is recorded, transmitted and stored in the cloud environment of the virtual assistant's provider.[1628] Unintended recordings may contain sensitive recordings of speech[1629] given the broad range of applications of virtual assistants, which are used at home, in cars and at any given location in case the virtual assistant service is used on a mobile phone. A whistle-blower who used to work for Apple revealed that he had listened to hundreds of recordings every day, often including unintentional recordings, for quality control purposes ('grading of Apple's virtual assistant'). According to the whistle-blower, these recordings concerned sensitive communications such as discussions between doctors and patients, business deals, seemingly criminal acts and sexual encounters.[1630] Such recordings are also interesting for law enforcement agencies.[1631]

[1620] Deng Li and Liu Yang, 'A Joint Introduction to Natural Language Processing and Deep Learning' in Deng Li and Liu Yang (eds) *Deep learning in natural language processing* (Springer 2018) 1.
[1621] Stan Franklin, 'History, motivations, and core themes' in Frankish Keith and Ramsey William M. (eds) *The Cambridge Handbook of Artificial Intelligence* (2014) 26.
[1622] Refer to Section 4.9.3 to learn more how virtual assistants work.
[1623] Andrea L Guzman, Seth C Lewis, 'Artificial intelligence and communication: A Human-Machine Communication agenda' (2020) Vol 22 Iss 1 New Media & Society 70, 71.
[1624] For instance, 'Hey Mercedes', which is able to understand different accents and will adjust to the driver over time; see <https://www.mercedes-benz.co.uk/passengercars/mercedes-benz-cars/models/eqc/comfort.pi.html/mercedes-benz-cars/models/eqc/comfort/standard-equipment/mbux> accessed 8 February 2024.
[1625] Hyunji Chung, Jungheum Park, Sangjin Lee, 'Digital forensic approaches for Amazon Alexa ecosystem' (2017) Vol 22 Digital Investigation 15, 18.
[1626] Tom Bolton et al, 'On the Security and Privacy Challenges of Virtual Assistants' (2021) Vol 21 Iss 7 Sensors 1-2.
[1627] Yousra Javed, Shashank Sethi, Akshay Jadoun, 'Alexa's Voice Recording Behavior: A Survey of User Understanding and Awareness' (ARES '19, Canterbury 26-29 August 2019) 7 <https://dl.acm.org/doi/10.1145/3339252.3340330> accessed 8 February 2024.
[1628] Hyunji Chung et al, 'Alexa, Can I Trust You?' (2017) Vol 50 Iss 9 Computer 100, 103.
[1629] Yousra Javed, Shashank Sethi, Akshay Jadoun, 'Alexa's Voice Recording Behavior: A Survey of User Understanding and Awareness' (ARES '19, Canterbury 26-29 August 2019) 2 <https://dl.acm.org/doi/10.1145/3339252.3340330> accessed 8 February 2024.
[1630] 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.
[1631] Hyunji Chung, Jungheum Park, Sangjin Lee, 'Digital forensic approaches for Amazon Alexa ecosystem' (2017) Vol 22 Digital Investigation 2.

Generating and understanding natural language in NLP requires analysis of personal communication. Virtual assistants such as Siri or Alexa unintentionally intercept and record personal communication from their users and other people such as relatives, children and friends. Developments in NLP provide means to listen to private communications and also facilitate the identification of the individual who is speaking. For example, Microsoft's Speaker Recognition Application Programming Interface (SAPI)[1632] allows one to identify individual speakers within a group and can be easily deployed.[1633] Because they are highly dependent on the processing of communication, these NLP empowered systems violate communicational privacy. This affects the confidentiality of communication in a wide range of situations and technologies regardless of the form and content of the communication.[1634] This constitutes a Type 1 legal problem.

The interception and identification problem (Type 1)

Generating and understanding natural language in NLP requires the processing of communication. Virtual assistants unintendedly intercept and record personal communication of their users and other individuals such as relatives, children, and friends. Developments in NLP such as Speaker Recognition APIs facilitate the identification of individual speakers within a group. This violates communicational privacy.

Keyword determination systems are based on the AI discipline NLP. They are highly problematic in the context of communication privacy. Such systems aim to detect keywords from recorded speech and use them for targeted advertising. Users suspected their smartphones to be secretly eavesdropping on them, and many reports[1635] have claimed that private conversations occurring in the presence of smartphones consequently resulted in targeted online advertisements. Advertisements referred to in these reports relate to a broad range of product categories matching either an overall discussion topic or a specific brand or product mentioned in a preceding face-to-face conversation.[1636] For example, 20 employees of the research and advisory firm Forrester reported that some of their 'real-life' conversations seemingly resulted in ads and sponsored posts on Facebook without having searched for the item advertised after the conversations took place.[1637]

[1632] A set of functions and procedures allowing the creation of applications that access features or data of an operating system, application or other service; see <https://www.dictionary.com/browse/api> accessed 8 February 2024.
[1633] <https://azure.microsoft.com/en-us/services/cognitive-services/speaker-recognition/> accessed 8 February 2024.
[1634] *A. v France* App no 14838/89 (ECtHR 23 November 1993) paras 35-37; *Frérot v France* App no 70204/01 (ECtHR 12 June 2007) para 54.
[1635] Jacob Leon Kröger, Philip Raschke, Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping' in: Simon N Foley (eds) *Data and Applications security and Privacy XXXIII* (Springer 2019) 102, 103.
[1636] Ibid.
[1637] Fatemeh Khatibloo, 'Is Facebook Listening (And So What If They Are)?' *Forbes* (New York, 17 March 2017) <https://www.forbes.com/sites/forrester/2017/03/17/is-facebook-listening-and-so-what-if-they-are/> accessed 8 February 2024.

Some consider the fear that private companies could target their ads based on eavesdropped conversation as baseless and paranoid.[1638] For example, a former product manager of Facebook stated that alleged eavesdropping would be economically and technically unfeasible, referring to CPU,[1639] battery and data storage limitations.[1640] The technological and economic feasibility argument has been rebutted in research, however.[1641] Smartphone-based eavesdropping can be deployed efficiently and scalable by means of keyword detection instead of full speech recognition. Keyword detection only recognises a predefined vocabulary of spoken words and runs on devices with much lower computational power than smartphones. It allows one to search for trigger words indicating a person's interest, such as 'love' or 'enjoy', to identify relevant sections of a private conversation instead of searching for millions or perhaps billions of targetable keywords.[1642]

Amazon's US patent 'Keyword Determinations from Voice Data'[1643] indicates that the technology for such advertisements is already available. The patent, which relies on NLP, describes a system that captures voice content when a user speaks into or near the device (e.g., Alexa), notably without activating the virtual assistant by mentioning the 'wake word' (e.g., 'hey Alexa'). Sniffer algorithms identify trigger words that indicate statements of preference (such as 'like' or 'love') and translate them into keywords. The identified keywords are subsequently transmitted to a location accessible to advertisers, who then use the keywords to select content that is likely relevant to the user.[1644] Amazon has denied that it uses voice recordings for advertising at the moment and claimed that the patent might never actually come to the market.[1645] This statement seems to be contradictory to a journalist's report that suspects Amazon to have listened to a private conversation between herself and her husband. The conversation involved a very specific kitchen gadget. She suspects that Alexa snooped into the conversation, as she has subsequently received an ad for that kitchen gadget on Amazon.[1646] When considering the capabilities of Amazon's keyword determination system, this does not seem to be an unrealistic or far-fetched claim. The Amazon patent clearly shows that the technical

[1638] Jacob Leon Kröger, Philip Raschke, Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping' in: Simon N Foley (eds) *Data and Applications security and Privacy XXXIII* (Springer 2019) 103.
[1639] Central Processing Unit (CPU), sometimes also called main processor, constitutes the physical heart of the entire computer system and is generally composed of the main memory, control unit, and arithmetic-logic unit; see <https://www.britannica.com/technology/central-processing-unit> accessed 8 February 2024.
[1640] Antonio García Martínez, 'Facebook's Not Listening Through Your Phone. It Doesn't Have To' *Wire* (New York, 18 November 2017) <https://www.wired.com/story/facebooks-listening-smartphone-microphone/> accessed 8 February 2024.
[1641] Jacob Leon Kröger, Philip Raschke, Is My Phone Listening in? On the Feasibility and Detectability of Mobile Eavesdropping' in: Simon N Foley (eds) *Data and Applications security and Privacy XXXIII* (Springer 2019) 112.
[1642] Ibid.
[1643] 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.
[1644] Ibid.
[1645] Griffin Andrew, 'Amazon files for Alexa patent to let it listen to people all the time and work out what they want' *The Independent* (London, 11 April 2018) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-alexa-patent-listening-to-me-facebook-phone-talking-ads-a8300246.html> accessed 8 February 2024.
[1646] Morgan Blake, 'Are Digital Assistants Always Listening?' *Forbes* (New York, 5 February 2018) <https://www.forbes.com/sites/blakemorgan/2018/02/05/are-digital-assistants-always-listening/#2f000e1a4eeb> accessed 8 February 2024.

means for such eavesdropping are available and could be used for targeted advertisement. A marketing team within media giant Cox Media Group claims it can listen to ambient conversations of consumers through embedded microphones in smartphones, smart TVs, and other devices to gather data and use it to serve targeted ads.[1647] Hence, advances in NLP such as keyword determination systems for targeted advertising may violate communicational privacy because they are designed to intercept and analyse communication with the aim of subsequently using the information for targeted advertising. This violates communicational privacy and constitutes a Type 1 legal problem.

The keyword problem (Type 1)

Keyword determination systems powered by approaches in NLP identify trigger words that indicate statements of preference (such as 'like' or 'love') from recorded speech and translate these into keywords. These keywords are then used by advertisers to select content that is likely relevant to the user. Such systems intercept and analyse communications, which violates the right to communicational privacy.

5.5.2 Legal problems: Type 2

No specific Type 2 legal problems arise when the AI disciplines introduced in Chapter 2 are applied to communicational privacy for the same reasons as outlined in Section 5.2.2. The fundamental right to privacy has been extensively enforced in the past ten years,[1648] and there are no indications that the enforcement of the fundamental right to privacy will decrease in the future due to AI.

5.5.3 Legal problems: Type 3

As already discussed in Sections 5.5 and 4.9.3, the developments in AI require protection of human-machine communication under the remit of communicational privacy. Historically, communication has been conceptualised as a human process potentially mediated by technology.[1649] Case law of the ECtHR refers to the historic conception of communication, i.e. communication between humans. Therefore, it might be argued that human-machine communications, such as between the user and its virtual assistant, do not neatly fall within the scope of communicational privacy. However, I do not think such an argument is valid. First, the ECtHR stressed that it will consider the extent to which 'intrusions into private life are made possible by new, more and more sophisticated technologies'.[1650] Second, the living instrument doctrine as described in Section 3.1.2 proved to be very effective to address issues at the forefront of technology. Third, the ECtHR interprets the confidentiality of

[1647] 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.
[1648] See HUDOC database accessed 8 February 2024.
[1649] Andrea L Guzman, Seth C Lewis, 'Artificial intelligence and communication: A Human-Machine Communication agenda' (2020) Vol 22 Iss 1 New Media & Society 70 -68.
[1650] *Köpke v Germany*, App No 420/07 (ECtHR 05 October 2010) emphasis added.

communication broadly, regardless of the *form* and *content* of the communication.[1651] Therefore, I take the view that communicational privacy as enshrined in the fundamental right to privacy not only covers communication between individuals, but also communication between humans and machines. Therefore, no Type 3 legal problems arise. However, if my broad interpretation of communicational privacy does not hold and the ECtHR will refrain from considering human to machine communications to fall under communicational privacy, it must be concluded that there is a Type 3 legal problem.

5.6 Access

In many cases, the right of access is the point of departure for the data subject in exercising control over his or her personal data. The right of access allows the data subject to verify the lawfulness[1652] of processing and enables the data subject to obtain, depending on the circumstances, the rectification, erasure or blocking of personal data by the controller.[1653] The right of access must be considered a conditio sine qua non for exercising other data subject rights and restrictions on or around this right cause a knock-on effect on the entire data protection law regime.[1654] The CJEU repeatedly stressed the importance of the right of access as a prerequisite to other data protection rights.[1655] Given the important role of the right of access, the analysis in this section will be more extensive than for other data subject rights.

The right of access is not an absolute right, which means that this right may be restricted. Indeed, the right of access may be restricted in to ways, namely, in line with the provisions contained in Article 23 GDPR and in accordance with Article 15 (4) GDPR. Both provisions refer to the rights and freedoms of others, which particularly encompasses *trade secrets* or IP rights, including copyrights protecting the software.[1656] Restrictions under Article 15 (4) GDPR differ from restrictions possible under Article 23 GDPR. Article 15 (4) *exclusively* applies to the right to obtain a copy of the personal data undergoing processing and allows restrictions on a *case-by-case* basis, whereas restrictions according to Article 23 GDPR need to be laid down in Member State or Union law. According to Custers and Hijne, both the tools used for data analysis (AI systems) and the resulting knowledge (output of the AI system) fall within the scope of IP, trade secrets or other rights of the controller deserving protection.[1657] This is particularly relevant when analysing the right of access in the light of AI. In Sections

[1651] *A. v France* App no 14838/89 (ECtHR 23 November 1993) paras 35-37; *Frérot v France* App no 70204/01 (ECtHR 12 June 2007) para 54.
[1652] Recital 63 GDPR.
[1653] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44.
[1654] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 285.
[1655] 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.
[1656] Recital 63 GDPR.
[1657] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 10

5.6.1 – 5.6.3, I outline that the relationship between the trade secrets directive ('TSD')[1658] and the GDPR is particularly problematic.[1659]

The scope of protection of the TSD covers AI itself, including the technical method used to process and obtain information. This protection applies to all AI disciplines,, as introduced in Chapter 2. Trade secrets are broadly defined in the TSD. To qualify as a trade secret according to Article 2 TSD, the information must (i) be secret, (ii) have commercial value due to its secrecy and (iii) be subject to reasonable steps to keep it secret.

Requirement (i), i.e. secrecy, is already met when the information is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question.[1660] Protection offered by the TSD might be sought for AI technology including the technical methods used to obtain and process information and thus algorithms, training data (created or selected) and methods to create and select training data and output data (for example, the detected emotional state of an individual).[1661] The TSD lists a diverse range of information that is protectable.[1662] According to Recital 2 TSD, trade secrets protect a wide range of know-how and business information. It comprises information such as business practices, information on or knowledge about customers, personal data inferred or predicted by controllers and personal data analytics itself.[1663] Recital 14 TSD specifically includes 'technological information' in the definition of trade secrets. Arguably, the definition of a trade secret is so broad to include nearly any data handled by a commercial entity, such as shopping habits and history of customers,[1664] information about a customer's behaviour (creditworthiness, lifestyle, reliability, etc.),[1665] customer lists and profiles,[1666] algorithms,[1667] personalised marketing plans (e.g. pricing) or forecasts about customer's future life based on probabilistic studies

[1658] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1 (TSD).
[1659] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 312.
[1660] Recital 14 Trade Secrets Directive; Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 307; Thomas Hoeren, 'The EU Directive on the Protection of Trade Secrets and its Relation to Current Provisions in Germany' (2018) Vol 9 Iss 2 JIPITEC 140 <https://www.jipitec.eu/issues/jipitec-9-2-2018/4725> accessed 8 February 2024.
[1661] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 197, 201.
[1662] Rochelle Cooper Dreyfusss, Mireille van Eechoud 'Choice of law in EU trade secrecy cases' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 177.
[1663] Claudio Malgieri, Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) Vol 7 No 4 International Data Privacy Law 243, 262.
[1664] Inge Graef, Martin Husovec, Nadezhda Purtova 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) Vol 19 Iss 6 German Law Journal 1359, 1381.
[1665] 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.
[1666] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 312; Nadezhda Prtova, 'Do property rights in personal data make ense after the Big Data turn?' (2017) Vol 10 No 2 Journal of Law & Economic Regulation 64, 71.
[1667] Guido Noto La Diega, 'Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information' (2018) Iss 1 Vol 9 JIPITEC 3, 4, 26, 28.

(life expectancy, estimated advancements in career, etc.).[1668] In addition, information or knowledge does not necessarily need to be correct or complete in order to enjoy protection under the TSD.[1669]

Protected information or knowledge has commercial value according to requirement (ii), if its unlawful acquisition, use or disclosure is likely to harm the interests of the person lawfully controlling it, in the sense that it undermines that person's business or financial interests, strategic position or ability to compete.[1670] Under the TSD, commercial value includes both *potential* or *actual* value. The latter seems to indicate that individual data may also be eligible for protection and, therefore, the notion of commercial value should be interpreted broadly. It refers to any harm to the scientific and technical capacity as well as the economic interests of the trade secret holder resulting from the disclosure of (secret) information, including the ability to compete in a broad sense.[1671]

Criterion (iii), i.e. the trade secret holder taking 'reasonable steps' to keep the protected information secret, is arguably the most tangible for businesses to demonstrate. To satisfy this requirement, companies may adopt non-disclosure agreements, include clauses banning reverse engineering into their licencing agreements or limit the number of possible licences altogether to not undermine secrecy.[1672] The threshold for this requirement seems to be rather low. It does not require trade secret holders to conclude individual confidentiality agreements with each third party to whom the trade secret is conveyed. In the absence of explicit non-disclosure agreements, even an implied duty of confidence might be sufficient to meet criterion (iii), for example, between the employer and employee.[1673]

AI is particularly valuable for companies because it may be used to derive or infer data, such as statistical inferences about a multitude of subjects, a given arrangement of a list of information and technical information related to a product or process.[1674] Trade secrets are extensively used by most types of companies. A study conducted by the EU Intellectual Property Office (EUIPO) in 2017[1675] demonstrated that the use of trade secrets is higher than the use of patents by most types of company,

[1668] 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.
[1669] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 200.
[1670] Recital 14 TSD; 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.
[1671] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 311, 411.
[1672] Nazrin Huseinzade, 'Algorithm Transparency: How to Eat the Cake and Have it Too' *European Law Blog* (27 January 2021) <https://europeanlawblog.eu/2021/01/27/algorithm-transparency-how-to-eat-the-cake-and-have-it-too/> accessed 8 February 2024.
[1673] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 315, 412.
[1674] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 197
[1675] EUIPO 'Protecting Innovation Through Trade Secrets and Patents: Determinants for European Union Firms' (2017) <https://euipo.europa.eu/ohimportal/en/web/observatory/news/-/action/view/3704420> accessed 8 February 2024.

in most economic sectors and in all Member States.[1676] A very high prevalence of trade secrets has been observed in the sectors of computer programming, consultancy and related services.[1677] AI systems and their underlying algorithms[1678] may undoubtedly[1679] fall under the broad term of trade secrets and are likely to be treated as such. As a result, these algorithms will rarely be disclosed to the public or individuals affected by it.[1680] In fact, most of the complex algorithms including the algorithms of Google or Facebook are proprietary and shielded as trade secrets while only a negligible minority of algorithms are open source.[1681] Amazon's recommendation system, the Instagram algorithm for publication diffusion and Google's search engine are among the most well-known examples of trade secrets.[1682]

The scope of protection of the TSD is broad and protects not only AI and its underlying algorithms, but also input data (including training data) and selection methods, as well as output data, which constitute personal data. This applies to *all* AI disciplines as introduced in Chapter 2 and thus allows restrictions of all data subject rights and principles introduced in Sections 3.3.4 and 3.3.3 provided that such restrictions comply with Article 23 GDPR. The wording contained in Article 23 GDPR concerns the ability of Member States to impose restrictions on data subject rights and principles by means of legislative measures and expressly refers to Union law. Thus, EU legislation may adopt, by legislative measures, any restriction on the rights and principles contained in the GDPR.[1683] In fact, the TSD constitutes such Union law and provides controllers with the possibility to restrict data subject rights, for example, the right of access, to protect their trade secrets. Such restrictions must respect both the fundamental right to data protection and trade secrets simultaneously.[1684] In addition, trade secrets may be protected by the right to property according to Article 17 EUCFR.[1685] AI may also be

[1676] This seems logical since the protected information under trade secrets is much broader than compared to patents where the patentability thresholds need to be met. Furthermore, there are no formal registration requirements as it is the case with IP laws.
[1677] EUIPO 'Protecting Innovation Through Trade Secrets and Patents: Determinants for European Union Firms' (2017) 8-9 37 <https://euipo.europa.eu/ohimportal/en/web/observatory/news/-/action/view/3704420> accessed 8 February 2024
[1678] Which arguably constitutes 'technological information' according to Recital 14 TSD.
[1679] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 409; Maja Brkan, Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas (2020) Vol 11 Iss 1 European Journal of Risk Regulation 18, 39.
[1680] Gintarė Surblytė-Namavičienė, *Competition and Regulation in the Data Economy* (Edward Elgar Publishing 2020) 243.
[1681] Nazrin Huseinzade, 'Algorithm Transparency: How to Eat the Cake and Have it Too' *European Law Blog* (27 January 2021) < https://europeanlawblog.eu/2021/01/27/algorithm-transparency-how-to-eat-the-cake-and-have-it-too/> accessed 8 February 2024.
[1682] Maja Brkan, Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas (2020) Vol 11 Iss 1 European Journal of Risk Regulation 18, 39.
[1683] Dominique Moore, Commentary of Article 23 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 552.
[1684] Recital 34 TSD states that the TSD 'respects the fundamental rights….[ ]…notably the right to protection of personal data.... [ ]…while respecting business secrecy'.
[1685] Case C-1/11 *Interseroh Scrap* [2012] ECR I-194 para 43; Case T-189/14 *Deza* [2017] para 163.

protected by intellectual property rights[1686] such as patents or copyrights[1687] - alone or in combination with trade secrets.[1688] Because trade secrets are more widely used than IP rights[1689] and easier for companies to rely on,[1690] I focus on trade secrets.

5.6.1 Legal problems: Type 1

Article 15 (1) lit h GDPR grants the right to data subjects to receive 'meaningful information about the logic involved' in automated decision-making (ADM). It is not yet clear what 'meaningful information' and the 'logic involved' mean when put into practice. In the view of AG Pikamäe, information about the 'logic involved' particularly includes the factors taken into account in the decision-making process and their weighting at an aggregate level.[1691] As indicated in Section 4.4.1, I interpret meaningful information according to Article 15 (1) lit h GDPR as information that is useful and/or has practical value for data subjects to (i) become aware of processing relating to ADM, (ii) enforce their data subject rights and (iii) exercise control over the processing of their personal data. AG Pikamäe stresses that such information must be useful for data subjects, so they can challenge 'decisions' within the meaning of Article 22 (1) of the GDPR.[1692] This is also in line with the CJEU's focus on intelligibility regarding Article 12 (1) GDPR, which ensures that the data subject fully understands the information provided to it.[1693] According to AG Pitruzella, Article 12 (1) GDPR aims to allow the data subject to effectively exercise the right of access and other data subject rights.[1694] In view of the AG, information should be provided in a manner that enables the data subject to familiarise itself with it fully, easily and without difficulty. Controllers do not comply with Articles 12 (1) and 15 GDPR if they provide information in a way that makes it 'extremely difficult or burdensome' for the data subject to be acquainted with that information.[1695] The emphasis on intelligibility is further justified by CJEU case law relating to the right of access.[1696]

There is limited understanding of how each data point impacts an ML model used for ADM.[1697] This holds true in case of complex models based on DL and ANNs and the problems described in Section

[1686] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 198.
[1687] 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, 600-604.
[1688] Recital 2 TSD.
[1689] EUIPO 'Protecting Innovation Through Trade Secrets and Patents: Determinants for European Union Firms' (2017) <https://euipo.europa.eu/ohimportal/en/web/observatory/news/-/action/view/3704420> accessed 8 February 2024.
[1690] Because it is not required to undergo the burdensome process of obtaining a patent, for instance. See also Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 10.
[1691] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 58.
[1692] Ibid.
[1693] Case C-487/21, *F.F.* [2022] ECR I-1000 paras 37-38, also Opinion of AG Pitruzella paras 55-56.
[1694] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella paras 55-56.
[1695] Ibid para 76.
[1696] Cases C/141/12 and C-372/12, *YS* [2014] ECR I-2081 paras 57, 60.
[1697] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 1 and 3 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.

2.2.1.4. More specifically, it seems impossible to understand what happened in the intermediate (hidden) layers of an ANN.[1698] Most of the current DL models lack reasoning and explanatory capabilities, which makes them vulnerable to produce unexplainable outcomes. In addition, ML becomes increasingly opaque, and even if the underlying principles of ML models are understood, they lack explicit declarative knowledge.[1699] Understanding the causes and correlations of algorithmic decisions currently constitutes one of the major challenges of computer science.[1700] There are some methods to facilitate comprehension of ADM logic.[1701] For example, external explanation systems aim to analyse an AI system and propose explanations by means of two approaches: the white-box approach analyses the code, and the black-box approach is used to probe the ADM by simulating different input and observing the results if no knowledge of the code is available. Both approaches have advantages and drawbacks. Due to technical constraints, the explanation might be limited in case of external black-box approaches, which cannot explain the different steps of an ADM process: only the output, i.e. the final step of the ADM, is explained. How the input is used to produce internal representations remains unknown. External white-box approaches need access to the source code and do not provide explanations in itself but only show some general properties of an ADM system.[1702] It remains unclear whether these methods are helpful for laypersons.[1703] It has been argued that they fall short in providing optimal granularity of explanation for non-experts.[1704] In particular, in ML which is often used for ADM, an affected individual may hardly have any concrete sense of how or why a particular classification results from input.[1705]

Even if an AI system in the future will be able to list all factors that have influenced the ADM process and rank them according to their statistical relevance, it is likely that such information exceeds a data subject's capacity to process such information, resulting in the provision of information that is meaningless rather than meaningful.[1706] Due to these technological shortcomings, controllers cannot

[1698] Ethem Alpaydin, *Machine Learning: The New AI* (3rd edn MIT Press 2016) 155.
[1699] Andreas Holzinger, 'From Machine Learning to Explainable AI' (IEEE DISA Conference, Kosice, August 2018) <https://www.aholzinger.at/wordpress/wp-content/uploads/2020/07/For-Students-HOLZINGER-2018.pdf> accessed 8 February 2024.
[1700] Maja Brkan, Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas' (2020) Vol 11 Iss 1 European Journal of Risk Regulation, 18.
[1701] 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 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[1702] Maja Brkan, Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas (2020) Vol 11 Iss 1 European Journal of Risk Regulation 18, 34, 37-38.
[1703] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 90.
[1704] 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 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[1705] Jenna Burrel, 'How the machine 'thinks': understanding opacity in machine learning algorithms' (2016) Vol 3 Iss 1 Big Data Society 1-12 < https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512 > accessed 8 February 2024.
[1706] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 89.

comply with the legal obligation imposed on them to provide meaningful information about the *logic* involved in ADM.[1707] According to Article 12 (1) GDPR, information must be intelligible, allowing the data subject to familiarise itself with it fully, easily and without difficulty.[1708] However, current approaches to explain the logic involved in ADM are hardly helpful for laypersons[1709] because they fall short in providing optimal granularity of explanation for non-experts[1710] such as data subjects. Rather, such information makes it 'extremely difficult or burdensome' for the data subject to be acquainted with that information.[1711] This leads to a Type 1 legal problem because meaningful information about the logic involved in ADM cannot be provided in an intelligible manner, which violates both Article 15 (1) lit h and Article 12 (1) GDPR. In fact, empirical research on the matter confirms this conclusion: controllers do not routinely comply with Article 15 (1) lit h GDPR in practice.[1712]

The meaningless information problem (Type 1)

With complex models based on DL and ANNs, it seems impossible to understand what happened in the intermediate (hidden) layers of an ANN when used for ADM. Even if future AI systems will be able to list all factors that have influenced an ADM process, it is likely that such information exceeds a data subject's capacity to understand it, resulting in the provision of meaningless, rather than meaningful information. This violates Articles 12 (1) and 15 (1) lit h GDPR.

5.6.2 Legal problems: Type 2

A Type 2 legal problem is caused by the non-absolute nature of the right of access combined with the broad scope of protection for AI as trade secrets. This Type 2 legal problem with respect to the enforcement of the right of access is twofold. As outlined in Section 5.6, the right of access may be restricted in two ways, i.e. in line with the provisions contained in Article 23 GDPR and in accordance with Article 15 (4) GDPR. Restrictions under Article 15 (4) GDPR differ from restrictions possible under Article 23 GDPR. Article 15 (4) *exclusively* applies to the right to obtain a copy of the personal data enshrined in Article 15 (3) GDPR and allows restrictions on a *case-by-case* basis, whereas restrictions according to Article 23 GDPR need to be laid down in Member State or Union law. Thus, trade secret protection allows controllers to restrict the right to obtain a copy of the personal data in line with Article 15 (4) GDPR, as well as to restrict access to information about processing according

[1707] Maja Brkan, Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas (2020) Vol 11 Iss 1 European Journal of Risk Regulation 18, 39.
[1708] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 76.
[1709] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 90.
[1710] 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 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[1711] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 76.
[1712] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 11.

to Article 15 (1) GDPR,[1713] provided this occurs in accordance with Article 23 GDPR. I begin with the latter.

Access to information

Many of the fundamental components required to understand AI systems and ensure accountability are barely subject to scrutiny because they are hidden by trade secrets or IP laws.[1714] According to an AI now report, 'one significant barrier to accountability is the culture of industrial and legal secrecy that dominates AI development.'[1715] In fact, Recital 14 TSD specifically includes 'technological information' in the definition of trade secrets, which is significant in the context of AI. Technological information related to an AI system is protected if there is a legitimate interest in maintaining the confidentiality of such information and if there is also a legitimate expectation in the preservation of such confidentiality.[1716] Technological information includes both information about the development and production of the product concerned, as well as information about its actual configuration and functionalities.[1717] In the context of AI systems used to process and generate personal data, technological information is protected in the form of the algorithm[1718] as well as the system's internal components expressed in source code format,[1719] its functionality[1720] and other system artefacts. Put simply, an algorithm is 'the sum of logic and control that has its origins in ancient mathematics'[1721] and is typically a numerical process that consists of a sequence of well-defined steps leading to the solution of a particular type of problem.[1722] The source code is a set of human readable computer commands written in high-level programming languages.[1723]

In order to thoroughly evaluate compliance with applicable legal provisions such as the fairness principle[1724] or ADM,[1725] access to the source code and algorithms at the heart of the AI systems would be required.[1726] For example, to assess potentially discriminatory outcomes of ADM, information regarding comparison groups would be needed. However, particular information about the functionality of algorithms is often poorly accessible[1727] and falls under the scope of trade secret protection within the

[1713] Most importantly information about the logic involved in ADM according to Article 15 (1) lit h GDPR.
[1714] Alex Campolo et al, 'AI Now Report' (2018) 11 < https://ainowinstitute.org/publication/ai-now-2018-report-2 > accessed 8 February 2024.
[1715] Ibid.
[1716] Recital 14 TSD.
[1717] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 346.
[1718] Ibid 72, 308.
[1719] Noam Shemtov, Beyond the Code: Protection of Non-Textual Features of Software (Oxford University Press 2017) 71.
[1720] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 346.
[1721] Andrew Goffey, 'Algorithm' in Matthew Fuller (ed) *Software Studies: A Lexicon* (MIT Press 2008).
[1722] Yadolah Dodge, 'Algorithm' in: *The Concise Encyclopedia of Statistics* (Springer New York 2006) 1-2.
[1723] Joasia Krysa, Grzesiek Sedek, 'Source Code' in Matthew Fuller (ed) *Software Studies: A Lexicon* (MIT Press 2008).
[1724] Art 5 (1) lit a GDPR.
[1725] Art. 22 GDPR, and applicable requirements regarding transparency according to Art 13 (2) lit f GDPR.
[1726] Danielle Citron Keats, Frank Pasquale, 'The scored society: Due process for automated predictions' (2014) Vol 89 Iss 1 Washington Law Review, 1, 14.
[1727] Brent Daniel Mittelstadt et al, 'The ethics of algorithms: Mapping the debate' (2016) Vol 3 Iss 2 Big Data & Society 1, 6.

EU.[1728] This makes it difficult for supervisory authorities (SAs) and individuals concerned to verify compliance with the existing legal framework. The legislator anticipated the need for data subjects to obtain information with respect to ADM by requiring controllers to inform them about 'meaningful information about the logic involved' when they enforce their right of access.[1729] Information about the logic involved could fall under the scope of trade secrets because protected technological information includes both information about the development and production of a product and information about its actual configuration and functionalities.[1730] Applied to AI systems and products, the protection offered is broad and comprises the technical method and tools[1731] used to process and obtain information[1732] and thus arguably also how the AI system achieved its automated decision.

For example, in a case dealing with the creation of score values concerning the creditworthiness of individuals, the German Federal Court of Justice ruled that the abstract method of the calculation of the score value, comprising of i) general operandi such as statistical values used, ii) the weighing of specific elements within the calculation of the probability value and iii) the creation of comparison groups do not have to be disclosed because it falls within the scope of trade secrets.[1733] One case[1734] pending at the CJEU specifically addresses the tension between trade secrets and the right of access enshrined in the GDPR. It concerns the German credit agency that automatedly calculated a credit score for a data subject. The data subject exercised her right to access according to Article 15 GDPR and requested the credit agency to provide 'meaningful information about the logic involved' with respect to the ADM to which she was subject (the automated calculation of the credit score). The CJEU is supposed to provide an answer to the question whether Article 15 (1) lit h GDPR obliges the controller to disclose the information which is essential for enabling the comprehensibility of the result of the ADM in the individual case, if necessary while maintaining an existing trade secret.[1735] One of the questions referred to the CJEU is of significant importance in the context of AI and trade secrets, namely, whether meaningful information about the logic involved requires the controller to disclose parts of the algorithm on which the ADM is based for achieving comprehensibility of the

[1728] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1 (Trade Secrets Directive).
[1729] Article 15 (1) lit h GDPR.
[1730] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 346.
[1731] Bart Custers, Anne-Sophie Heijne, 'The right of acces in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 10.
[1732] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 197, 201.
[1733] VI/ZR 156/13, BGH (German Federal Court of Justice), judgement of 28 January 2014 [27].
[1734] Case C-203/22 *Dun & Bradstreet Austria.*
[1735] Among other, the CJEU needs to answer whether the data subject exercising its right of access in the context of an ADM must be provided with a) information outlining in which manner personal data are processed, b) input data used for profiling, c) parameters and input variables used in the assessment determination, d) the influence of theses parameters and input variables on the calculated rating, e) information on how the parameters or input variables were arrived at and f) explanations on why the data subject was assigned to a certain evaluation result and presentations of the statement associated with this evaluation, enumeration of the profile categories and explanation of which evaluation statement is associated with each of the profile categories. Article 15 (1) lit h GDPR.

ADM.[1736] In my view, it is unlikely that the CJEU answers this question in the affirmative because the partial disclosure of an algorithm is not intelligible as required by Article 12 (1) GDPR. According to Article 12 (1) GDPR, information must be intelligible, allowing the data subject to familiarise itself with it fully, easily and without difficulty.[1737] This criterion will not be met if the controller provides the data subject with the algorithm or a part of it. AG Pikamäe agrees. He notes that Article 12 (1) GDPR precludes the provision of highly complex information, such as the algorithm used to calculate a score value.[1738]

Information according to Article 15 (1) lit h GDPR may be restricted provided that the requirements set out in Article 23 GDPR are complied with. Article 23 GDPR allows for restrictions of the rights enshrined in Articles 12 to 22 GDPR if (i) provided for in EU or Member State law applying to the controller, (ii) the restriction respects the essence of the fundamental rights and freedoms and (iii) is a necessary and proportionate measure to safeguard, among others, the rights and freedoms of others. Thus, in the situations listed in Article 23 GDPR, private interests can limit the scope of the rights conferred on data subject as introduced in Section 3.3.4 and the corresponding obligations imposed on controllers mentioned in Section 3.3.3.[1739] This holds true regardless of the AI discipline used because trade secret protection applies to all AI disciplines. As outlined in Section 5.6, the term 'rights and freedoms of others' includes trade secrets and IP rights. The TSD and its national laws implementing it constitute EU or Member State law in the sense of the first requirement (i).

With regard to requirement (iii), Malgieri and Comandé argue that there is a legal preference for data protection rights when the latter clash with trade secrets and that the GDPR has intensified this preference.[1740] Among others, they derive this prevalence from Recital 35 TSD which states that the latter should *not affect* the fundamental right to data protection, particularly the right of access and other rights enshrined in the GDPR,[1741] whereas Recital 63 GDPR states that data protection rights should not *adversely* affect trade secrets. According to the authors, the adverb 'adversely' contained in the GDPR reveals that trade secrets can never affect data protection rights, while the right of access can affect trade secrets, but not 'adversely'.[1742] However, that EU law provides greater priority to the

[1736] 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.
[1737] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 76.
[1738] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 57.
[1739] Case C-620/19 *Land Nordrhein Westfalen* [2020] ECR I-1011 paras 42, 46; Case C-620/19 *Land Nordrhein Westfalen* [2020] ECR I-649, Opinion of AG Bobek, para 81.
[1740] Claudio Malgieri, Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) Vol 7 No 4 International Data Privacy Law 243, 262, 264.
[1741] Note that Recital 35 TDS refers to the Data Protection Directive which was replaced by the GDPR.
[1742] Claudio Malgieri, Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) Vol 7 No 4 International Data Privacy Law 243, 263.

fundamental right to data protection than safeguarding commercial interests covered by trade secrets is not an accurate claim.[1743]

First, the TSD itself clearly does *not* contain a priority for the fundamental right to data protection. Article 5 TSD limits the scope of trade secret protection,[1744] among others, by restricting trade secret protection in situations of conflicts with the fundamental right to freedom of expression and information (Article 11 EUCFR). If the intention of the EU legislator was to grant the fundamental right to data protection priority over trade secret protection, it would have referred to Article 8 EUCFR in the text of Article 5 TSD, as it did with the fundamental right to freedom of expression and information.

Second, the claim of prevalence for the fundamental right to data protection neglects relevant case law adopted by the CJEU in the context of balancing the fundamental right to data protection with IP rights. Case law indicates that the protection of IP rights may prevail over the protection of personal data: The CJEU considered that the obligation to communicate personal data to private persons in civil proceedings was likely, in principle, to ensure a fair balance between the protection of IP rights and the protection of personal data.[1745] This requirement affirms the rule of non-prevalence in line with other CJEU case law and also rejects arguments made in academia that trade secrets generally prevail over the interests of data subjects and their right of access.[1746] The CJEU stressed the need to reconcile the requirements of the protection of different fundamental rights, such as the fundamental right to privacy and data protection, on the one hand, and the fundamental right to property (including IP and trade secrets[1747]) on the other hand.[1748] 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.[1749] More specifically, Article 23 (1) GDPR seeks to strike a fair balance between the data subjects fundamental right to data protection and the need to safeguard other legitimate interests. This necessitates weighing the fundamental right to data protection conferred on natural persons against the interests that those restrictions are intended to preserve.[1750]

[1743] 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 19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[1744] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 211.
[1745] See C-461/10 *Bonnier Audio AB* [2012] paras 57-60.
[1746] See, for instance, 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, 17.
[1747] Case C-1/11 *Interseroh Scrap* [2012] ECR I-194 para 43; Case T-189/14 *Deza* [2017] para 163.
[1748] Dominique Moore, Commentary of Article 23 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 548.
[1749] Case C-275/06 *Promusicae* [2008] ECR I-00271 paras 65, 68.
[1750] Case C-620/19 *Land Nordrhein Westfalen* [2020] ECR I-1011 para 48; Case C-620/19 *Land Nordrhein Westfalen* [2020] ECR I-649, Opinion of AG Bobek, paras 86 and 88.

Third, the TSD also indicates that the fundamental right to data protection and trade secrets must be respected simultaneously.[1751] Fourth, 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 to strike an appropriate balance between these two rights.[1752]

Therefore, it is possible that meaningful information about the logic involved in ADM might be restricted in accordance with Article 23 GDPR. Regulatory guidance adopted by the EDPB acknowledges this possibility by providing the example that a controller is not bound to reveal any part of the technical operating of software as long as such information can be regarded as a trade secret.[1753] Ultimately, the CJEU will provide clarity on how to proceed when the information to be provided according to Article 15 (1) lit h GDPR is classified as a trade secret within the meaning of Article 2 TSD.[1754] It seems clear that access to certain information is required in order to accurately evaluate compliance with applicable legal provisions such as the fairness principle[1755] or to evaluate ADM[1756] and enforce other data protection rights.

In the case pending at the CJEU, the technical expert appointed by the referring court concluded that specific information is required to ensure the comprehensibility of the calculated credit score. The expert argued that to make the concrete arithmetic operation used to calculate the credit score comprehensible, the detailed mathematical formula used needs to be disclosed next to the processed data. In addition, the expert concluded that comprehensibility is only given if the part of the algorithm is disclosed that was *actually used* by the controller for the calculation of the concrete credit score.[1757] If access to such information is denied in accordance with Article 23 GDPR, the individual concerned will have no opportunity to accurately assess compliance with applicable data protection rules and subsequently enforce other data protection rights, such as the right to rectification or erasure of personal data.[1758] This is because the AI system itself and the technical methods used to process and obtain information might be protected as a trade secret and/or as an IP right.[1759] As a consequence, Article 15 (1) lit h GDPR cannot be enforced, which constitutes a Type 2 legal problem. In fact, empirical research on Article 15 (1) lit h GDPR shows that most of the information required by this

[1751] Recital 34 TSD states that the TSD 'respects the fundamental rights….[ ]…notably the right to protection of personal data.... [ ]…while respecting business secrecy'.
[1752] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 55.
[1753] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 173.
[1754] Case C-203/22 *Dun & Bradstreet Austria*.
[1755] Art 5 (1) lit a GDPR.
[1756] Art. 22 GDPR, and applicable requirements regarding transparency according to Art 13 (2) lit f GDPR.
[1757] Case C-203/22 *Dun & Bradstreet Austria* p 12-14 <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.
[1758] Case C-553/07 *Rijkeboer* [2009] ECR I-03889, paras 51-52.
[1759] About IP rights, see 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 1-20.

provision is rarely or not at all provided in practice because controllers invoke trade secret protection to block or restrict such access requests.[1760]

The information restriction problem (Type 2)

Trade secret protection under the TSD covers AI itself including the technical methods used to process and obtain information and arguably also the particular way how the AI system achieved its ADM. Meaningful information about the logic involved in ADM according to Article 15 (1) lit h GDPR could therefore fall under trade secret protection, allowing controllers to restrict or refuse the provision of such information if this complies with the requirements set out in Article 23 GDPR. Consequently, data subject cannot enforce Article 15 (1) lit h GDPR.

It has been argued that even though algorithms may be protected by trade secrets, explaining the ADM based on that algorithm would not necessarily disclose the trade secret, for example, if only the main factor influencing a decision is required to explain the ADM. Alternatives proposed that do not involve the unlawful disclosure of trade secrets are probing the algorithm by a court or reverse engineering of the protected algorithm in the public domain.[1761] ADM is often influenced by more than one main factor. Probing the algorithm by a court does not seem to be a practical solution for the data subjects and would be in contravention with the law. The GDPR imposes the duty to explain the logic involved in ADM on the controller – it is not the data subject's task to invest time and financial resources to obtain such information. Article 12 (1) GDPR stipulates that information must be intelligible, meaning that it should be understandable for a data subject.[1762] Information should be provided in a manner that enables the data subject to familiarise herself with it fully, easily and without difficulty. Asking the data subject to probe the algorithm by a court would make it 'extremely difficult or burdensome' for the data subject to be acquainted with the information[1763] according to Article 15 (1) lit h GDPR. The same conclusion applies to reverse engineering, a technique to understand how a product was designed and operates[1764] (see also Section 6.5.2). In addition, the data subject should not have to extensively seek out information,[1765] as it must be 'easily accessible'[1766] and the verb 'provide' implies that the data subject is not required to actively search for information covered by Article 15 GDPR.[1767]

[1760] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1-16.
[1761] Maja Brkan, Grégory Bonnet, 'Legal and Technical Feasibility of the GDPR's Quest for explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas (2020) Vol 11 Iss 1 European Journal of Risk Regulation 18, 41.
[1762] Art 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP 260 rev.01, 11 April 2018) at 9.
[1763] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 76.
[1764] Noam Shemtov, Beyond the Code: Protection of Non-Textual Features of Software (Oxford University Press 2017) 71.
[1765] Art 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP 260 rev.01, 11 April 2018) at 11.
[1766] Article 12 (1) GDPR.
[1767] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 130; Art 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP 260 rev.01, 11 April 2018) at 33.

The transparency principle and particularly Article 12 GDPR is intertwined with the right of access. Article 12 GDPR is an expression of the transparency principle and aims to ensure that the data subject fully understands the information provided, allowing to effectively exercise the right of access and other data subject rights.[1768] Controllers must inform data subjects under Article 15 (1) GDPR in a way that enables complete access to the requested information.[1769] The two alternatives proposed, namely, probing by the Court and reverse engineering in the public domain, would conclusively lead to a Type 1 legal problem. The alternatives violate the modalities to provide information as required by Article 12 (1) GDPR, because that information must be intelligible and easily accessible.

Obtaining a copy of personal data

As mentioned in Section 3.3.4.1, the concept of copy is not defined in the GDPR. The CJEU ruled that a 'copy' refers to '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.[1770] In addition, the right to obtain a copy also includes information resulting from the processing of personal data, for example, a credit score.[1771] Faithful means 'true and accurate; not changing anything'[1772] and/or 'true or not changing any of the details, facts, style, etc. of the original'.[1773] The copy must enable the data subject to effectively exercise the right of access in full knowledge of all personal data undergoing processing, including personal data *generated* by the *controller*.[1774] The latter makes crystal clear that personal data generated by the controller with the support of AI systems or applications do fall within the scope of the right to obtain a copy of the personal data undergoing processing. However, Article 15 (3) GDPR does not require the provision of a copy of the document, but a copy of the personal data. The CJEU found that there is no right to obtain a copy of the document containing the personal data.[1775] In addition, Article 15 (3) GDPR does not provide the data subject with a right to obtain information regarding the criteria, models, rules or internal procedures (whether or not computational) used for processing the personal data.[1776]

Article 15 (4) GDPR states that the right to obtain a copy of personal data undergoing processing according to Article 15 (3) GDPR 'should not adversely affect the rights or freedoms of others'. Recital 63 GDPR clarifies that this refers to trade secrets, intellectual property and copyright protecting the software. By directly referring to Article 15 (3) GDPR, this limitation of the right of access

[1768] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella paras 55-56.
[1769] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 130.
[1770] Case C-487/21, *F.F.* [2022] ECR I-1000 para 21.
[1771] Ibid, para 26.
[1772] See <https://www.oxfordlearnersdictionaries.com/definition/english/faithful?q=faithful> and < accessed 8 February 2024.
[1773] See < https://dictionary.cambridge.org/dictionary/english/faithful > accessed 8 February 2024.
[1774] Case C-487/21, *F.F.* [2022] ECR I-1000 paras 26, 39; see also the opinion of AG Pitruzella paras 45, 70.
[1775] Cases C/141/12 and C-372/12, *YS* [2014] ECR I-2081 paras 58-59.
[1776] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 52.

only applies to the right to obtain a copy of personal data undergoing processing, but not to Article 15 (1) GDPR.[1777]

As outlined in Section 5.6, Article 15 (4) GDPR allows controllers to restrict the right to obtain a copy of the personal data on a case-by-case basis. This gives controllers more leeway and flexibility in restricting access requests concerning Article 15 (3) GDPR, because these restrictions do not have to be enshrined in EU or MS law.[1778] The restriction of the right to obtain a copy of the personal data enshrined in Article 15 (4) GDPR is particularly relevant if the information protected as a trade secret constitutes personal data. As outlined in Section 5.6, trade secret protection covers training and output data,[1779] information[1780] on or knowledge about customers, information about a customer's behaviour (creditworthiness, lifestyle)[1781] and predictions such as a customer's future life (life expectancy, estimated advancements in career, etc.).[1782] More generally, any output generated by an AI system constituting personal data, such as a data subject's detected emotional state could fall under the trade secret protection.[1783] Therefore, the exception enshrined in Article 15 (4) GDPR is particularly problematic in the context of AI.

Imagine, for instance, an AI system that intends to detect the emotional state of an individual powered by the discipline AC. The data subject enforces her right of access by specifically requesting a copy of the personal data undergoing processing[1784] to determine what emotional state the system has discovered. Then, the controller refers to trade secret protection and argues that he is not obliged to disclose the detected emotional state (e.g., fear or anger) even though such information constitutes sensitive personal data. In the sketched situation, the data subject cannot gain access to her own personal data generated by AI (AC).

The same applies to the AI system introduced in Section 4.4.3 which uses unsupervised ML techniques to automatically predict the life expectancy of insurance companies' clients based on relatively simple personal data, such as the gender and place of residence of the clients. Also, here, the controller may refuse to disclose the life expectancy predictions due to trade secret protection.

[1777] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 169. However, such restriction might be possible under Article 23 GDPR.
[1778] As it is the case of restrictions made on the basis of Article 23 GDPR.
[1779] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 197, 201.
[1780] Teresa Trallero Ocaña, *The Notion of Secrecy* (Nomos 2021) 312.
[1781] 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.
[1782] 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; 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.
[1783] 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.
[1784] Article 15 (3) GDPR

Output produced by AI that constitute personal data does not need to be correct to fall under trade secret protection: information or knowledge protected under the TSD may be very well incorrect or incomplete.[1785] Therefore, if a data subject enforces the right of access in order to 'be aware of, and verify, the lawfulness of the processing',[1786] controllers are likely to argue that disclosure of output produced by an AI system constituting personal data infringes their trade secrets or IP rights.[1787] Companies may merely provide restricted information, such as naming the category 'emotion data' or 'life expectancy prediction' instead of disclosing the predicted life expectancy or detected emotional state. This approach would be in line with Recital 63 GDPR, which states that considerations with respect to trade secrets should not result in 'a refusal to provide all information to the data subject'. This will likely be considered acceptable by supervisory authorities (SAs). Regulatory guidance concerning transparency[1788] simply requires controllers to inform data subjects about the 'categories of the inferred data processed'.[1789] Both emotional states as well as life expectancy predictions are inferred data defined as 'the product of probability-based processes'.[1790] Furthermore, a data subject cannot request a copy of the *document* containing the personal data undergoing processing, such as the report generated by AC system HireVue.[1791] Article 15 (3) GDPR does not require the controller to provide a copy of the document containing personal data.[1792] Indeed, the CJEU confirmed that there is no right to receive a copy of the document containing the personal data undergoing processing.[1793] Likewise, Article 15 (3) GDPR does not provide the data subject with a right to obtain information regarding the criteria, models, rules or internal procedures (whether or not computational) used for processing the personal data.[1794] Again, instead of disclosing the detected emotional state or predicted life expectancy, the controller may just indicate the category of personal data, such as 'emotion data' or 'life expectancy prediction', in order to protect its trade secrets.

[1785] Ana Nordberg, 'Trade secrets, big data and artificial intelligence innovation: a legal oxymoron?' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds) *The Harmonization and Protection of Trade Secrets in the EU* (Edward Elgar Publishing 2020) 200.
[1786] Recital 63
[1787] Bart Custers, Anne-Sophie Heijne, 'The right of acces in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 10.
[1788] Dealing with the transparency principle and Articles 12-14 GDPR.
[1789] Art 29 Working Party, 'Guidelines on transparency under Regulation 2016/679' (WP 260 rev.01, 11 April 2018) in footnone 30 at page 14.
[1790] 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.
[1791] 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.
[1792] Note however that this depends on local guidance and local case law, arguably leading to 'unharmonized' results across the EU; Gabriela Zanfir-Fortuna, Commentary of Article 15 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 464.
[1793] Cases C-141/12 and C-372/12, *YS* [2014] ECR I-2081 paras 58-59. Note that the CJEU relativated this to some extent. It might be needed to provide the reproduction of extracts from documents or even entire documents ore extracts from databases containing personal data to ensure the copy provided is intelligible. See Case C-487/21, *F.F.* [2022] ECR I-1000 para 41.
[1794] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella para 52.

As a result of this, the individual concerned has no means of accessing the specific emotional state detected by the AI system or the predicted life expectancy. This is particularly relevant because the right of access is decisive for other data protection rights and enables the data subject to obtain, depending on the circumstances, rectification, erasure or blocking of his or her personal data by the controller. This leads to a significant loophole because the data subject cannot verify the accuracy of the emotion data detected by the AI system. I use the term 'loophole' because in my view, data subjects should be able to see which emotion the machine recognises, in particular when considering the sensitive nature of emotion data.[1795] Without that knowledge, an individual will hardly be able to obtain rectification of inaccurate data because it is the individual that must demonstrate the inaccuracy of personal data (see Section 5.7). Note that life expectancy predictions or emotional states detected by the AI system may be protected under the TSD even if they are incorrect.[1796]

Because the TSD provides extensive protection for input data and output data in all AI disciplines and because trade secrets are widely used, it will hardly be possible for individuals concerned to accurately assess compliance with the GDPR and enforce other data subject rights such as rectification or erasure. Controllers are likely to invoke trade secret protection to deny full or partial access to personal data undergoing processing.[1797] Already in 2011, Facebook denied a data subject access to his personal data because such disclosures 'would adversely affect trade secrets'.[1798] Trade secret protection hampers the thorough enforcement of the right to obtain a copy of the personal data processed, which constitutes a Type 2 legal 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.

[1795] I derive this requirement from the underlying ideas of the transparency *and* fairness principle.
[1796] Information or knowledge protected under the TSD does not have to be correct or complete.
[1797] Bart Custers, Anne-Sophie Heijne, 'The right of acces in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 15.
[1798] See < http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf > accessed 8 February 2024.

5.6.3 Legal problems: Type 3

The trade secrets problem explained in Section 5.6.2, i.e. that controllers may deny data subjects copies of personal data undergoing processing, also leads to a Type 3 legal problem. Because data subjects cannot gain access to the personal data processed by a controller to verify the lawfulness of processing[1799] and to obtain the rectification, erasure or blocking of personal data,[1800] Article 15 (3) GDPR is not fit for purpose to effectively[1801] protect the fundamental right to data protection. The right of access is a conditio sine qua non for exercising other data subject rights and restrictions on or around this right cause a knock-on effect on the entire data protection law regime.[1802] The CJEU stressed the importance of ensuring that data subject rights granted by the GDPR are effective.[1803] Article 15 (3) GDPR is not effective because it allows controllers to extensively restrict this right based on Article 15 (4) GDPR. Controllers may easily invoke this provision by arguing that the disclosure of personal data generated by means of AI violates their trade secret protection. In such cases, the data subject must initiate legal proceedings against the controller[1804] or lodge a complaint with the competent SA[1805] to challenge the controller's restriction of Article 15 (3) GDPR. The lack of sufficient resources for SAs[1806] and the EDPB[1807] is widely known, which causes delay of regulatory enforcement. According to a report published by the EDPB in 2021, it took the Irish SA an average of 16 months to formally decide on purely *national cases* and 23 months for cases subject to the *cooperation procedure*.[1808] The Irish SA is the lead supervisory authority for most of the 'big tech' companies, including Meta Platforms Ireland Limited, Google Ireland Limited, WhatsApp Ireland Limited, Airbnb Ireland UC, Twitter International Company, Microsoft Ireland Operations Limited, LinkedIn Ireland UC and Apple Distribution International.[1809] In terms of private enforcement, according to Article 79 GDPR, the timeframe to obtain a final decision is even longer, when considering that 'big tech' companies may be willing to exhaust all possible legal remedies and that such cases raise new points of law and ultimately end up at the CJEU. Thus, when taking the broad exception

[1799] Recital 63 GDPR.
[1800] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44.
[1801] Recital 11 GDPR.
[1802] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 285.
[1803] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[1804] Article 79 GDPR.
[1805] Article 77 GDPR.
[1806] EDPB, 'Overview on resources made available by Member States to the Data Protection Supervisory Authorities' (2022) at 5 <https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstates-tosas2022_en.pdf> accessed 8 February 2024.
[1807] 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.
[1808] EDPB, 'Overview on resources made available by Member States to the Data Protection Supervisory Authorities' (2021) at 21 < https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf > accessed 8 February 2024.
[1809] See < https://www.dataprotection.ie/sites/default/files/uploads/2022-03/DPC%20statistical%20report%20on%20OSS%20cross-border%20complaints.pdf > accessed 8 February 2024.

according to Article 15 (4) GDPR and the long enforcement timeframes into account, Article 15 (3) GDPR is not an effective right.

Articles 15 (3) and 15 (4) GDPR also fail to achieve the GDPR's legislative aim to strengthen the rights of data subjects.[1810] As noted by the CJEU, effective protection of personal data requires the strengthening of the rights of data subjects, which is emphasised by Recital 11 GDPR.[1811] Article 15 (3) GDPR specifically aims to strengthen the position of the data subject.[1812] Instead of strengthening the right of access, the broad scope of restrictions possible under Article 15 (4) GDPR weakens this right and thus fails to achieve the GDPR's legislative aim. Additionally, these newly introduced provisions do not achieve the GDPR's goal that 'natural persons should have control of their own personal data',[1813] although this was one of the main reasons for the data protection reform.[1814] As outlined in Section 4.4.3, one of the main mechanisms for data subjects to exercise control over the processing of their personal data under the GDPR are data subject rights. Control in the sense of the GDPR is rather limited from a conceptual point of view. In a preliminary ruling, the AG acknowledged that 'the scope for individual action is limited' and 'confined to the exercise of those rights in specified circumstances'.[1815] Article 15 (4) GDPR further restricts the already limited mechanism for data subjects to exercise control over the processing of their personal data.

This is especially true for AC, which can generate inaccurate personal data (see Section 4.7.1). Without access to the specific emotional state detected by the AI system deploying AC approaches, a data subject cannot verify the accuracy of the output data and subsequently request the rectification or erasure of such personal data. The same applies to ML, which generates predictions and establishes correlations that are probabilistic and thus constitute uncertain knowledge, which may lead to inaccurate evaluations and representations of data subjects. Article 15 (3) GDPR is the last resort for data subjects to obtain the specific emotional state detected by AC or the exact prediction or correlation generated by ML to subsequently enforce other rights of the data subject, such as the right to rectification or erasure. Due to the broad scope of protection provided by the TSD for *all AI* disciplines as introduced in Chapter 2, this Type 3 legal problem constitutes a general problem and relates to all AI disciplines discussed in Chapter 2.

It remains unclear how a controller must, in fact, respond to an access right request according to Article 15 (1) GDPR and what information must be included in such a response. The standard adopted by the GDPR requires that information must be provided to data subjects in a 'concise, intelligible

[1810] Recital 11 GDPR.
[1811] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[1812] Case C-487/21, *F.F.* [2022] ECR I-1000 para 33; see also the opinion of AG Pitruzella para 69.
[1813] Recital 7 GDPR.
[1814] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona paras 69, 70.
[1815] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona para 72.

and easily accessible form, using clear and plain language'.[1816] It is unclear what this means in the context of the right of access, particularly when it concerns meaningful information about the *logic* involved in ADM. Research[1817] suggests that such information refers to a description of the technologies used rather than access to the code or software itself. The dearth of corresponding literature underscores that the matter has not received much attention in academia or practice,[1818] nor in regulatory guidance.

With regard to information according to Article 15 (1) lit h, the EDPB takes the view that such information could be based on the privacy notice of a controller subject to being 'updated and tailored' to the data subject making the request[1819] and should, *if possible*, 'be more specific in relation to the reasoning that lead to specific decisions concerning the data subject who asked for access'.[1820] Regulatory guidance also states that such information does not necessarily entail complex information of the algorithms used or disclosure of the algorithm.[1821] Instead of providing a complex mathematical explanation about how algorithms and AI used for ADM work, controllers should provide general information such as factors taken into account for the ADM process and their respective weight on an aggregated level. In addition, controllers should disclose the categories of data that have been or will be used for ADM, why these categories are pertinent, how any profile used in the ADM process is built, including any statistics used in the analysis, why this profile is relevant to the ADM process and how it is used for a decision with respect to the data subject.[1822] In addition, regulatory guidance seems to indicate that Article 15 (1) lit h GDPR does not oblige controllers to explain *particular decisions* to data subjects, but rather to oblige them to provide information about the envisaged consequences of the processing. In view of the EDPB, the right to receive meaningful information about the logic involved in ADM does *not* seem to entail a right for data subjects to obtain explanation of particular decisions because Article 15 (1) lit h GDPR entitles data subjects to obtain the *same information* as required under Articles 13 (2) lit f and 14 (2) lit g GDPR.[1823]

Views in scholarship diverge on what information controllers must provide under Article 15 (1) lit h GDPR. There is a vivid debate whether or not the GDPR provides a right to explanation of specific ADM or not.[1824] With regard to the information to be provided specifically under Article 15 (1) lit h

[1816] Article 12 (1) GDPR.
[1817] Bart Custers, Anne-Sophie Heijne, 'The right of acces in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 16.
[1818] Ibid.
[1819] European Data Protection Board, 'Guidelines 01/2022 on data subject rights – Right of access Version 2.0' (28 March 2023) at 20, 113.
[1820] Ibid at 119.
[1821] 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 25.
[1822] Ibid 31; see also Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 58.
[1823] 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 26, 27.
[1824] 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

GDPR, Malgieri and Comandé argue that such information must adhere to the standard of legibility, which requires that the information provided is both transparent and comprehensible and that such information must go 'beyond the mere mathematical functionality of an algorithm' and consider contextual use, expected and actual impact, rationales and purposes.[1825] Wachter, Mittelstadt and Floridi take the view that the right of access only grants an explanation of the logic and general functionality of an ADM system, but not the rationale and circumstances of specific decisions. Additionally, 'meaningful information' would not entail an obligation to disclose the algorithm, but only the provision of 'basic information' about its logic.[1826] Finally, empirical research on Article 15 (1) lit h GDPR suggests interpreting it as information that is useful and/or has practical value for data subjects.[1827] Obviously, this interpretation has a contextual component. It refers to useful and practical information for data subjects to (i) become aware of processing relating to ADM, (ii) enforce their data subject rights (e.g. contesting to ADM) and thus (iii) exercise control over the processing of their personal data. This interpretation is also in line with the requirement of intelligibility as enshrined in Article 12 (1) GDPR. This provision ensures that the data subject fully understands the information provided,[1828] enabling *effectively* exercise of the right of access and other data subject rights.[1829]

However, as pointed out in Section 5.6.2, in a CJEU case relating to explanation of the logic involved in ADM, the technical expert appointed by the referring court concluded that, in order to comprehend the logic involved and evaluate the ADM at hand, at least the disclosure of a part of the algorithm would be required, together with other detailed information. The latter include the concrete factors and mathematical formula used, the concrete value assigned to the data subject and the disclosure of the intervals within which different data on the same factor are assigned to the same value.[1830] It is unlikely that the CJEU will accept this interpretation. As AG Pikamäe notes, the requirement of intelligibility enshrined in Article 12 (1) GDPR precludes the provision of highly complex information, such as the algorithm or the mathematical formula used.[1831] As outlined in Section 5.6.2, this information is meaningless rather than meaningful for most data subjects.

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.

[1825] Giancludio Malgieri, Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) Vol 7 Iss 4 IDPL 243, 245, 257, 258.

[1826] 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, 84, 90.

[1827] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 14.

[1828] Case C-487/21, *F.F.* [2022] ECR I-1000 paras 37, 38.

[1829] Case C-487/21, *F.F.* [2022] ECR I-1000, Opinion of AG Pitruzella paras 55-56.

[1830] 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.

[1831] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 57.

Another highly relevant question is whether controllers must provide meaningful information about the logic involved with regard to a *particular decision*. Regulatory guidance[1832] as well as the scholars Wachter, Mittelstadt and Floridi[1833] suggest answering this question negatively. I do not agree. If information according to Article 15 (1) lit h GDPR does not relate to a particular decision, it cannot be useful or meaningful for data subjects. To determine what information could be useful and/or of practical value ('meaningful') for data subjects, it is worth considering what is typically required if humans are asked for an explanation of a specific decision. What humans usually want to know is whether and how certain input factors affected the final decision or outcome.[1834] Such causal explanation helps individuals to modify their behaviour or consider which factors they must challenge in order to change the decision.[1835] Thus, in order to be meaningful for data subjects, information according to Article 15 (1) lit h GDPR needs to explain how certain input factors affected the final ADM.[1836] Causal explanation relating to a *specific* automated decision would enable data subjects to determine which factors they must challenge in order to change the ADM,[1837] by obtaining human intervention, expressing their point of view and contesting the decision as foreseen in Article 22 (3) GDPR. AG Pikamäe seems to agree. With regard to the automated establishment of a score value, controllers must provide 'sufficiently detailed explanations of the method for calculating the score value and the reasons that led to a *particular* result.'[1838]

However, neither the GDPR and its corresponding recitals nor regulatory guidance seem to suggest such an interpretation of meaningful information about the logic involved in a specific automated decision. The opinion of AG Pikamäe is not legally binding, and the CJEU completely ignored this point in the corresponding ruling. Thus, data subjects do not know the input factors that affected a specific automated decision and cannot effectively enforce their right to contest ADM according to Article 22 (3) GDPR. Therefore, information according to Article 15 (1) lit h GDPR is not useful and/or of practical value for data subjects. In addition, empirical legal research on Article 15 (1) lit h GDPR concludes that the right of access, particularly Article 15 (1) lit h GDPR, does not function adequately in practice.[1839]

[1832] 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 26, 27.
[1833] 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, 84, 90.
[1834] Finale Doshi-Velez et al, 'Accountability of AI Under the Law: The Role of Explanation' (2017) Berkman Klein Center Working Group on Explanation and the Law Working Paper 1 <https://dash.harvard.edu/bitstream/handle/1/34372584/2017-11_aiexplainability-1.pdf> accessed 8 February 2024.
[1835] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 88.
[1836] Finale Doshi-Velez et al, 'Accountability of AI Under the Law: The Role of Explanation' (2017) Berkman Klein Center Working Group on Explanation and the Law Working Paper 1 <https://dash.harvard.edu/bitstream/handle/1/34372584/2017-11_aiexplainability-1.pdf> accessed 8 February 2024.
[1837] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 88.
[1838] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 58.
[1839] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 16.

Therefore, Article 15 (1) lit h GDPR is not fit for purpose to effectively protect the fundamental right to data protection[1840] and strengthen data subject rights as envisaged by the GDPR.[1841] The CJEU emphasised that effective protection of personal data requires the strengthening of the rights of data subjects[1842] and also stressed the importance of ensuring that data subjects rights granted by the GDPR are effective.[1843] A right that fails to provide data subjects with information that is useful and/or of practical value with regard to other data subject rights enshrined in the GDPR is ineffective. Consequently, it also fails to strengthen the rights of the data subject. Likewise, this provision fails to achieve the GDPR's legislative goals to enhance legal and practical certainty for data subjects and to provide data subjects with control over the processing of their own personal data.[1844] As outlined in Section 4.4.3, control in the sense of the GDPR is limited to two main mechanisms, namely, consent and data subject rights. Regarding the latter, even AG Campos Sánchez-Bordona acknowledged that 'the scope for individual action is limited' and 'confined to the exercise of those rights in specified circumstances'.[1845] Article 15 (1) lit h GDPR further restricts the mechanism for data subjects to exercise control, in particular regarding their right to contest to ADM according to Article 22 (3) GDPR. Due to the lack of causal explanation relating to a *specific* automated decision, it may be difficult for data subjects to determine which factors they must challenge to change the ADM,[1846] by obtaining human intervention, expressing their point of view and contest the decision as foreseen in Article 22 (3) GDPR. This leads to a Type 3 legal problem occurring regardless of which AI discipline is used for ADM. The problem is caused by the wording enshrined in Article 15 (1) lit h GDPR, which does not impose an obligation on controllers to provide data subjects with a causal explanation about a specific automated decision. It is therefore a general problem and relates to all AI disciplines as introduced in Chapter 2.

The logic and causal explanation problem (Type 3)

The right to obtain meaningful information about the logic involved in ADM according to Article 15 (1) lit h GDPR does not seem to require controllers to provide causal information about specific ADM, i.e. how input factors affected the final decision. Consequently, data subjects cannot determine which factors they must challenge when contesting ADM according to Article 22 (3) GDPR. Therefore, Article 15 (1) lit h GDPR is not fit for purpose to protect the fundamental right to data protection.

[1840] 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.
[1841] Recital 11 GDPR.
[1842] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[1843] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[1844] Recital 7 GDPR.
[1845] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona para 72.
[1846] Thomas Wischmeyer, 'Artificial Intelligence and Transparency: Opening the Black Box' in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer Nature 2020) 88.

5.7 Rectification

Both the EUCFR and the GDPR provide individuals with a right to have personal data rectified.[1847] Article 16 GDPR is more specific and grants data subjects a right to obtain the rectification of inaccurate personal data with respect to him or her or to have incomplete personal data completed. The right to rectification constitutes a key element of the fundamental right to data protection.[1848] Its significance has been emphasised by both the ECtHR[1849] and CJEU.[1850] It applies to false, inaccurate and incomplete information.[1851] Neither the GDPR itself, nor CJEU case law nor regulatory guidance yield details about the standard of proof applying to the rectification of personal data. It remains unclear which requirements data subjects must meet concerning the accuracy or completeness of the personal data designated to *replace* the personal data currently processed by the controller when they exercise their right to rectification.

A case relating to the request to erasure of inaccurate personal data and the freedom of expression according to Article 17 (3) lit a GDPR provides some insight about the standard of proof to be met in order to establish the inaccuracy of personal data processed. According to the CJEU, the data subject bears the burden of proof to establish the manifest inaccuracy of the information in question.[1852] To avoid an excessive burden, the data subject must provide evidence that can reasonably be required. It must submit '*relevant* and *sufficient* evidence capable of substantiating his or her request and of establishing the *manifest inaccuracy* of the information'.[1853] Apparently, the CJEU did not follow the opinion of AG Pitruzella, who suggested a lower evidence threshold. In his view, the data subject must provide 'prima facie evidence of the false nature of the content'.[1854] However, the context of this case must be taken into account. It relates to the weighing of the fundamental rights to privacy and the protection of personal data on the one hand and the fundamental right to freedom of expression and information on the other. Arguably, the CJEU might establish a lower standard when balancing the rights and freedoms of data subjects against those of controllers. Therefore, I do not give the standard of 'manifest inaccuracy' much weight. Rather, I rely on a PNR opinion issued by the CJEU which suggests that rectification somehow relates to the notion of verification because it used the terms 'verified' and 'unverified' personal data in the opinion.[1855] The CJEU has pointed to the significant 'margin of error' that may result from the automated processing of personal data, in particular

[1847] Article 8 (2) EUCFR and Article 16 GDPR.
[1848] Cécile de Terwangne, Commentary of Article 16 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 473.
[1849] *Leander v Sweden,* App No 9248/81 (ECtHR 26 March 1987) para 48; *Rotaru v Romania,* App No 28341/95 (ECtHR 4 May 2000) para 46.
[1850] Case C-434/16, *Nowak* [2017] ECR I-994 para 49; Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECR I-650 para 95; Case C-553/07 *Rijkeboer* [2009] ECR I-03889 para 51.
[1851] *Cemalettin Canli v Turkey* App No 22427/04 (ECtHR 18 February 2009) para 37 and 42; Case C-131/12 Google Spain [2014] ECR I-317 para 70.
[1852] Case C-460/20, *TU* [2022] ECR I-962 para 68.
[1853] Case C-460/20, *TU* [2022] ECR I-962 paras 68, 72.
[1854] Case C-460/20, *TU* [2022] ECR I-962, Opinion AG Pitruzella para 50.
[1855] Opinion 1/15 CJEU [2017] ECR I-592 paras 131, 169.

if such processing is carried out on the basis of '*unverified* personal data […] and pre-established *models* and criteria'.[1856]

According to the ECtHR, natural persons should adduce 'objectively verifiable evidence' for having personal data relating to them changed.[1857] Case law on the right to rectification in the Netherlands seems to apply a similar standard: inaccuracies in personal data to be rectified must be 'easily' and 'objectively' verifiable.[1858] In Germany, the standard concerning the right to rectification amounts to 'objective reality': correct data reflect reality, and data are incorrect if not corresponding with reality.[1859] Differences in local case law with respect to the standard of proof are caused by the principle of national procedural autonomy. In the absence of EU procedural law, Member States may set up the procedural system as they deem fit.[1860] Thus, the manner of regulating procedural law is generally considered a matter of Member State autonomy, as long as it satisfies the minimum principles of effectiveness and equivalence[1861] (see Section 5.7.1). Unfortunately, there are no standards that define the required degree of accuracy[1862] that could serve as a benchmark when a data subject wishes to rectify personal data (see Section 4.7.2).

Because this thesis relates to EU law, I introduce a distinct 'EU' standard. From ECtHR case law[1863] as well as the CJEU's PNR opinion,[1864] it can be concluded that the right to rectification relies on the notion of verification. Thus, when data subjects dispute the accuracy or completeness of personal data processed by the controller ('current data'), they must provide verifiable evidence that the 'new' personal data envisaged to replace the current data are accurate. I call this 'the objective verifiability standard'. The latter is seemingly met with ease when the personal data in question is verifiable by nature (such as a name, date of birth, email address).[1865] In what follows, I explain that this is not the case regarding personal data processed in the context of AI. Personal data generated by AI is often unverifiable by nature. This applies particularly to inferred personal data (including predictions) produced by means of ML and emotion data generated by AC.

[1856] Opinion 1/15 CJEU [2017] ECR I-592 paras 169, 170 emphasis added.
[1857] *Ciubotaru v Moldov* App No 27138/04 (ECtHR 27 July 2010) para 59.
[1858] Raad van State, ECLI:NL:RVS:2021:1020, 20 February 2019 para 5.1.
[1859] BVerwG – 6 C 7.20 [2022], ECLI:DE:BVerwG:2022:020322U6C7.20, para 32.
[1860] Bart Krans, Anna Nylund, 'Aspects of Procedural Autonomy' in Bart Krans, Anna Nylund (eds) *Procedural Autonomy Across Europe* (Intersentia 2020) 1.
[1861] Anna Wallerman, 'Towards an EU law doctrine on the exercise of discretion in national courts? The Member States' self-imposed limits on national procedural autonomy' (2016) Vol 53 Iss 2 Common Market Law Review 339-360.
[1862] 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 25.
[1863] *Ciubotaru v Moldov* App No 27138/04 (ECtHR 27 July 2010) para 59.
[1864] Opinion 1/15 CJEU [2017] ECR I-592 paras 131, 169.
[1865] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) Vol 2 Columbia Business Law Review 494, 548.

5.7.1 Legal problems: Type 1

When applied to AI-generated personal data, the right to rectification could be violated due to the procedural law applicable in a given Member State ('MS'). More specifically, the right to rectification may be violated when the procedural law and/or judicial practice of a Member State does not meet the minimum principles of equivalence and effectiveness as elaborated by CJEU case law. These principles appear in numerous cases[1866] and are, together with the principle of effective judicial protection, the most widely recognised limits on national procedural autonomy.[1867] The principle of equivalence essentially amounts to the law of remedies concerning the general principle of non-discrimination.[1868] More importantly in the context of this thesis, the minimum principle of *effectiveness* demands that procedural rules applicable in any given MS must not render the exercise of rights conferred to individuals by EU law '*virtually impossible or excessively difficult*'. [1869] In a landmark ruling, the CJEU found that any provision, legislative, administrative or judicial practice that 'might prevent, even temporarily, Community rules from having full force and effect'[1870] is incompatible with the very essence of EU law.[1871]

One case in Germany dealing with the right to rectification further illustrates this problem. The German Federal Administrative Court ruling[1872] mentioned in Section 5.7 arguably violates the right to rectification according to the GDPR because the judicial practice and national procedural law make it *excessively difficult* for data subjects to enforce their right to rectification conferred to them by Article 16 GDPR. In the dispute of this ruling, the Republic of Turkey issued a new passport for the data subject containing a corrected date of birth (01.01.1953 'new date'), following the ruling of a Turkish district court that declared the data subject's date of birth currently registered (01.01.1958 'current date') to be incorrect. Consequently, the data subject requested that the entry of his date of birth contained in the German population register (current date) be changed in accordance with the newly issued Turkish passport containing the new date of birth.[1873]

[1866] Case 33–76, *Rewe-Zentralfinanz eG and Rewe-Zentral AG* [1976] European Court Reports 1976-01989; Joined cases C-430/93 and C-431/93, *Jeroen van Schijndel et al* [1995] ECR I-4705 para 17; Case C-312/93 Peterbroeck [1995] ECR I-437; Case C-126/97, *Eco Swiss China Time Ltd* [1999] ECR I-269; see Bart Krans, Anna Nylund, 'Aspects of Procedural Autonomy' in Bart Krans, Anna Nylund (eds) *Procedural Autonomy Across Europe* (Intersentia 2020) in Footnote 5 at page 3 for more cases.
[1867] Anna Wallerman, 'Towards an EU law doctrine on the exercise of discretion in national courts? The Member States' self-imposed limits on national procedural autonomy' (2016) Vol 53 Iss 2 Common Market Law Review 339, 342.
[1868] Koen Lenaerts, 'National Remedies for Private Parties in the Light of the EU Law Principles of Equivalence and Effectiveness' (2011) Vol 46 Irish Jurist 13, 14.
[1869] Case C-353/20, Skeyes [2022] ECR I-423 para 52; Case C-497/20, *Randstad Italia SpA* [2021] ECR I-1037 para 58, Joined Cases C-222/05 and C-225/05, *Van der Weerd* [2007] ECR I-4233 para 28; *Jeroen van Schijndel et al* [1995] ECR I-4705 para 17.
[1870] Case C-213/89, Factortame [1990] ECR I-527 para 20.
[1871] Bart Krans, Anna Nylund, 'Aspects of Procedural Autonomy' in Bart Krans, Anna Nylund (eds) *Procedural Autonomy Across Europe* (Intersentia 2020) 3.
[1872] BVerwG – 6 C 7.20 [2022], ECLI:DE:BVerwG:2022:020322U6C7.20.
[1873] BVerwG – 6 C 7.20 [2022], ECLI:DE:BVerwG:2022:020322U6C7.20, paras 1-3.

Although the data subject provided the newly issued passport as evidence for the rectification of his personal data, the German Federal Administrative Court concluded that the controller cannot be obliged to change the registered date of birth in the German population register as, in accordance with Germany's code of civil procedure concerning the evidentiary value of public documents,[1874] the 'correctness of the date of birth as "01.01.1953" *[new date]* does not follow from the entry in the plaintiff's Turkish passport'.[1875] The Court referred to the accountability principle according to Article 5 (2) GDPR that puts the burden of proof on the controller to demonstrate compliance with the accuracy principle. Considering this burden of proof, the controller cannot be required to rectify the current date and instead process the new date of birth of which the accuracy cannot be determined, in particular, where the data subject *fails to prove the correctness* of the new date as required by applicable procedural law. According to the Court, the burden of proof regarding the accuracy of the new data lies on the data subject. The data subject's inability to prove the correctness of the new data is at the data subject's expense.[1876] Hence, the data subject cannot exercise the right to rectification according to Article 16 GDPR if it cannot establish the accuracy of personal data designated to replace the current personal data processed by the controller with sufficient certainty.[1877]

In my view, the judicial practice adopted by the German Court, as well as the procedural laws in Germany, render it 'virtually impossible or excessively difficult'[1878] for data subjects to exercise their right to rectification according to EU data protection law. Ultimately, this contradicts the minimum principle of effectiveness and thus, in itself, may violate EU law. In addition, the judicial practice is contrary to the GDPR's objectives to ensure that the level of protection is *equivalent* in all MS,[1879] strengthening data subject rights,[1880] and particularly providing the same level of legally enforceable data subject rights.[1881] Also, in my view, a newly issued passport containing the correct date of birth should be considered to meet the objective verifiability standard as introduced in Section 5.7. Furthermore, the Court's ruling appears to adopt a prevalence for 'current' data processed by the controller, making it excessively difficult, if not impossible, for data subjects to obtain rectification of such personal data and opens the door for controllers to easily reject rectification requests. In addition, it should be kept in mind that this case concerned personal data whose accuracy appears to be easy to verify, as opposed to personal data generated by AI (see Sections 5.7.2 and 5.7.3). When the judicial practice adopted by the German court as well as the German procedural laws are applied to the rectification of unverifiable and highly subjective personal data generated by AI, it will be virtually

[1874] Zivilprozessordnung (ZPO) § 418 Beweiskraft öffentlicher Urkunden mit anderem Inhalt.
[1875] BVerwG – 6 C 7.20 [2022], ECLI:DE:BVerwG:2022:020322U6C7.20, para 7, emphasis added by the author.
[1876] BVerwG – 6 C 7.20 [2022], ECLI:DE:BVerwG:2022:020322U6C7.20, paras 9, 52.
[1877] BVerwG – 6 C 7.20 [2022], ECLI:DE:BVerwG:2022:020322U6C7.20, paras 9, 51.
[1878] Joined Cases C-222/05 and C-225/05, *Van der Weerd* [2007] ECR I-4233 para 28; *Jeroen van Schijndel et al* [1995] ECR I-4705 para 17.
[1879] Recital 10 GDPR.
[1880] Recital 11 GDPR, Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[1881] Recital 13 GDPR.

impossible or excessively difficult for data subjects to rectify inaccurate personal data. This constitutes a Type 1 legal problem.

> ***The procedural autonomy problem (Type 1)***
> *Due to the principle of national procedural autonomy, Member States (MS) may set up their own procedural laws as they deem fit. This may lead to the violation of the right to rectification when the procedural law and/or judicial practice of a MS renders it virtually impossible or excessively difficult for data subjects to exercise their right to rectification according to Article 16 GDPR. This problem applies particularly to the rectification of unverifiable and highly subjective personal data generated by the AI disciplines ML and AC as discussed in Sections 5.7.2 and 5.7.3.*

5.7.2 Legal problems: Type 2

ML as introduced in Section 2.2.1 is particularly eligible to generate inferred data, defined as 'the product of probability-based processes' used to create predictions of behaviour[1882] (see also Sections 4.4.1 and 4.4.3). ML applies data-driven methods, combining fundamental concepts in computer science with approaches from statistics, probability and optimisation[1883] and is used for classification as well as the detection of patterns and predictions. Therefore, ML constitutes a powerful tool of computational methods using experience to make predictions.[1884] Due to its probabilistic approach, ML is closely related to the field of statistics and is particularly helpful to handle ambiguous cases.[1885] Given that predictions produced by ML, such as life expectancy, score value ratings and career perspectives are probabilistic by nature, ML poses the risk that personal data generated by it might be inaccurate, wrong or incomplete. Essentially, ML-based predictions or classifications constitute 'educated guesses or bets, based on large amounts of data'.[1886] ML systems that aim to predict the future behaviour of individuals cannot achieve absolute accuracy due to the predictive nature of the generated output and the lack of a baseline truth for comparison.[1887] Thus, as outlined in Section 4.7.1, ML generates output that constitutes uncertain knowledge because it is probabilistic by nature and not based on human reasoning. Therefore, such an output can be inaccurate.

[1882] 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.
[1883] Mehryar Mohri, Afshin Rostamizadeh, Ameet Talwalkar, *Foundations of Machine Learning* (MIT Press 2012) 1.
[1884] Mehryar Mohri, Afshin Rostamizadeh, Ameet Talwalkar, *Foundations of Machine Learning* (MIT Press 2012) 1.
[1885] Kevin P Murphy, *Machine Learning: A Probabilistic Perspective* (MIT Press 2012) 1, 4.
[1886] 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.
[1887] 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.

With the output generated by ML, it is rather difficult or even impossible to meet the objective verifiability standard. The main reason for this is that the predictions generated by ML relate to *future behaviour* that has not yet happened. Examples of such output generated by ML are predictions about a customer's future life, including estimated advancements in career,[1888] credit risk scores, life expectancy or likelihood of future health outcomes.[1889] An individual's phone-charging habit is currently used as a relevant factor for determining individual creditworthiness. AI, in particular when powered by ML, assesses data points such as phone-charging habits that would commonly not be considered when determining someone's creditworthiness. For example, Smart Finance disclosed that customers who regularly let their phone batteries drop below 12% are not considered good prospects. Another FinTech company called Lenddo considers hyper well-maintained smartphone batteries as a red flag because such a phone-charging habit seems to be robotic or not human enough.[1890] In fact, research suggests that behaviour revealed in mobile phone usage can predict the likelihood of credit repayment. By means of ML, the likelihood of repayment was predicted using behavioural features derived from mobile phone usage.[1891]

Often, predictions or correlations are essentially considered *facts*, although the output generated by ML is probabilistic and can relate to conduct that has not yet happened. Such inferred data can be used by controllers for decision-making with respect to data subjects, whether automated or not. Output generated by ML is not only problematic due to the possible impact they may have for the data subject concerned, but also because such output may be fed back into the AI system and influence future decisions and predictions which could lead to discrimination.[1892] Difficulties concerning the provision of objectively verifiable evidence are particularly problematic when considering the highly subjective nature of predictive inference techniques such as ML:[1893] predictions generated by ML are essentially educated guesses based on large amounts of data.[1894] Inferred data generated by ML may also ascribe attributes to people using ML techniques such as regression, classification (see Section

[1888] 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.
[1889] 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.
[1890] Tanya Goodin, 'The battery life of your phone could affect your loan application' (2022) <https://tanya-goodin.com/2022/08/credit-rating-algorithmic-transparency/> accessed 8 February 2024.
[1891] Daniel Björkegren, Darrell Grissen, 'Behavior Revealed in Mobile Phone Usage Predicts Credit Repayment' (2020) Vol 34 Iss 3 The World Bank Economic Review 618, 623.
[1892] Solon Barocas, Andrew D Selbst 'Big Data's disparate impact' (2016) Vol. 104 California Law Review 671, 681, 726; Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops' in Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press 2018) 113.
[1893] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 302.
[1894] 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.

2.2.1.1) or clustering (Section 2.2.1.2) and thus amount to profiling as defined in Article 4 (4) GDPR (see also Section 4.4.3). Attributes ascribed to data subjects are quite imprecise (e.g., inferred from Facebook likes) and constitute estimates rather than factual information. Therefore, profiles are simply new inferred personal data.[1895]

In terms of accuracy, personal data can be divided into three categories: i) factual data that accurately reflect a known reality about an individual, ii) counter-factual data that inaccurately reflect a known reality about an individual and iii) data that cannot be described as completely falling under the former or the latter.[1896] I call the last category 'unverifiable personal data'. According to CJEU case law, facts are susceptible to proof.[1897] Unverifiable personal data, e.g. inferred personal data such as ML predictions or subjective emotion data are not susceptible to proof because they do not constitute factual nor counter-factual data.

Inferred data, including estimates or predictions generated by AI systems and other output generated by ML, fall into the category of unverifiable personal data. For example, life expectancy and estimated advancements in career may prove to be wrong or true in the future, but in essence they are probabilistic and not verifiable at the time when they are generated. Data subjects cannot meet the objective verifiability standard when they intend to enforce their right to rectify the output generated by ML. This is mainly due to the fact that such data relates to the future, its highly probabilistic nature and the lack of a baseline truth for comparison.[1898] In addition, it is generally impossible for individuals to prove that personal data inferred by means of AI is inaccurate without having access to the tools used to infer the data.[1899] As outlined in Section 5.6, such tools, including specific technological information, are likely to be subject to trade secret protection which hinders individuals from proving the inaccuracy of inferred personal data.[1900]

Therefore, it seems extremely difficult, if not impossible, for data subjects to meet the objective verifiability standard regarding unverifiable data inferred by ML. Possibly, this leads to serious consequences for data subjects as inferred data may propagate existing biased patterns, leading to disparate

[1895] Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops' in Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press 2018) 112.
[1896] 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, 4-5.
[1897] Case C-460/20, *TU* [2022] ECR I-962 para 66.
[1898] 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 17-18; 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.
[1899] Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops' in Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press 2018) 114.
[1900] The situation is even more difficult in the case of emotion data because it is questionable if and how such data in fact can be verified.

impacts.[1901] Additionally, it is highly problematic when unverifiable data are essentially considered as *facts*, although they are not. The personal data generated by ML are probabilistic and relate to future behaviour that has not yet occurred. Actions taken based on probabilistic predictions and correlations may have real impact on human interests[1902] (e.g., to receive a loan or to be employed). Regulatory guidance indicates that data subjects cannot rectify inferred personal data such as a prediction if this *may* be factually correct, even if the prediction *never materialises*. If, according to this guidance, a computer system puts the data subject into the group that 'most likely will develop heart disease', the data subject cannot request the rectification of the inferred personal data because the prediction solely states that the data subject is more likely to develop heart disease. This might be factually correct as a matter of statistics, even if the data subject will never suffer from heart disease.[1903] Because output generated by ML, including inferred data, represents unverifiable personal data, data subjects cannot meet the objective verifiability standard when they enforce their right to rectification. This constitutes a Type 2 legal problem.

The unverifiable data problem (Type 2)

ML generates probabilistic output concerning a data subject's future life such as credit risk and life expectancy scores, or future health, constituting uncertain knowledge. Due to the lack of truth serving as a verification mechanism and the lack of access to the tools used to generate them, this output represents unverifiable personal data. Consequently, data subjects cannot meet the objective verifiability standard when enforcing their right to rectification.

The difficulty to meet the objective verifiability standard applicable the right of rectification also occurs regarding emotion data generated by the AI discipline AC. To illustrate this problem in more detail, I take the example of emotion data inferred by an AI system that relies on the AI discipline AC combined with other AI disciplines (e.g., CV for facial movements or NLP). Emotion data are subjective by nature and, therefore, are not objectively verifiable.

Naturally, emotion data can only be a known reality for the natural person that has these emotions (and not for other parties or entities) because every individual has its own personal experience of emotion.[1904] Thus, emotion data are not objectively verifiable due to the subjective perception of emotion. Rather, it is subjectively verifiable: Emotion data can uniquely be verified by the individual

[1901] Bart Custers, 'Profiling as inferred data. Amplifier effects and positive feedback loops' in Emre Bayamlıoğlu, Irina Baraluic, Liisa Janssens and Mireille Hildebrandt (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press 2018) 115.
[1902] 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.
[1903] 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.
[1904] Jennifer Healey, 'Physiological Sensing of Emotion' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 213, 214.

experiencing the emotional state in question. Emotion data derived from AC-powered applications represent unproven and factually uncertain information about the emotional states of individuals. As described in Section 4.7.1, it is likely that emotion data detected by AC systems is inaccurate. For example, imagine that an AC-powered automated video assessment wrongfully detects that the job applicant was angry while performing the automated video assessment. Because the data subject in fact was surprised by an unexpected question posed during the automated video assessment, he seeks the rectification of the inaccurate emotional state of anger to be replaced by the emotional state 'surprise'. Because emotion data are subjective by nature, it is impossible for the data subject to meet the objective verifiability standard. Emotional states cannot be verified objectively because they are by definition subjective as every individual has its own, personal, experience of emotion.[1905] Because emotion data are subjective by nature, data subjects cannot meet the objective verifiability standard when enforcing their right to rectification to correct inaccurate emotion data. This leads to a Type 2 legal problem.

The subjectivity problem (Type 2)

Scientific research suggests that AC powered systems are likely to generate inaccurate emotional data. Emotional data are highly subjective because every individual has its own personal experience of emotion. Due to this inherently subjective nature, data subjects cannot meet the objective verifiability standard when they seek the rectification of inaccurate emotional data.

The right to rectification enshrined in Article 16 GDPR also allows data subjects to provide a 'supplementary statement'. This amounts to adding missing elements rather than rectifying inaccurate personal data.[1906] It seems unclear what specific obligations such a supplementary statement imposes on the controller.[1907] Regulatory guidance simply states that Article 16 GDPR contains a right for the data subject to complement the personal data with additional information.[1908] Thus, the right to have incomplete personal data completed may not be particularly helpful in the context of AI because it does not solve the problem of inaccurate data. Even if the data subject could prove that personal data generated by AI is inaccurate, similar issues arise in the context of the right to erasure (Section 5.8.1). Such issues concern the practical consequences for controllers, e.g. whether and how they should rectify the personal data contained in the ML model, for example, by means of machine unlearning.

[1905] Jennifer Healey, 'Physiological Sensing of Emotion' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 213, 214.
[1906] Cécile de Terwangne, Commentary of Article 16 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 473.
[1907] 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.
[1908] 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.

5.7.3 Legal problems: Type 3

Two views have been presented that significantly restrict the scope of the right to rectification in Article 16 GDPR. First, it has been argued that inferred data 'cannot be rectified under data protection law and can only be contested if there is a procedure in place to contest the evaluation'.[1909] According to this view, the right to rectification is limited to assess the accuracy and completeness of the input data, but excludes the output data generated by means of AI, including opinions.[1910] Second, AG Sharpston takes the view that 'only information relating to *facts* about an individual can be personal data'.[1911] Consequently, only factual personal data can be rectified under the right to rectification. In the Netherlands, there is established case law restricting the right to rectification to *factual* personal data.[1912] Accordingly, the right to rectification is in principle not applicable to impressions, assessments and conclusions relating to the data subject.[1913] If only factual personal data fall under the scope of this right, inferred data cannot be rectified because such data represent unproven and factually uncertain knowledge relating to the future, rather than facts. The view that only *input data* and *factual* personal data fall within the scope of Article 16 GDPR unduly limits the right to rectification. When applied to personal data inferred by AI-powered systems such as ML predictions or emotional states inferred by AC approaches, such personal data cannot be rectified at all. However, this narrow interpretation of the right to rectification not only contradicts regulatory guidance[1914] but also the CJEU's teleological approach to interpret data subject rights.[1915]

In my view, the problem is not the scope of Article 16 GDPR, but the objective verifiability standard. According to CJEU case law, facts are susceptible to proof.[1916] Since unverifiable data are neither factual nor counter-factual data, it is extremely difficult if not impossible to provide evidence that they are inaccurate. As outlined in the unverifiable data and subjectivity problems discussed in Section 5.7.2, data subjects cannot rectify unverifiable and subjective personal data generated by AI when the objective verifiability standard is applied. Regarding both unverifiable and subjective personal data, the question arises of what information the data subject can adduce in order to meet the objective verifiability standard.

[1909] 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 1, 550-551; see also 549, 590.
[1910] 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 1, 550-590.
[1911] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081, Opinion of AG Sharpston para 56.
[1912] Raad van State, ECLI:NL:RVS:2011:BR6338, 31 August 2011 para 2.3; Raad van State, ECLI:NL:RVS:2019:520, 20 February 2019 para 7.2; Rechtbank Den Haag, ECLI:NL:RBDHA:2022:2432, 25 February 2022 para 7.3.
[1913] Raad van State, ECLI:NL:RVS:2019:520, 20 February 2019 para 7.2; Rechtbank Den Haag, ECLI:NL:RBDHA:2022:2432, 25 February 2022 para 7.3.
[1914] 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 and 17-18.
[1915] Case C-434/16, *Nowak* [2017] ECR I-994 para 53.
[1916] Case C-460/20, *TU* [2022] ECR I-962 para 66.

In terms of subjective emotion data, I refer to the example mentioned in Section 5.7.2. An automated video assessment powered by AC wrongfully detects that the applicant was angry while conducting the assessment, although the job applicant was surprised. The data subject can put forward a simple statement indicating he has experienced another emotional state, It is difficult to imagine objectively verifiable evidence for this, however. Ultimately, only the data subject can determine the accuracy of a detected emotional state because emotion data are inherently subjective as every individual has his or her own, personal, experience of emotion.[1917] Emotions can only be a known reality for the natural person that has these emotions and not for other parties or entities. There is simply no such thing as objectively verifiable evidence that a data subject may adduce to rectify inaccurate emotion data. Consequently, the data subject cannot request the controller to replace the emotional state detected by the AI system (sadness) with the correct emotional state (surprise).

In case of inferred personal data generated by ML, the data subject cannot request the rectification of the inferred personal data because there are *no facts* available to prove inaccuracy. The prediction simply states that the data subject is more likely to develop heart disease, which might be correct as a matter of statistics, even if the data subject in fact will never suffer from heart disease.[1918] As pointed out in the unverifiable data problem in Section 5.7.2, ML can generate probabilistic output with respect to the data subject's future life. Examples are estimated career advancements, credit risk scores, life expectancy scores or the likelihood of future health outcomes, constituting uncertain knowledge. This output represents unverifiable personal data because it relates to future behaviour that has not (yet) happened and cannot be considered as facts, even if such output is based on mathematical calculations.[1919] It is unverifiable because it is probabilistic. There is a lack of truth serving as a verification mechanism, and data subjects cannot access the tools used to generate the output. Consequently, a data subject is unable to meet the objective verifiability standard and provide the corresponding factual evidence outlining that a prediction is wrong. This is problematic when considering that inferred personal data might have adverse consequences for the data subject, in particular when considered and treated as facts, despite their probabilistic nature. This occurs, for example, when a data subject seeks to obtain health care insurance or a loan. Likewise, inaccurate emotion data can have adverse consequences for data subjects when used by controllers, for example, in an employment context or when such data are used to influence or manipulate the data subject (see Section 4.3.3).

Due to the objective verifiability standard, data subjects cannot enforce their right to rectification regarding personal data generated by AI. Such data are unverifiable and/or subjective, and factual data eligible to prove inaccuracy are absent. Therefore, the right to rectification is not fit for purpose

[1917] Jennifer Healey, 'Physiological Sensing of Emotion' in Rafael Calvo et al (eds), *The Oxford Handbook of Affective Computing* (OUP 2015) 213, 214.
[1918] 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.
[1919] A chance of something based on e.g. mathematical/statistical calculations can also be considered factual data.

to achieve the GDPR's legislative aim to strengthen the rights of data subjects.[1920] As noted by the CJEU, effective protection of personal data requires the strengthening of the rights of data subjects, which is emphasised by Recital 11 GDPR.[1921] A right that cannot be enforced with regard to unverifiable and subjective personal data generated by AI systems is not suitable to strengthen the rights of data subjects. Furthermore, the objective verifiability standard hampers the GDPR's aim to improve the legal and practical protection of data subjects (Recital 7). It remains unclear how data subjects can enforce their right to rectification regarding unverifiable or highly subjective personal data generated by AI systems.

According to the CJEU, it is important that the data subject rights granted by the GDPR are effective.[1922] However, this is not the case with the right to rectification. Data subjects can hardly enforce this right regarding unverifiable or highly subjective personal data generated by AI due to the objective verifiability standard. Article 16 GDPR does not achieve the GDPR's goal that 'natural persons should have control of their own personal data',[1923] although this was one of the main reasons for the data protection reform.[1924] As outlined in Section 4.4.3, one of the main mechanisms for data subjects to exercise control over the processing of their personal data under the GDPR are data subject rights. Control in the sense of the GDPR is rather limited from a conceptual point of view. In his opinion concerning a preliminary ruling, AG Campos Sánchez-Bordona acknowledged that 'the scope for individual action is limited' and 'confined to the exercise of those rights in specified circumstances'.[1925] The objective verifiability standard further restricts the mechanism for data subjects to exercise control because data subjects cannot rectify arguably inaccurate personal data generated by means of AI. This leads to a Type 3 legal 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.

[1920] Recital 11 GDPR.
[1921] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[1922] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[1923] Recital 7 GDPR.
[1924] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona paras 69, 70.
[1925] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona para 72.

5.8 Erasure

The right to erasure of personal data, as currently understood by courts and regulators, relies on conceptions of how human memories work and how they 'forget'. However, the seemingly easy request to erase or 'forget' personal data poses various practical problems in the context of AI, arguably on the edge of impossibility.[1926]

5.8.1 Legal problems: Type 1

ML models are trained with historical personal data to make predictions and inferences about the future.[1927] Data deletion[1928] in the context of AI is very complex, and machines could be considered as unable to 'forget' because they must be able to go back to an older state of the system in order to be compliant with technical requirements, for example compliance with provisions with respect to databases.[1929] ML models can remember data they have been trained on or - in some cases - simply store it as part of the models.[1930] ANNs unintendedly memorise training data, which is convincingly demonstrated in experiments conducted by researchers at the Berkeley Artificial Intelligence Research Centre.[1931] With a generative text model trained on a data set including one piece of personal data in the form of a credit card number, it is possible to extract the latter from the model itself completely. Thus, where predictive ML models are trained with personal data of users, the models can unexpectedly disclose such personal data, in the case of an ANN in particular. The ANN quickly memorises data contained in the training set, even when these values are rare and the models do not overfit in the traditional sense[1932] (see also Section 4.7.1).

Personal data used as training data for an ML system might, in some cases, be reconstructed from an ML model, for example, by means of model inversion. This permits the training data to be estimated. Membership-inference recovers information to figure out whether or not a particular data subject was

[1926] Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) Vol 34 Iss 2 Computer Law & Security Review 304, 305, 313.
[1927] Asia Biega, Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' (2021) Technology and Regulation 44, 60 <https://arxiv.org/abs/2101.06203> accessed 8 February 2024.
[1928] I use the term 'deletion' as a synonym for erasure.
[1929] Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) Vol 34 Iss 2 Computer Law & Security Review 304, 305, 313.
[1930] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 295-296; Michael Veale et al, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) A 376 Philosophical Transactions of the Royal Society A 376.
[1931] Nicholas Carlin, 'Evaluating and Testing Unintended Memorization in Neural Networks' (*Berkeley Artificial Intelligence Research Blog*, 13 August 2019) < https://bair.berkeley.edu/blog/2019/08/13/memorization/ > accessed 8 February 2024
[1932] Nicholas Carlini et al, 'The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks' (USENIX Security Symposium, Santa Clara, August 2019) <https://arxiv.org/abs/1802.08232> accessed 8 February 2024; Nicholas Carlin, 'Evaluating and Testing Unintended Memorization in Neural Networks' (*Berkeley Artificial Intelligence Research Blog*, 13 August 2019) < https://bair.berkeley.edu/blog/2019/08/13/memorization/ > accessed 8 February 2024.

in the training set.[1933] Making ML systems forget is a difficult challenge.[1934] It is not even straightforward to detect that a training algorithm attempts to memorise personal data within the ML model although there are several techniques and places for encoding such information.[1935] Having ML models forget necessitates knowledge of exactly how individual training points contributed to model parameter updates. This is possible when the algorithm queries the data in a previously defined order. However, when the data are queried adaptively, the divergence induced is bounded only for relatively simple models, which require a small number of iterations for learning. However, efficient approaches for complex models such as ANNs introduced in Section 2.2.1.4 do not yet exist.[1936] If individuals request the deletion of their personal data initially used as training data for the ML model, there are basically two ways for the erasure of personal data *and* what the ML model has learnt from it. These are re-training or amending the ML model by means of machine *un*learning.[1937]

For most of the standard ML models, the only way to completely remove an individual's personal data is to retrain the whole model from scratch on the remaining data.[1938] From a computational perspective, re-training the affected ML models is inefficient and typically also requires one to re-access the original training data and redeploy the retrained model. [1939] Such re-training is considered to constitute a naïve way to have ML models provably forget due to the large computational and time overhead associated with it.[1940] It leads to significant efforts in terms of costs, time, labour and energy consumption and is therefore a rather burdensome task for the controller.[1941] Re-training is computationally often not practical because large-scale algorithms can take weeks to train and learning algorithms known to support fast data deletion operations are scarce.[1942] Ultimately, requiring a controller to retrain a prediction model could create a vicious circle, in particular when many data subjects want

[1933] Michael Veale et al, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) A 376 Philosophical Transactions of the Royal Society A 376, 2 and 4.
[1934] Yinzhi Cao, Junfeng Yang, 'Towards Makign Systems Forget with Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2015) 464 <https://www.ieee-security.org/TC/SP2015/papers-archived/6949a463.pdf> accessed 8 February 2024.
[1935] Congzheng Song, Thomas Ristenpart, Vitaly Shmatikov, 'Machine Learning Models that Remember Too Much' (2017) in Bhavani Thuraisingham et al (eds) Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017 Dallas US, 587, 598.
[1936] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 1 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.
[1937] Michael Veale et al, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) A 376 Philosophical Transactions of the Royal Society A 376, 9.
[1938] Antonio Ginart et al, 'Making AI Forget You: Data Deletion in Machine Learning', Advances in Neural Information Processing Systems (2019) 1 <https://proceedings.neurips.cc/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf > accessed 8 February 2024.
[1939] Sebastian Schelter, 'Amnesia – A Selection of Machine Learning Models That Can Forget User Data Very Fast' (Conference on Innovative Data Systems, Amsterdam, January 2020) <http://cidrdb.org/cidr2020/papers/p32-schelter-cidr20.pdf> accessed 8 February 2024.
[1940] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 1 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.
[1941] Michael Veale et al, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) A 376 Philosophical Transactions of the Royal Society A 376, 9.
[1942] Antonio Ginart et al, 'Making AI Forget You: Data Deletion in Machine Learning', Advances in Neural Information Processing Systems (2019) 2 <https://proceedings.neurips.cc/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf> accessed 8 February 2024.

to erase their personal data. It would lead to less training data and consequently lower accuracy[1943] which ultimately negatively affects the accuracy principle as outlined in Section 3.3.3.6.

The second approach, 'machine unlearning', might be described as the process to revert the effects of the training data on the extracted features and models.[1944] Because ML models might memorise personal data used for training (training data), these models must unlearn what they have learnt from data that must be deleted. Machine unlearning assures that the ML model is no longer trained using the personal data to be deleted.[1945] It has been argued that machine unlearning is rarely possible in modern systems and that methods currently available cannot be retrofitted onto existing systems.[1946] Any ML model trained with personal data may have memorised it and having ML models unlearn is notoriously difficult. First, there is a rather limited understanding of how each data point impacts the ML model because work that measures the influence of a particular training point on the parameters of a model is scarce if not to say non-existent.[1947] This argument particularly applies to complex models based on DL and ANNs and the problems described in Section 2.2.1.4, as it seems impossible to understand what happened in the intermediate (hidden) layers of the ANN.[1948] The second reason is stochasticity. This refers to the lack of any predictable order or plan in the training methods for complicated models such as DL and ANNs. Third, training is an incremental process in which any given update reflects all updates that have occurred previously. For example, if a model is updated based on a particular training data point at a particular time, all subsequent model updates will depend implicitly on this training point.[1949] Approaches for quick 'machine unlearning' are relatively unexplored and not ready for deployment.[1950] Thus machine unlearning seems not to be readily available due to technological difficulties. It is, however, subject to ongoing research.[1951]

There seems to be a disconnect between the right to erasure and the technical reality[1952] in the context of AI and particularly ML. Approaches to remove personal data from ML models do not seem to be

[1943] The more data are fed into the algorithm, the better the performance of the algorithm, namely the accuracy rate of the prediction model.
[1944] Yinzhi Cao, Junfeng Yang, 'Towards Making Systems Forget with Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2015) 464 <https://www.ieee-security.org/TC/SP2015/papers-archived/6949a463.pdf> accessed 8 February 2024.
[1945] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 1 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.
[1946] Michael Veale et al, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) A 376 Philosophical Transactions of the Royal Society A 376, 9.
[1947] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 1 and 3 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.
[1948] Ethem Alpaydin, *Machine Learning: The New AI* (3rd edn MIT Press 2016) 155.
[1949] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 3 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.
[1950] Michael Veale et al, 'Algorithms that Remember: Model Inversion Attacks and Data Protection Law' (2018) A 376 Philosophical Transactions of the Royal Society A 376, 9.
[1951] For an overview see Asia Biega, Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' (2021) Technology and Regulation 44, 60 <https://arxiv.org/abs/2101.06203> accessed 8 February 2024.
[1952] Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li 'Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) Vol 34 Iss 2 Computer Law & Security Review 304, 305, 313.

technically or economically feasible at present. Challenges concerning the reliable deletion of personal data are not constrained to ML models, but extend to the entire data management lifecycle, including data replication when run in cloud environments.[1953] From a computational perspective, re-training seems to be impractical due to the significant effort needed in terms of time, labour and energy consumption. Also, amending ML models after training seems to be technically unfeasible because research is still ongoing in this area, and the scarce approaches are arguably not yet ready for deployment. Ultimately, this violates the right to erasure and leads to a Type 1 legal problem.

The training data problem (Type 1)

When data subjects submit requests to delete their personal data used for the purpose of training ML models, it will in most cases technically not be feasible for the controller to delete such personal data, re-train or unlearn the ML model in question or alternatively anonymise the personal data. The right to erasure enshrined in Article 17 GDPR will then be violated.

At first sight, this problem might be solved by rendering the personal data to be erased anonymous. Recital 26 GDPR describes anonymous data as 'information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. In the view of the CJEU, anonymisation hinges on whether identification is 'practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant'.[1954] Recital 26 outlines what must be considered to determine whether means are 'reasonably likely' to be used for identification: all objective factors, such as costs, the amount of time required for identification, available technology at the time of the processing and technological developments.[1955] In particular, technological developments and related research indicate that there is no solid technical basis for assuming de-identification that will be effective in the long run.[1956] Perfect anonymisation is often unfeasible if not impossible[1957] and computer scientists already warned more than a decade ago that de-identification of personal data constitutes an 'unattainable goal'.[1958] In light of the technological developments, many data formats simply cannot be anonymised, which particularly

[1953] Sebastian Schelter, 'Amnesia – A Selection of Machine Learning Models That Can Forget User Data Very Fast' (Conference on Innovative Data Systems, Amsterdam, January 2020) 9 <http://cidrdb.org/cidr2020/papers/p32-schelter-cidr20.pdf> accessed 8 February 2024.
[1954] Case C-582/14 *Breyer* [2016] ECR I-779 para 46.
[1955] See also Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (10 April 2014).
[1956] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 294; Arvind Narayanan et al, 'A Precatuionary Approach to Big Data Privacy' in Serge Gutwirth et al (eds) *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer Netherlands 2014); Solon Barocas, Helen Nissenbaum, 'Big Data's End Run around Anonimity and Consent' in *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014).
[1957] Michèle Finck, Frank Pallas 'They who must not be identified- distinguishing personal from non-personal data under the GDPR' (2020) Vol 10 No 1 International Data Privacy Law 12.
[1958] Arvind Narayanan and Vitaly Shmatikov, 'Myths and Fallacies of Personally Identifiable Information' (2010) 53 Communications of the ACM 24, 26.

holds true in the case of ML models. These can remember data on which they have been trained or in some cases simply store it as part of their models.[1959]

5.8.2 Legal problems: Type 2

The training data problem outlined in Section 5.8.1 automatically leads to a Type 2 legal problem. If controllers cannot erase personal data used to train ML models, the right to erasure cannot be enforced. This constitutes a Type 2 legal problem.

Article 17 (1) lit d GDPR allows data subjects to request the erasure of their personal data if these have been unlawfully processed. This provision constitutes a general clause for data subjects to request the erasure of their personal data if the processing thereof does not comply with the GDPR in a broad sense.[1960] Based on Article 17 (1) lit d GDPR, data subjects may obtain the erasure of inaccurate personal data. According to the CJEU, the accuracy of personal data constitutes one of the 'conditions of lawfulness'.[1961] Also, Recital 65 GDPR supports this interpretation by stating that 'the data subject has the right to have his or her personal data erased […] where the processing of his or her data does not *otherwise comply* with this Regulation'.

Article 17 (1) lid d GDPR is closely intertwined with the right of access according to Article 15 GDPR, which enables the data subject to verify the lawfulness[1962] and allows one to obtain the rectification, erasure or blocking of its personal data by the controller.[1963] In Section 5.6, I have outlined that input data as well as output data produced by AI, including personal data generated by it, is likely to fall under trade secrets protection and that controllers can therefore restrict access to such personal data. This has a knock-on effect on the entire data protection law regime[1964] and particularly regarding the enforcement of data subject rights such as the right to erasure. The CJEU repeatedly stressed the importance of the right of access as a prerequisite to other data protection rights.[1965] Limitations on the right of access have significant consequences for the right to erasure, because it will be hardly possible for data subjects concerned to assess compliance with the GDPR and subsequently request the erasure of personal data in case of detected non-compliance. Non-compliance is likely to occur as indicated by the various Type 1 legal problems discussed in Chapter 4. For example, the principle of

[1959] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 295-296.
[1960] Herke Kranenborg, Commentary of Article 17 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 481.
[1961] Case C-136/17, *GC and Others* [2019] ECR I-773 para 64; see also Case C-460/20, *TU* [2022] ECR I-962 Opinion AG Pitruzella para 32.
[1962] Recital 63 GDPR.
[1963] Joined Cases C-141/12 & C-372/12, *YS, M* [2014] ECR I-2081 para 44.
[1964] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 285.
[1965] 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.

fairness (Section 4.3.1) and accuracy (Section 4.7.1) is likely to be violated by the AI disciplines ML and AC. Consequently, data subjects cannot enforce their right to erasure and request the controller to delete their personal data unlawfully processed by means of AI systems. This constitutes a Type 2 legal problem.

The erasure problem (Type 2)

Access requests to personal data generated and otherwise processed by means of AI can be denied due to trade secret protection. This has a knock-on effect for the right to erasure, because data subjects cannot verify the lawfulness of such processing. As indicated by the various Type 1 legal problems identified in Chapter 1, non-compliance is likely to occur when personal data are processed by AI systems. Consequently, data subjects cannot request the erasure of personal data unlawfully processed as enshrined in Article 17 (1) lit d GDPR.

5.8.3 Legal problems: Type 3

No Type 3 legal problems arise when the right to erasure is applied to the AI disciplines introduced in Chapter 2. This is mainly due to the broad wording contained in Article 17 (1) lit d GDPR,[1966] which allows data subjects to request the erasure of personal data that 'have been unlawfully processed'. Data subjects may enforce their right to erasure according to Article 17 (1) lit d GDPR regarding all Type 1 legal problems identified in this thesis, provided that the violation in question concerns the GDPR and no exception enshrined in Article 17 (3) GDPR applies. However, there is one important caveat. As mentioned in Section 5.7, the data subject bears the burden of proof to establish the manifest inaccuracy of the information in question. The CJEU seems to place the emphasis on *factual* evidence. The CJEU ruled that facts, in particular, are susceptible to provable evidence. [1967] In Section 5.7.2, I have outlined that it is extremely difficult, not to say impossible, for data subjects to provide factual evidence for unverifiable personal data generated by means of AI (e.g. predictions or emotion data).

5.9 Portability

The right to data portability enshrined in Article 20 GDPR enables data subjects to transfer personal data among controllers[1968] and to the data subject's own systems. Recital 68 GDPR emphasises its strong connection with the legislative objective to strengthen the data subjects' control over their own personal data.[1969] As outlined in Section 4.4.3, the main mechanism for data subjects to exercise control over the processing of their personal data under the GDPR are data subject rights. The right to

[1966] Herke Kranenborg, Commentary of Article 17 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 481.
[1967] Case C-460/20, *TU* [2022] ECR I-962 para 66.
[1968] Inge Graef, Martin Husovec, Nadezhda Purtova 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) Vol 19 Iss 6 German Law Journal 1359, 1364.
[1969] Recitals 7 and 68 GDPR.

data portability empowers data subjects to exercise control as it facilitates to move, copy or transmit personal data easily from one IT environment to another, regardless of whether this refers to the data subject's own systems or the systems of others (e.g., other controllers).[1970] The wording of Article 20 (1) GDPR indicates that the right is twofold meaning that the data subject has the right to receive the personal data '*and*' the right to transmit those to another controller. Article 20 (2) GDPR states that the data subject may request the controller to transfer the personal data *directly* to another controller, which would be obsolete if Article 20 (1) GDPR would mean to exclude the possibility to have the data transferred to the data subject's own system.

5.9.1 Legal problems: Type 1

No Type 1 legal problems arise when the right to data portability is applied to the AI disciplines introduced in Chapter 2. As will be outlined in Sections 5.9.2 and 5.9.3, the right to data portability is particularly problematic with regard to its enforcement and scope.

5.9.2 Legal problems: Type 2

As outlined in the copy problem discussed in Section 5.6, trade secret protection under the TSD covers AI itself as well as output generated by the AI system, including emotional states and life expectancy predictions. Like the right of access (Section 5.6.2), the right to data portability contains a provision that enables the controller to restrict the right to data portability on a case-by-case basis. Article 20 (4) GDPR states that the right to data portability 'shall not adversely affect the rights and freedoms of others'. This gives controllers more leeway and flexibility in restricting data portability requests by means of Article 20 (4) GDPR, because these restrictions do not have to be enshrined in EU or MS law.[1971] Therefore, controllers could argue that the transmission of personal data constituting the output of AI systems from one IT environment to another (thus to the data subject or another controller) infringes their trade secrets and refuse to transmit such data. Consequently, data subjects cannot enforce their right to data portability, which constitutes a Type 2 legal problem. Because the broad scope of protection under the TSD applies to *all AI* disciplines as introduced in Chapter 2, this Type 3 legal problem constitutes a general problem and relates to all AI disciplines discussed in Chapter 2.

The transmission problem (Type 2)

Due to the broad scope of trade secrets protection in the EU, controllers are likely to argue that the transmission of personal data constituting outputs generated by AI systems from one IT system to another infringes their trade secrets. Consequently, data subjects cannot enforce their right to data portability.

[1970] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 4.
[1971] As it is the case of restrictions made on the basis of Article 23 GDPR.

5.9.3 Legal problems: Type 3

The text of Article 20 (1) GDPR limits the scope of the right to data portability in two ways. First, the right applies only to processing of personal data based on the lawful bases of consent or performance of a contract and therefore not to processing which is based on a controller's legitimate interest.[1972] Second, the scope of the right is limited to personal data that are 'provided by' the data subject[1973] which only refers to personal data actively and knowingly disclosed by the data subject. Examples mentioned in regulatory guidance include the email address or user name submitted via online forms, the photos and videos uploaded on social media and personal data *observed* by the controller. The latter, according to the regulator, includes raw personal data observed in the context of the use of the service or device, for example, search history, traffic data, location data and heartbeat, all tracked by a wearable device.[1974] According to both regulatory guidance and the European Commission, [1975] observed data constitutes 'raw data' and *excludes* personal data generated by the controller.[1976] Regulatory guidance specifically mentions that data generated by the controller, such as a user profile created by analysis of raw data collected by the controller, does *not* fall under the notion of personal data 'provided by the data subject'. Thus, regulatory guidance explicitly excludes *inferred* and *derived* personal data from the scope of the right to data portability.[1977] As I outline in the following paragraphs, this limitation is significant regarding processing of personal data in the context of AI.

Regulatory guidance does not further explain the two terms 'inferred' and 'derived' personal data but indicates that this may include 'algorithmic results'.[1978] It seems that the regulatory guidance relies on a paper published by the OECD which introduces a data taxonomy distinguishing between four categories: provided, observed, derived and inferred data.[1979] Derived data are described as 'data generated from other data, after which they become new data elements related to a particular individual' created by simple reasoning and basic mathematics to detect patterns and create classifications (e.g. detection of common attributes among profitable customers used for classification). Inferred data are defined as 'the product of probability-based processes' and used, for instance, to create predictions of behaviour deployed to categorise individuals.[1980] Unlike derived data, inferred data are based on probabilistic reasoning and may include 'statistical data' (e.g., credit risk scores, life expectancy scores) and

[1972] Art. 6 (1) lif f GDPR.
[1973] Art. 20 (1) GDPR, Recital 68.
[1974] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 10.
[1975] See letter from Member of the European Commission Věra Jourová to Chairman of WP29 (2017) < https://zwenneblog.weblog.leidenuniv.nl/files/2018/06/Letter-Cssr-Jourova-to-Falque-Pierrotin.pdf > accessed 8 February 2024.
[1976] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 10.
[1977] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 10.
[1978] Ibid.
[1979] OECD Working Party on Security and Privacy in the Digital Economy JT03357584 (2014) 5 <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en> accessed 8 February 2024.
[1980] Ibid.

'advanced analytical data' (e.g., likelihood of future health outcomes based on analysis of extensive medical data sets).[1981]

Considering the AI discipline ML as introduced in Section 2.2.1, I take the view that ML-generated data most likely constitutes both derived and/or inferred personal data. ML applies data-driven methods, combining fundamental concepts in computer science with approaches from statistics, probability and optimisation[1982] and is used for classification and the detection of patterns and predictions. Unsupervised ML detects patterns by means of clustering and dimensionality reduction techniques. Supervised ML uses classification and regression techniques. Recommendations or predictions generated by ML, for example, personalised suggestions for Netflix users[1983] or predictions concerning one's sexual orientation[1984] either constitute derived or inferred personal data. Additionally, the AI discipline CV applies basic mathematics and might produce derived data. In particular, face recognition systems rely on the mathematical concept convolution, which is considered a specialised kind of linear operation (see Section 2.2.3.2). Models combining CV and ML disciplines and applying convolutional ANNs and regression techniques were able to predict sexual orientation from dating profile photographs.[1985] In addition, personal data generated by systems relying on any other discipline of AI combined with ML approaches might constitute derived or inferred personal data that falls outside the scope of application of the right to data portability.

Consider, for example, emotion data generated by an AI system using AC and ML. Regulatory guidance states that data generated by the controller's algorithms, including derived or inferred profiles and the outcome of an assessment, personalisation or recommendation process, are excluded from the scope of the right to data portability. According to the regulator, this limitation also applies to inferred or derived personal data which relate to special categories of personal data, for example data concerning health.[1986] Thus, personal data derived and inferred by means of the AI disciplines CV, AC, ML and potentially any other AI discipline combined with ML does not fall within the scope of the right enshrined in Article 20 GDPR.[1987] This also holds true if the personal data generated by the controller with the help of AI constitutes special data according to Article 9 (1) GDPR.

[1981] OECD Working Party on Security and Privacy in the Digital Economy JT03357584 (2014) 5 <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage=en> accessed 8 February 2024.
[1982] Mehryar Mohri, Afshin Rostamizadeh, Ameet Talwalkar, *Foundations of Machine Learning* (MIT Press 2012) 1.
[1983] See <https://research.netflix.com/research-area/recommendations> accessed 8 February 2024.
[1984] John Leuner, 'A Replication Study: Machine Learning Models Are Capable of Predicting Sexual Orientation From Facial Images' (2018) <https://arxiv.org/pdf/1902.10739.pdf> accessed 8 February 2024.
[1985] Ibid 52.
[1986] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 10, 11.
[1987] 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, 519.

Arguably, the right to data portability was drafted without considering AI systems that can generate derived or inferred personal data. Consequently, individuals have limited control over their personal data, which is contrary to the legislative aim of the right, as emphasised in Recital 68 GDPR. This recital stresses the strong connection of the right to portability of data with the legislative objective of strengthening the control of data subjects over their own personal data as propagated in Recital 7 GDPR. The right to data portability intends to empower data subjects by facilitating them to move, copy or transmit personal data easily from one IT environment to another, including their own systems.[1988] Because personal data generated by AI systems, including inferred or derived special personal data such as predictions concerning sexual orientation and mental health, do not fall under the scope of the right to data portability, individuals have no control with regard to such data. This particularly holds true when considering that data subjects even cannot obtain access to such data by means of Article 15 GDPR due to the trade secrets problem discussed in Section 5.6.2. In other words, the right of access cannot close this gap, although it is precisely the right of access that is supposed to do so. It is acknowledged that the scope of the right to data portability is intentionally limited when compared to Article 15 GDPR, as indicated by the European Commission.[1989]

The limited scope of the right to portability about personal data inferred and/or derived by the controller ultimately leads to a Type 3 legal problem. This right is not fit for purpose to achieve the GDPR's goal that 'natural persons should have control of their own personal data'.[1990] It was one of the main reasons for the data protection reform[1991] and was *specifically intended* to 'further strengthen the control over his or her own data'.[1992] As outlined in Section 4.4.3, one of the main mechanisms for data subjects to exercise control over the processing of their personal data under the GDPR are data subject rights. Due to the limited scope with regard to inferred and / or derived personal data, the right to data portability does not achieve the goal of strengthening the control of the data subject over the processing of personal data. Likewise, Article 20 GDPR fails to strengthen the rights of data subjects as envisaged by the GDPR.[1993] As noted by the CJEU, effective protection of personal data requires the strengthening of the rights of data subjects, which is emphasised by Recital 11 GDPR.[1994] A right of which the scope excludes personal data inferred and/or derived by the controller fails to strengthen the data subject's rights, in particular when considering that the right to obtain a copy of the personal data undergoing processing allows for restrictions due to trade secret protection. The CJEU has stressed the importance of ensuring that data subject rights granted by the GDPR are

[1988] Article 29 Working Party, 'Guidelines on the right to data portability' (WP 242rev.01, 5 April 2017) at 10, 11.
[1989] See letter from Member of the European Commission Věra Jourová to Chairman of WP29 (2017) page 2 < https://zwenneblog.weblog.leidenuniv.nl/files/2018/06/Letter-Cssr-Jourova-to-Falque-Pierrotin.pdf > accessed 8 February 2024.
[1990] Recital 7 GDPR.
[1991] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona paras 69, 70.
[1992] Recital 68 GDPR.
[1993] Recital 11 GDPR.
[1994] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.

effective.[1995] However, this is not the case for the right to data portability due to the severely restricted scope concerning personal data generated by AI. This Type 3 legal problem occurs regardless of which AI discipline has been used to infer or derive personal data because the problem is caused by the restricted scope of Article 20 GDPR. It is therefore a general problem and potentially relates to all AI disciplines introduced in Chapter 2.

The restricted scope problem (Type 3)
The right to data portability excludes personal data derived and/or inferred by AI from its scope and thus fails to enhance the data subjects' control over their own personal data. The right to data portability is therefore not fit for purpose to protect the fundamental right to data protection.

5.10 Objection

As introduced in Section 3.3.4.5, Article 21 (1) GDPR provides the data subject a right to object to processing 'on grounds relating to his or her particular situation'. Simultaneously, it imposes a duty on the controller to cease processing unless it can demonstrate 'compelling legitimate grounds for the processing' which override the interests, rights and freedoms of the data subject *or* for the establishment, exercise or defence of legal claims.[1996] The right to object *exclusively* applies to processing based on the legal ground 'performance of a task carried out in the public interest' according to Article 6 (1) lit e and legitimate interest according to Article 6 (1) lit f GDPR. Data subjects do not have a right to object to processing if controllers rely on legal grounds other than those mentioned.

5.10.1 Legal problems: Type 1

As described in Section 4.2.1, AI has the potential to determine why and how to process personal data due to its autonomous and adaptive characteristics. The balancing problem explained in Section 4.2.1 also applies to the right to object because processing based on the legal basis of 'legitimate interest' constitutes one of the two grounds on which data subjects can exercise this right. In essence, the balancing problem refers to the incapability of autonomous AI systems to appropriately balance the fundamental rights and freedoms of the parties involved in accordance with the Legitimate Interest Assessment (LIA) and the proportionality principle (Sections 4.2.1 and 3.3.2 respectively). This is caused by the reasoning deficiencies in the AI discipline AR. The said problem also applies to the balance of interests that a controller must perform in order to demonstrate its 'compelling legitimate ground' according to Article 21 (1) GDPR.

[1995] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[1996] Article 21 (1) GDPR.

If a data subject objects to processing based on Article 21 (1) GDPR and the controller does not intend to cease such processing, it must be able to demonstrate its compelling legitimate ground for processing overrides the interests, rights and freedoms of the data subject.[1997] As explained in Section 3.3.4.5, the burden of proof that the conditions in Article 21 (1) are met lies with the controller.[1998] However, current AI systems have been called to be clueless[1999] to understand cause and effect and to be devoid of common sense.[2000] Common sense reasoning constitutes a major challenge in AI,[2001] particularly in the discipline of automated reasoning (see Sections 2.2.5, 4.3.1, 4.4.1 and 4.7.1). Apparently, there is not one AI system today which has a semblance of common sense or has capabilities such as human cognition. Hence, AI systems are unable to think on par with human thinking[2002] and are therefore not able (at least not in the near future) to appropriately weigh the fundamental rights and freedoms of the parties involved as required by the 'compelling legitimate ground' balancing according to Article 21 (1) GDPR.

Data processing is likely to continue after a data subject enforced the right to object. AI systems autonomously perform processing activities meaning that the AI system makes its own decisions and executes tasks on the controller's behalf.[2003] When a data subject exercises the right to object, whether successful or not, the controller must *immediately* restrict the processing pursuant to Article 18 (1) lit d GDPR.[2004] It is unlikely that a controller immediately restricts the processing of personal data. In addition, there is arguably not 'one' command that the controller can execute that immediately restricts all relevant processing activities that occur in the complex environment of AI systems. Take, for example, a supermarket chain that processes personal data of its customers by means of an ML-powered system to obtain valuable insights about the personal aspects of the customers based on purchase history. The supermarket relies on its legitimate interest according to Article 6 (1) lit f GDPR as the legal ground for such processing. Based on two dozen products used as proxies, the powerful ML prediction model identifies pregnant customers. After becoming aware, one customer objected to such processing according to Article 21 (1) GDPR. The processing performed by the ML-powered

[1997] Article 21 (1) GDPR.
[1998] 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.
[1999] 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.
[2000] 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.
[2001] 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.
[2002] 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.
[2003] Eduardo Alonso, 'Actions and agents' in Frankish Keith and Ramsey William M. (eds) *The Cambridge Handbook of Artificial Intelligence* (2014) 235, 236.
[2004] 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) 518.

system is complex and entangled, and the customer's personal data are incorporated into the system's models. As mentioned in Section 5.8.1, ML could store personal data as a part of its models.[2005] But the system processes also personal data of all other customers of the supermarket, who did not object to such processing. It seems rather unlikely that the supermarket chain shuts down the whole ML system, simply because one customer objected to such processing. Instead, the supermarket may consider to retrain the ML models to cease the processing of personal data relating to the customer who successfully objected to it. However, such re-training is computationally burdensome because large-scale algorithms can take weeks to train.[2006] In any case, the controller will not be able to *immediately* restrict processing pursuant to Article 18 (1) lit d GDPR.[2007]

Due to the balancing problem explained in Section 4.2.1, AI systems cannot balance interests to demonstrate the controller's 'compelling legitimate ground' according to Article 21 (1) GDPR. This is mainly caused by the reasoning deficiencies in the AI discipline AR explained in Section 4.3.1. Processing is likely to continue after the data subject enforced its right to object because AI systems autonomously perform processing activities.[2008] Controllers are unable to *immediately* restrict the processing pursuant Article 18 (1) lit d GDPR because processing performed by AI is complex. In addition, ML systems process personal data of various data subjects, and it seems unlikely that controllers shut down a whole system simply because only one data subject enforced its right to object. Therefore, processing of personal data does not cease, but continues. This violates the right to object according to Article 21 (1) GDPR. This Type 1 legal problem applies to all AI disciplines as introduced in Chapter 2 because the ability to autonomously make decisions and execute tasks on the designer's behalf[2009] constitutes a key element of AI (see Section 2.1).

The continuance problem (Type 1)

The balancing problem introduced in Section 4.2.1 also applies to the 'compelling legitimate ground' balancing required by Article 21 (1) GDPR allowing data subjects to object to processing performed by autonomous AI systems. Because AI systems make their own decisions and execute tasks independently, processing of personal data can continue after the data subject has enforced its right to object. Because processing performed by AI systems is highly entangled and complex, controllers cannot immediately restrict processing as required by Article 18 (1) lit d GDPR. Consequently, the right to object is violated.

[2005] Jef Ausloos, Michael Veale, René Mahieu, 'Getting Data Subject Rights Right' (2019) Vol 10 Iss 3 JIPITEC 283, 295-296.
[2006] Antonio Ginart et al, 'Making AI Forget You: Data Deletion in Machine Learning', Advances in Neural Information Processing Systems (2019) 2 <https://proceedings.neurips.cc/paper/2019/file/cb79f8fa58b91d3af6c9c991f63962d3-Paper.pdf> accessed 8 February 2024.
[2007] 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) 518.
[2008] Eduardo Alonso, 'Actions and agents' in Frankish Keith and Ramsey William M. (eds) *The Cambridge Handbook of Artificial Intelligence* (2014) 235, 236.
[2009] Ibid.

5.10.2 Legal problems: Type 2

No Type 2 legal problems arise when the right to object is applied to the AI disciplines introduced in Chapter 2. This is mainly because the controller must demonstrate a compelling legitimate ground if the controller intends to continue with the processing of personal data after the data subject has enforced its right to object. Thus, the burden of proof is imposed on the controller. In addition, data subjects may object to processing for direct marketing unconditionally: no conditions are attached to effectively enforce this right. The data subject simply needs to object to processing for direct marketing purposes to be successful.[2010]

5.10.3 Legal problems: Type 3

AI provides powerful tools to infer and otherwise generate personal data. Such data provides controllers with valuable insights about data subjects, their personal aspects in particular. Controllers may use AI for profiling as defined in the GDPR. Article 4 (4) GDPR defines profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person'. Inferred data generated by ML may ascribe attributes to individuals using ML techniques such as regression, classification (see Section 2.2.1.1) or clustering (Section 2.2.1.2) and thus amount to profiling as defined in the GDPR. ML infers personal data by detecting patterns and correlations and making predictions, such as likelihood of pregnancy, life expectancy or credit risks (see Section 4.4.1). AC as introduced in Section 2.2.4 generates personal data which indicates the emotional state of a data subject. Processing through AC amounts to profiling as defined in the GDPR because it evaluates a particular aspect of the data subject, namely, his emotional state exhibited during a given activity (for example, during the data subject's conversation with its virtual assistant). When the right to object according to Article 21 (1) GDPR is applied to profiling, problems arise regarding the subsequent erasure of inferred personal data in cases in which the rights and interests of the data subject prevail.

Let me explain this through the supermarket's ML-powered system introduced in Section 5.10.1, which infers valuable information about the personal aspects of its customers based on their purchase history. After identifying pregnant customers through the powerful ML system, the supermarket sends them a targeted email announcement and offers vouchers for baby food. One of the customers concerned, a 21-year-old student still living at home, is rather upset and considers the marketing communication of the supermarket very intrusive. She is also very concerned that her parents will learn about her unexpected pregnancy because the family shares a common account with the

[2010] 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.

supermarket.[2011] Curious about her data protection rights, the customer consults the supermarket's privacy notice and objects to the processing of her personal data for marketing purposes according to Article 21 (2) GDPR. According to Articles 12 (3) and 21 (3) GDPR, the supermarket confirms to the data subject by email that it does not process information about her pregnancy for marketing purposes. Understandably, the customer assumes that the supermarket has erased this sensitive information.

However, the conclusion drawn by the customer is incorrect. Following a successful objection according to Article 21 (2) GDPR, the personal data are not erased from the supermarket's systems. On the contrary, the wording contained in Article 21 (3) GDPR points to the possibility of processing for *other* purposes[2012] because the provision states that 'personal data shall no longer be processed for such [direct marketing] purposes'. To do so, the supermarket needs to comply with all the requirements of the GDPR, in particular the data protection principles introduced in Section 3.3.3. Nevertheless, as already outlined in Section 4.5.3, if controllers make an effort to define purposes with sufficient specificity and can demonstrate that such purposes are legitimate, any purpose is a valid purpose under the GDPR.[2013] This holds particularly true given the lack of judicial guidance with respect to the relevant criteria for determining the precision of the purpose.[2014] Thus, it is not unlikely that controllers will successfully fiddle about a new purpose. To have her personal data concerning pregnancy deleted, the customer must submit a separate erasure request based on Article 17 (1) lit c GDPR. However, even then, the supermarket may opt to only erase the pregnancy-related personal data from a dedicated list or database kept for direct marketing purposes and continue with processing for other purposes.[2015] Then, the supermarket can argue that Article 17 (1) lit a GDPR does not apply because processing is still necessary for these other purposes. This provision requires controllers to erase personal data that 'are no longer necessary in relation to the purposes for which they were collected or otherwise processed'.

The outcome is the same with respect to the profile and the personal data inferred by AC. Take, as an example, Amazon's patent introduced in Section 5.5.1, which specifically refers to AI disciplines NLP and ML (particularly ANN as applied in DL). Following the claims of this patent, Amazon's virtual assistant Alexa is able to detect a user's emotional state such as happiness, joy, anger, sorrow,

[2011] Example taken from Viktor Mayer-Schönberger; Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think* (Houghton Mifflin Harcourt 2013) 58.
[2012] Helena U Vrabec, 'Uncontrollable: Data Subject Rights and the Data-driven Economy' (Dissertation, Leiden University 2019) 180; 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) 518.
[2013] 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.
[2014] Maximilian von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws* (Nomos 2017) 232, 233, 244.
[2015] 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) 518.

sadness or fear based on analysis of acoustic features as determined from the user's speech.[2016] This enables Alexa to intuitively advertise specific products based on the user's current emotional state.[2017] As in the supermarket example, if the data subject objects to the processing of its emotion data for direct marketing purposes, Amazon is not required to entirely erase such emotion data, even if the data subject hands in a separate erasure request. Amazon may simply erase such data from a dedicated list or database kept for direct marketing purposes and further process emotion data for other purposes. Obviously, such further processing for other purposes requires a corresponding assessment of the controller.

As an alternative to object to processing for direct marketing purposes according to Article 21 (2) GDPR, the customer may also object to the processing of her personal data based on Article 21 (1) GDPR. The customer could argue that on grounds relating to her particular situation, namely, that her pregnancy constitutes rather sensitive information and her parents are not yet aware of it, the controller must cease the processing of the personal data for all *conceivable or envisaged* purposes. It is unlikely that the supermarket in this case can demonstrate 'compelling legitimate grounds for processing', which override the interests, rights and freedoms of the customer. It has been argued that, if the objection of the data subject has merit (like in this particular case), the controller cannot retain the personal data in question but must erase it[2018] without undue delay.[2019] According to this view, the controller cannot retain personal data subsequent to a successful objection because storage constitutes a form of processing defined in Article 4 (2) GDPR, and, when interpreted together with Article 17 (1) lit c GDPR, imposes the obligation on the controller to erase the personal data in question, without requiring the data subject to submit a separate erasure request according to Article 17 (1) lit c GDPR.

In my view, it must be added that particularly the storage limitation principle as introduced in Section 3.3.3.7 obliges the controller to erase the personal data in question. This principle requires controllers to not store personal data longer than necessary in relation to the purpose of processing. When applied to the supermarket case, the supermarket must erase the personal data concerning the pregnancy of the customer. Processing is no longer necessary in relation to all conceivable processing purposes because the customer's rights and interests prevail. However, the view that controllers are obliged to erase personal data after a successful objection request, without a separate erasure request according to Article 17 (1) lit c GDPR, is by no means supported by CJEU case law. On the basis of a

[2016] Huafeng Jin, Shuo Wang, 'Voice-based Determination of Physical and Emotional Characteristics of Users' US Patent Number US 10096319B1 (Assignee: Amazon Technologies, Inc.) October 2018 <https://patentimages.storage.googleapis.com/f6/a2/36/d99e36720ad953/US10096319.pdf>, accessed 8 February 2024.
[2017] James Cook, 'Amazon patents new Alexa feature that knows when you're ill and offers you medicine' *The Telegraph* (London 9 October 2018) < https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/> accessed 8 February 2024.
[2018] 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) 518.
[2019] Article 17 (1) lit c GDPR.

teleological interpretation, the CJEU could confirm this interpretation, but has not done so yet. However, as demonstrated by the training data problem contained in Section 5.8.1, in most cases it will technically not be feasible for the controller to delete such personal data, retrain or unlearn the ML model or alternatively anonymise the personal data.

The AI disciplines AC, NLP and ML provide controllers with powerful means for profiling and allow them to infer and otherwise generate personal data. If controllers rely on their legitimate interest for profiling and infer personal data by means of these AI disciplines, and if data subjects successfully object to this, personal data generated by AI systems will not be automatically erased and may be further processed for *other* purposes. The outcome of an objection according to Article 21 (1) and (2) GDPR varies regarding the subsequent erasure of the personal data in question. If the data subject opts to object to the processing for direct marketing purposes, the personal data inferred or otherwise generated by means of AC, NLP and ML approaches will not necessarily be entirely erased by the controller, if the latter specified another purpose for processing. If the data subject objects based on paragraph 1 instead of paragraph 2 of Article 21 GDPR, the personal data must be erased by the controller if the teleological interpretation of Articles 21 and 17 GDPR is affirmed by the CJEU. In any case, it is highly unlikely that the data subjects are aware of these legal nuances when objecting to the processing of their personal data. Data subjects are arguably more likely to rely on paragraph 2 of Article 21 GDPR because there are no conditions attached to enforce this right.[2020]

Therefore, the right to object is not fit for purpose to effectively[2021] protect the fundamental right to data protection. In its case law, the CJEU has repeatedly stressed that EU data protection law aims to effectively protect[2022] the data subject's personal data against risk of misuse.[2023] Such risk of misuse seems likely to occur when controllers are not obliged to erase highly sensitive personal data because data subjects chose paragraph 2 instead of paragraph 1 when objecting to processing according to Article 21 GDPR. Examples of such sensitive data generated by means of AI are emotion data derived by means of AC or pregnancy predictions facilitated by ML. Similarly, the legal nuances contained in Article 20 GDPR fail to achieve the GDPR's aim of enhancing the legal and practical certainty for data subjects (Recital 7). In addition, Article 21 GDPR does not achieve the GDPR's goal that 'natural persons should have control of their own personal data',[2024] although this was one of the main reasons for the data protection reform.[2025] As outlined in Section 4.4.3, enforceable rights are one of the main

[2020] 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) 518.
[2021] Recital 11 GDPR.
[2022] 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.
[2023] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECR-I 238 paras 54 and 66; Joined Cases C-203/15 and C-698/15 [2016] *Tele 2 Sverige* ECR-1 970 paras 109 and 122; Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECR I-650 para 91.
[2024] Recital 7 GDPR.
[2025] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona paras 69, 70.

mechanisms for data subjects to exercise control over the processing of their personal data. However, due to the complex legal nuances in Article 21 GDPR, data subjects cannot really exercise control over the processing of their personal data. When the data subject objects based on Article 21 (2) GDPR, personal data will not necessarily be erased, and it can be further processed for purposes other than direct marketing.

The erasure after objection problem (Type 3)
ML, NLP and AC provide controllers with powerful means for profiling. When data subjects object to such profiling, controllers are not necessarily required to erase the generated personal data because erasure depends on legal nuances of which data subjects are most likely not aware. This right is not fit for purpose to protect the fundamental right to data protection, as it fails to effectively protect data subjects from misuse and to provide data subjects with control concerning processing of profiling outcomes generated by AI for purposes other than direct marketing.

5.11 Automated decision-making

As outlined in Section 3.3.4.6, Article 22 (1) GDPR grants individuals the right 'not to be subject to a decision based only on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Preparatory documents on the drafting of Article 22 GDPR provide little explanation about its rationale. It seems that the rationale is rooted in the predecessor of Article 22 GDPR, namely, Article 15 DPD. Article 15 DPD aimed to address the potential weakening of the ability of individuals to exercise influence over decision-making processes that significantly affect them considering the growth of automated decision-making (ADM) and concerns about the quality of ADM. Other concerns are the fear that ADM will cause humans to take the validity of ADM for granted, thereby reducing own responsibility to investigate the matters involved, and the concern to uphold human dignity by ensuring that humans keep their autonomy. The same concerns arguably also apply to Article 22 GDPR in addition to harms related to profiling, on which the preparatory documents of the GDPR mainly focus.[2026] This would also match with the rationale of Article 22 GDPR identified by the CJEU: protecting individuals effectively against the particular risks associated with the automated processing of personal data, including profiling.[2027] In AG Pikamäe's opinion, Article 22 GDPR aims to safeguard human dignity. It also prevents data subjects from being subject to ADM without any human intervention, which monitors whether ADM has been taken properly, fairly and without discrimination.[2028]

[2026] 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.
[2027] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 57.
[2028] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 19.

AI contributes significantly to ADM. As outlined in Section 2.2.1, ML uses data-driven methods, combining fundamental concepts in computer science with approaches from statistics, probability and optimisation in order to achieve its main goal, which is to generate accurate predictions for unseen data and to design efficient algorithms to produce these predictions.[2029] ADM may be facilitated by ML alone or in combination with other AI disciplines. In fact, ML may be fused with other AI disciplines in dedicated systems, for example, emotion detection systems which, depending on the system at hand, combine the disciplines ML, CV, NLP and AC in order to produce automated decisions concerning the data subject.

Article 22 GDPR suffers from significant weaknesses[2030] and the ambiguity and complexity of the right makes it difficult to apply in practice.[2031] The complexity also relates to the mechanics of Article 22 GDPR: The first paragraph provides for a right not to be subject to ADM, and the second paragraph provides exceptions to that right, while the third paragraph qualifies two of those exceptions by adding requirements to them ('suitable safeguards'). Finally, the fourth paragraph introduces a further qualification to all the exceptions provided in paragraph 2, i.e. a prohibition on ADM based on special categories of personal data but simultaneously provides some exceptions to this prohibition.[2032]

5.11.1 Legal problems: Type 1

As outlined in Sections 4.2.1 and 5.10.1, AI has the potential to decide itself why and how to process personal data due to its autonomous characteristics. Current AI systems have been called to be clueless[2033] to understand cause and effect and to be devoid of common sense.[2034] Common sense reasoning constitutes a major challenge in AI,[2035] particularly in the discipline AR (see Sections 2.2.5, 4.3.1, 4.4.1 and 4.7.1). Because AI systems make their own autonomous decisions[2036] about the processing of personal data and lack cognitive skills on par with human thinking,[2037] they are prone to violate the

[2029] Mehryar Mohri, Afshin Rostamizadeh, Ameet Talwalkar, *Foundations of Machine Learning* (MIT Press 2012) 1.
[2030] 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.
[2031] 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.
[2032] 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) 85.
[2033] 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.
[2034] 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 8 February 2024.
[2035] Brandon Bennet, Anthony G Cohn, 'Automated Common-sense Spatial Reasoning: Still a Hughe Challenge' in Stephen Muggleton, Nicholas Chater (eds) Human-Like Machine Intelligence (Oxford University Press 2021) 405; Gary Marcus, Ernest Davis, *Rebooting AI: Buidling Artificial Intelligence we can trust* (Pantheon Books 2019); 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.
[2036] Eduardo Alonso, 'Actions and agents' in Frankish Keith and Ramsey William M. (eds) *The Cambridge Handbook of Artificial Intelligence* (2014) 235, 236.
[2037] 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-

prohibition of ADM enshrined in Article 22 (1) GDPR. The balancing problem explained in Section 4.2.1 outlines that autonomous AI systems cannot balance the fundamental rights and freedoms of the parties involved due to the reasoning deficiencies in the AI discipline AR. Due to exactly these reasoning deficiencies, autonomous AI systems are also not capable of assessing whether ADM produces legal or similarly significant effects for the data subjects concerned. Consequently, autonomous AI systems can produce ADM with legal or similarly significant effects for data subjects despite the prohibition contained in Article 22 (1) GDPR. Due to these reasoning deficiencies, it is unlikely that these systems can determine which exception to the prohibition according to Article 22 (2) GDPR applies to a particular case, that is, whether ADM is (i) necessary to enter or perform a contract, (ii) authorised by EU or MS law and (iii) based on the consent of the data subject. This Type 1 legal problem applies to all AI disciplines as introduced in Chapter 2 because the ability to make autonomous decisions and execute tasks on the designer's behalf[2038] constitutes a key element of AI (see Section 2.1).

The autonomous ADM problem (Type 1)

Autonomous AI systems could make their own decisions on how and why to process personal data. Due to the reasoning deficiencies in the AI discipline AR, such systems are likely to generate automated decisions that have legal or similarly significant effects for data subjects, even in cases in which the prohibition of ADM takes effect and none of the exceptions applies. This violates Article 22 (1-2) GDPR.

5.11.2 Legal problems: Type 2

Provided that all cumulative requirements mentioned in Article 22 (1) GDPR are met, Article 22 (3) GDPR provides the data subject with the right to obtain human intervention on the part of the controller. The corresponding Recital 71 does not further elaborate on what is required for such human intervention. To be effective, it has been argued that human intervention must be meaningful[2039] - and this is a rightful claim. Regulatory guidance explains that the human reviewer should undertake a thorough assessment of all the relevant data, including additional information provided by the data subject.[2040]

In my view, the human reviewer seems to have an almost unachievable task when taking the problems with respect to the interpretability of AI systems into account. As outlined in Section 4.4.1, most

have-a-legal-right-to-know-of-ai-inferences-about-you-including-those-via-ai-based-self-driving-cars/amp/> accessed 8 February 2024.

[2038] Eduardo Alonso, 'Actions and agents' in Frankish Keith and Ramsey William M. (eds) *The Cambridge Handbook of Artificial Intelligence* (2014) 235, 236.

[2039] 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.

[2040] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) at 27.

current DL models lack reasoning and explanatory capabilities, making them vulnerable to produce unexplainable outcomes. In particular, DL methods based on ANNs generally lack interpretability[2041] due to the hierarchical and nonlinear structure of ANNs. There is limited understanding of how each data point impacts the ML model and the ADM produced by it. Methods to measure the influence of a particular training point on the parameters of a model are scarce and subject to ongoing research.[2042] I take the view that in the case of complex AI systems, for example, involving DL and ANNs, obtaining meaningful human interventions in ADM is currently hardly possible due to the lack of interpretability of the AI systems and the ADM deployed by them. An additional factor is the incapacity of humans to grasp the logic of multidimensional ML algorithms. Typically, humans will struggle even more than machines with decisions produced by the ML algorithms currently used simply because humans cannot handle such an array of operational factors.[2043] Therefore, the right to obtain human intervention as enshrined in Article 22 (3) GDPR – if it shall be meaningful – cannot be enforced. This constitutes a Type 2 legal problem.

The intervention problem (Type 1)

AI systems deploying DL and ANN approaches are likely to produce output that is not interpretable for humans. When used in the context of ADM, meaningful human intervention as required by Article 22 (3) is impossible. Consequently, the data subject's right to obtain human intervention cannot be enforced.

Even if issues concerning interpretability can be overcome, it seems questionable whether humans are, in fact, able to assess the quality of output generated by means of AI correctly. There is experimental evidence suggesting that humans are not, although the concept of human oversight (intervention) rests on the assumption that humans are able to do so.[2044] Thus, the concept of human intervention seems to be flawed, which could also lead to a Type 3 legal problem.

5.11.3 Legal problems: Type 3

Article 22 GDPR creates three Type 3 legal problems when applied to AI. These three legal problems are the cumulativeness, opaque ADM and procedural safeguard problems.

[2041] Deng Li and Liu Yang, 'A Joint Introduction to Natural Language Processing and Deep Learning' in Deng Li and Liu Yang (eds) *Deep learning in natural language processing* (Springer 2018) 11, 12.
[2042] Lucas Bourtoule et al, 'Machine Unlearning' (IEEE Symposium on Security and Privacy, San Jose, May 2021) 1 and 3 <https://arxiv.org/abs/1912.03817> accessed 8 February 2024.
[2043] 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, 51.
[2044] Jan Biermann, John Horton, Johannes Walter, 'Algorithmic Advice as a Credence Good' (2022) Centre for European Economic Research Discussion Paper No 22-071 at 14, 17 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4326911 > accessed 8 February 2024.

Narrow and ambiguous scope

As outlined in Section 3.3.4.6, Article 22 (1) GDPR rests on three cumulative conditions to apply: (i) a decision is made that is (ii) based only on automated processing, including profiling, and (iii) has either legal or similarly significant effects.[2045]

Regarding condition (i), serious difficulties exist in determining precisely when a decision has been made, in particular in ML contexts.[2046] Apart from Recital 71 GDPR, which states that a decision 'may include a measure', and the first case on Article 22 GDPR referred to the CJEU,[2047] there is little guidance on what constitutes a 'decision' as mentioned in Article 22 (1) GDPR. In the first case dealing with Article 22 GDPR, the CJEU ruled that the automated establishment of a probability value concerning the ability of a data subject to service a loan ('score value')[2048] adopted by the credit agency SCHUFA in itself constitutes a solely-automated decision in the sense of Article 22 (1) GDPR.[2049] In this scenario, that score value is transmitted to a third party controller (financial institution), which then enters into or refrains from entering into contractual relationships with the data subject strongly drawing on that score value.[2050] However, it could be argued that a score value in itself does not represent a decision in the sense of Article 22 (1) GDPR. It rather constitutes a prediction of the data subject's future behaviour and/or the result of profiling that evaluates personal aspects about the data subject which *could subsequently* be used for decision-making (whether automated or not).[2051] Bygrave suggests that a decision in the sense of Article 22 (1) GDPR covers a large range of situations and should be viewed in a fairly generic sense, provided it is formalised and can be distinguished from other stages that prepare, support or complement decision-making.[2052] A decision in this sense usually requires some degree of binding effect which follows from the very concept of a decision.[2053] It can be argued that this binding effect is absent in this specific case because it is *another controller*, i.e. the financial institution, that takes the decision by applying the score value when determining whether the data subject receives the loan. However, the CJEU and AG Pikamäe reject such an interpretation. Following AG Pikamäe's opinion, [2054] the CJEU interprets the notion of a

[2045] 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.
[2046] 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) 253.
[2047] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957.
[2048] Based on personal data of the data subject.
[2049] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 73.
[2050] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 14-21.
[2051] Regulatory guidance names the example that where a human decides to agree the loan based on a profile based by purely automated means constitutes decision-making based on profiling; see Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) at 6, 7.
[2052] 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.
[2053] Lee A Bygrave, 'Automated Profiling, minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling' (2001) Vol 17 No. 1 Computer & Law Security Report 1, 18-19; Andreas Häuselmann, 'Profiling and the GDPR: Harmonised Confusion' (2018) Jusletter 13 <https://jusletter.weblaw.ch/juslissues/2018/924/profiling-in-the-gdp_3b8e8a124f.html__ONCE&login=false> accessed 8 February 2024.
[2054] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe paras 42, 47, 52.

decision broadly.[2055] According to the CJEU, such a broad interpretation is needed to prevent a circumvention of Article 22 GDPR and to avoid the resulting lacuna in legal protection.[2056] In the view of the CJEU, this interpretation also serves the purposes and objectives pursued by the GDPR. In addition, it reinforces the effective protection which Article 22 GDPR aims to achieve.[2057]

Even when interpreting the notion of a decision broadly, the question is whether ML-powered systems actually produce decisions in the sense of Article 22 GDPR. In many cases, ML will generate output that lacks the binding effect. ML merely generates predictions, which is one of its core goals.[2058] Thus, the output of an ML system constitutes something which *may* be used for decision-making, whether automated or not. ML models mostly generate classifications or uncertain estimations as they are incapable of synthesising the estimation and relevant uncertainties into a decision for action.[2059] Therefore, the output generated by ML, notably predictions concerning the future behaviour of data subjects, does arguably not constitute decisions in the sense of Article 22 (1) GDPR. Such output lacks the degree of binding effect required by the very concept of a decision. Instead, they prepare, support or complement decision-making. Predictions may have a binding effect once they are *applied towards* the data subject. Whereas obvious cases, such as the automated establishment of a score value constitute decisions in the sense of Article 22 (1), this is less clear in the context of AI. Decision-making processes with several stages[2060] are more complex, making it difficult to determine when and how a decision is made. Think, for example, of all the actors involved in targeted advertisement online.

Requirement (ii), i.e. the decision must be based 'solely' on automated processing, excludes AI systems that only provide decisional support for decision-making from the scope of Article 22 GDPR.[2061] When there is a 'human in the loop', which is the case when the automated processing functions solely as decisional support, Article 22 GDPR is not applicable.[2062] According to regulatory guidance, Article 22 (1) GDPR cannot be circumvented by 'fabricating' human intervention in the decision process so that the decision is no longer 'solely' automated.[2063] Thus, the crucial question concerning requirement (ii) is whether the processing of personal data involves human intervention and if so, what the extent of such intervention is. In fact, the first case on ADM referred to the CJEU for a

[2055] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 44-46.
[2056] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 61.
[2057] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 51 and 60.
[2058] See Section 2.2.1.
[2059] 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, 46.
[2060] For an overview see Ruben 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.
[2061] 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.
[2062] 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 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[2063] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) at 27.

preliminary ruling addresses this issue. The establishment of the score value adopted by the controller SCHUFA meets requirement (ii) as such processing constitutes profiling and is thus 'based solely on automated processing'.[2064]

However, the *SCHUFA* ruling did not address the question what type of human involvement renders Article 22 (1) GDPR inapplicable, meaning processing is not 'solely automated' anymore. In many cases, this will be the decisive question regarding the applicability of Article 22 GDPR. Due to the lack of judgements at the CJEU level, it is worth considering case law at the level of the Member State ('MS'). Cases at MS level have tended to result in findings that the automated processing at issue was not fully automated.[2065] In fact, a report assessing ADM in light of the GDPR concludes that 'Courts across the EU have found that some (often limited) degree of human involvement...[..] was enough to set aside the application' of Article 22 GDPR.[2066] One case[2067] in the Netherlands specifically addressed the question what constitutes 'solely' automated processing according to Article 22 (1) GDPR. In this case, the data subjects (Uber drivers) contested the arguably fully automated deactivation of their Uber Driver account resulting from potential fraud signals detected by Uber's algorithm intended to prevent and detect fraud.[2068] However, Uber argued that its 'risk team' ultimately takes the decision to deactivate the Uber account of the drivers.[2069] The Amsterdam district Court accepted Uber's argumentation and ruled that there were no fully automated decisions. Consequently, the Court also denied the drivers' right to obtain meaningful information about the logic involved according to Article 15 (1) lit h GDPR with respect to the processing performed by Uber.[2070] This strongly underscores the problem regarding condition (ii). The Court of Appeal overturned the district Court's ruling. In the opinion of the Court of Appeal, Uber failed to sufficiently substantiate actual human intervention.[2071] Although Uber claimed that one or more members of Uber's risk team carried out manual investigations in each deactivation case, it failed to make this sufficiently plausible. In view of the Court of Appeal, Uber did not in any way demonstrate that the actions performed by the members of Uber's risk team was much more than merely a token gesture[2072] as mentioned in

[2064] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 47.
[2065] 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 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[2066] 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.
[2067] Amsterdam District Court 13 March 2021, ECLI:NL:RBAMS:2021:1018.
[2068] Ibid paras 2.4, 3.1, 3.2.
[2069] Ibid para 4.19.
[2070] Ibid para 4.26; Raphaël Gellert, Marvin van Bekkum, and Frederik Zuiderveen Borgesius, 'The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making' *EU Law Analysis* (28 April 2021) accessed 8 February 2024.
[2071] Amsterdam Court of Appeal 4 April 2023, ECLI:NL:GHAMS:2023:793 para 3.24; Amsterdam Court of Appeal 4 April 2023, ECLI:NL:GHAMS:2023:796 para 3.37.
[2072] Amsterdam Court of Appeal 4 April 2023, ECLI:NL:GHAMS:2023:793 para 3.24.

regulatory guidance.[2073] A decisive factor for this was the lack of any personal conversation between members of Uber's risk team and the drivers affected by the deactivations. In the only deactivation case involving such a personal conversation, the Court of Appeal ruled that there was indeed sufficient human intervention.[2074] Thus, a personal conversation seems to satisfy the requirements of actual human intervention, at least in view of the Amsterdam Court of Appeal. To me, this seems to be a rather low threshold. Ultimately, the ruling reaffirms the conclusion of a report assessing ADM in light of the GDPR: 'Courts across the EU have found that some (often limited) degree of human involvement...[..] was enough to set aside the application' of Article 22 GDPR.[2075]

In the context of AI, the requirement (i) that Article 22 (1) GDPR applies exclusively to decisions 'solely' based on automated processing creates a significant loophole because the output generated by AI is often used to support nonautomated decision-making. For example, the AC-powered HireVue software analyses the emotions a job candidate portrays during the video assessment[2076] and automatically assigns the candidate with an average rating (score) and recommendation whether or not to be employed. Subsequently, the recruiter has the discretion to decide, i.e. to select one of the recommended candidates. In such a scenario, Article 22 (1) GDPR does not apply because the decision-making process is not 'solely' automated. This is different with the automated establishment of a credit score adopted by a credit agency, which occurs without any human involvement. Also, credit scores are proven to play a pivotal role in the bank's decision to grant a loan.[2077] Requirement (i) is also problematic regarding decision-making processes involving multiple stages[2078] and multiple processing activities and controllers. AG Pikamäe acknowledges the difficulty in identifying the ultimately relevant decision, particularly[2079] when processing in the context of ADM involves several actors.

Requirement (iii) states that the decision produces legal effects concerning the data subject or 'significantly affects' him or her. Recital 71 GDPR names only two examples: automatic refusal of an online credit application or e-recruiting practices without any human intervention. Legal effects are effects that are able to alter or determine a person's rights or duties.[2080] An automated court decision

[2073] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) at 21.
[2074] Amsterdam Court of Appeal 4 April 2023, ECLI:NL:GHAMS:2023:793 para 3.25.
[2075] 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.
[2076] 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.
[2077] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 50.
[2078] See for an overview: Ruben 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.
[2079] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 40.
[2080] Lee A. Bygrave, 'Automated Profiling, minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling' 2001 Vol 17 No 1 Computer & Law Security Report 19.

is an example of a decision with legal effects.[2081] Regulatory guidance names as examples the cancellation of a contract, entitlement or denial of social benefits or refused admission to a country or denial of citizenship.[2082] The real ambiguity of requirement (iii) lies within the wording 'significantly affects'. This appears to be rather vague, and it is difficult to determine what should be considered 'sufficiently significant' to meet the threshold, which is even acknowledged in regulatory guidance.[2083] AG Pikamäe sheds some light on this notion. In his view, these significant effects may be of economic and/or social nature and relate to severe consequences for the data subject's freedoms and autonomy. They include adverse effects resulting from a negative score value, if it significantly restricts the data subject in exercising its freedoms or even stigmatises the data subject.[2084] In its decision in *SCHUFA*, the CJEU ruled that the automated establishment of a credit score by a credit agency significantly affects the data subject in the sense of requirement (iii). An insufficient credit score leads, in almost all cases, to the bank refusing to grant the loan applied for.[2085]

The ambiguity surrounding the notion of significant effects is quite unfortunate when considering that requirement (iii) constitutes one of the three decisive components that determines whether Article 22 (1) GDPR is applicable or not. Indeed, Belgium, Germany, Ireland, Italy, Finland, Poland and the UK stated during the law-making process that this wording is unclear and needs further clarification.[2086] Italy mentioned that 'it should be specified that this expression covers, for example, the application of network analysis instruments, user behaviour tracking, the creation of movement profiles via portable applications and the creation of personal profiles through social networking sites'.[2087] Poland argued that the vague term may lead to abuses by entities using profiling techniques.[2088] Finally, the EDPB's predecessor WP29 doubted in its opinion on the data protection reform proposals if the approach taken is sufficient to reflect the issues of creating and using profiles, an online environment in particular. Further need for clarification was mentioned by promoting that the term 'significantly affects' also 'covers the application of, for example, web analysis tools, tracking for assessing user behaviour, the creation of location profiles by mobile applications, or the creation of personal profiles by social networks'.[2089]

[2081] Frederik Zuiderveen Borgesius, 'Improving Privacy Protection in the area of Behavioural Targeting' (Doctoral thesis, Universiteit van Amsterdam 2015) 375 <https://dare.uva.nl/search?identifier=c74bdba6-616c-4cd9-925e-33a5858935e5> accessed 8 February 2024.
[2082] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) 21.
[2083] Ibid 22.
[2084] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe paras 38, 39, 42, 43.
[2085] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 48-50.
[2086] Belgium p 12, Germany p 48, Ireland p 129, 137 Italy p 137, 172 Poland p 172, Finland p 189, UK pa 237 see < https://data.consilium.europa.eu/doc/document/ST-14147-2012-INIT/en/pdf > accessed 8 February 2024.
[2087] Ibid 137.
[2088] Ibid 172.
[2089] Article 29 Working Party, 'Opinion 1/2012 on the data protection reform proposals' (WP 191, 23. March 2012) at 14.

Despite these numerous requests for clarification, the term 'significantly affects' was not further specified, not even in the corresponding Recital 71 GDPR. Typically, targeted advertising based on profiling does not meet this threshold according to regulatory guidance. However, this might be different due to the intrusiveness of the profiling process, the expectations of the data subjects, the way the advertisement is delivered or when using knowledge of the vulnerabilities of the targeted data subject.[2090] AI is very well suited to facilitate such intrusive profiling. Take, for example, Amazon's US patent 'Keyword Determinations from Voice Data'[2091] introduced in Section 4.5.1. The patent relies on the AI discipline NLP and describes a system that can capture voice content when a user speaks into or near the device (e.g., Alexa), notably without activating the virtual assistant by mentioning the 'wake word' (e.g., 'hey Alexa'). Sniffer algorithms attempt to identify trigger words that indicate statements of preference (such as like or love) and translate them into keywords. The identified keywords are then transmitted to a location accessible to advertisers, who can use the keywords to select content that is likely relevant to the user.[2092] Amazon has denied that it uses voice recordings for advertising at the moment and mentioned that the patent might never actually come to the market.[2093] In any case, it is questionable whether controllers and Courts will agree that such kind of intrusive advertisement significantly affects the data subjects in the sense of requirement (iii). Neither the GDPR nor its preparatory documents provide substantive guidance on the threshold that must be met in this regard, which ultimately leads to legal uncertainty.

It is problematic when life decisions about a person[2094] such as being hired or receiving a loan are influenced by or based on possibly inaccurate data (see Section 4.7.1) automatically *generated* by AI. The relatively narrow scope of Article 22 GDPR and the cumulative requirements that must be met to render it applicable actually provide far less support for data subjects seeking control over ADM involving automated processing facilitated by AI than initially expected.[2095] In my view, this holds true despite the CJEU's broad interpretation of a decision in *SCHUFA*[2096] because conditions (ii) and (iii) must be met simultaneously. In many cases, processing is not 'solely automated' as required by condition (ii). In addition, the vagueness in terms of the required effects foreseen by condition (iii) comes into play often.

[2090] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) 22.
[2091] 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.
[2092] Ibid.
[2093] Griffin Andrew, 'Amazon files for Alexa patent to let it listen to people all the time and work out what they want' *The indipendent* (London, 11 April 2018) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-alexa-patent-listening-to-me-facebook-phone-talking-ads-a8300246.html> accessed 8 February 2024.
[2094] Tim Lewis, 'AI can read your emotions. Should it?' *The Guardian* (London 17 August 2019) <https://www.theguardian.com/technology/2019/aug/17/emotion-ai-artificial-intelligence-mood-realeyes-amazon-facebook-emotient> accessed 8 February 2024.
[2095] 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, 46.
[2096] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 45, 60.

MS-level case law concerning Article 22 GDPR places upon data subjects the onus of showing that all the cumulative requirements are fulfilled. Often, this may be difficult to satisfy considering that the AI systems used for ADM utilise non-transparent logic and come with covert consequences.[2097] Thus, the right of data subjects not to be subject to ADM creates a Type 3 legal problem. This right is not fit for purpose to strengthen the rights of data subjects.[2098] As noted by the CJEU, effective protection of personal data requires the strengthening of the rights of data subjects, which is emphasised by Recital 11 GDPR.[2099] With its cumulative and vague requirements determining the applicability of Article 22 GDPR, this right does not effectively contribute to the GDPR's aim to strengthen data subject rights. The CJEU has stressed the importance of ensuring that data subject rights granted by the GDPR are effective.[2100] Thus, Article 22 GDPR fails to *effectively* protect individuals against the particular risks associated with the automated processing of personal data, which is the aim of this provision according to the CJEU.[2101] Controllers are likely to exploit the ambiguousness of the requirements enshrined in Article 22 GDPR to argue that this right does not apply.[2102] For example, a report assessing ADM in light of the GDPR concludes: 'Courts across the EU have found that some (often limited) degree of human involvement...[..] was enough to set aside the application' of Article 22 GDPR.[2103] A right with vague cumulative requirements cannot be considered effective.

In addition, Article 22 GDPR fails to protect data subjects against risk of misuse[2104] and from concerns relating to ADM which the GDPR aims to address. These include, among others, (i) potential weakening of the ability of individuals to exercise influence over ADM and (ii) concerns over the quality of ADM.[2105]

The ability to exercise influence over ADM (i) is intertwined with the GDPR's goal that 'natural persons should have control of their own personal data'.[2106] As outlined in Section 4.4.3, enforceable rights are one of the main mechanisms for data subjects to exercise control over the processing of

[2097] 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.
[2098] Recital 11 GDPR.
[2099] Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42.
[2100] Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[2101] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 57, 60.
[2102] 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 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721118> accessed 8 February 2024.
[2103] 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.
[2104] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECR-I 238 paras 54 and 66; Joined Cases C-203/15 and C-698/15 [2016] *Tele 2 Sverige* ECR-1 970 paras 109 and 122; Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECR I-650 para 91.
[2105] Recitals 4 and 71 GDPR; see also the rationales mentioned in COM(92) 422 final—SYN 287 at page 26 and COM(90) 314 final—SYN 287 at page 29 relating to Article 22 GDPR's predecessor DPD which remain valid for the GDPR as convincingly outlined by 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.
[2106] Recital 7 GDPR.

their personal data. Due to the narrow scope and the cumulative criteria enshrined in Article 22 GDPR, this right is in many cases not applicable to personal data automatedly processed by AI systems. Control in the sense of the GDPR is rather limited as acknowledged by AG Campos Sánchez-Bordona, stating that 'the scope for individual action is limited' and 'confined to the exercise of those rights in specified circumstances'.[2107] Article 22 (1) GDPR further restricts the already limited means for data subjects to exercise control with respect to the automated processing by means of AI systems and therefore fails to achieve this goal. Data subjects cannot obtain human intervention, express their point of view and contest the decision because Article 22 GDPR is not applicable due to the restricted scope and cumulative criteria that must be met.

Article 22 GDPR fails to protect data subjects from issues relating to the quality of ADM and 'the particular risks to their rights and freedoms associated with the automated processing of personal data, including profiling' which is the rationale of Article 22 GDPR according to the CJEU.[2108] As explained in the inaccuracy and rebuttal problems discussed in Section 4.7.1, ML and AC may *automate the generation of* inaccurate personal data. Such inaccurate data might be used for partially automated decision-making with significant effects for data subjects, like the decision to receive a loan, job offer or to be allowed to pass border control. This is also problematic with respect to Recital 4 GDPR, which states that 'processing of personal data should be designed to serve mankind'. In the examples mentioned, automated processing performed by AI serves the interest of controllers, rather than those of natural persons who want to obtain a loan, seek employment or cross a border. Thus, Article 22 GDPR fails to safeguard *human dignity*, which is another rationale of this provision, as noted by AG Pikamäe.[2109] In conclusion, Article 22 GDPR fails to achieve its aim, which is, according to the CJEU, *effective protection* against the particular risks associated with the automated processing of personal data, including profiling.[2110]

This Type 3 legal problem occurs regardless of which AI discipline has been used for ADM because the problem is caused by the cumulativeness requirement enshrined in Article 22 GDPR. It is therefore a general problem and potentially relates to all AI disciplines, as introduced in Chapter 2.

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.

[2107] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona para 72.
[2108] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 57.
[2109] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-220, Opinion AG Pikamäe para 19.
[2110] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 paras 57, 60.

Information about the logic involved in ADM

As described in Section 3.3.4.6, Article 22 GDPR applies only if all three cumulative requirements are met simultaneously. Only then can the data subject enforce its right to obtain meaningful information about the logic involved in ADM and the significance and the envisaged consequences of such processing. If Article 22 GDPR is not applicable, for example, because the decision is not *solely* automated, the result will be that the data subject cannot enforce its right according to Article 15 (1) lit h GDPR. This interpretation is confirmed by regulatory guidance. Article 15 (1) lit h GDPR is discussed under Chapter IV of the guidelines on ADM, which 'explains the specific provisions that *only* apply to solely automated individual decision-making, including profiling'.[2111]

However, research on Article 15 (1) lit h GDPR suggests that 'meaningful information about the logic involved and the significance and consequences for data subjects can also be invoked where decision-making processes are only partially (rather than completely) automated'.[2112] Whereas this interpretation is certainly welcome from the data subject's perspective, it does not stand when applying the grammatical (literal) and systematic method of interpretation. The wording contained in Article 15 (1) lit h GDPR obliges controllers to inform data subjects about 'the existence of automated decision-making, including profiling, referred to in *Article 22(1)* and (4) and, *at least in those cases*, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.[2113] Due to the wording '*at least in those cases*', controllers are *not* legally required to inform data subjects about decision-making which is only partially automated. This follows from a grammatical (literal) interpretation of Article 15 (1) lit h (see also Section 4.4.3). The result is the same when applying the method of systematic interpretation. Systematically, Article 15 (1) lit h GDPR explicitly refers to Article 22 (1) GDPR, which outlines that decisions must be based *solely* on automated processing to fall within the scope of this right. Consequently, the data subjects concerned are not entitled to receive meaningful information about the logic involved in the output generated by AI systems simply because the decision taken is not fully automated.

The HireVue software and similar services[2114] aim to detect the emotional states portrayed during the automated video assessment. It will be difficult for applicants to assess the accuracy of emotion data detected by this software without having access to additional information concerning the logic involved in the processing performed by the AI system. Within the iBorderCtrl system, an 'automatic

[2111] Adding, in Footnote 3 of the guidelines 'as defined in Article 22 (1) GDPR'; see Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP 251rev.01, 6 February 2018) at 10.
[2112] Bart Custers, Anne-Sophie Heijne, 'The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice' (2022) Vol 46 Computer Law & Security Review 1, 5.
[2113] Emphasis added by the author.
[2114] HumeAI which provides AI-powered tools helping recruiters to assess personality traits as well as emotional states of candidates, see < https://hume.ai/products/facial-expression-model/ > and < https://gethume.com/blog5/artificial-intelligence-for-recruiting > accessed 8 February 2024.

deception detection system' quantifies the probability of deceit in interviews by analysing interviewees' non-verbal micro-gestures.[2115] There is an inherent risk of inaccuracy, namely, false positives that wrongly identify the interviewee as being deceptive, which might lead to a stigmatisation or prejudice against the interviewee, for example when talking to the human border guard.[2116] Because the final decision will be made by a human border guard, Article 22 GDPR is not applicable.[2117] Therefore, interviewees do not have to be informed about the logic and functionality of the iBorderCtrl system.[2118] In addition, the human border guard taking the final decision could be unduly influenced by the possibly inaccurate output of the iBorderCtrl system.[2119]

Individuals might be subject to decisions enabled or supported by AI, but do not have the means to verify whether the relevant legal provisions were respected. They face difficulties with regard to effective access to justice in case such decisions negatively affect them.[2120] Individuals cannot obtain information about the logic involved in the processing performed by the AI system because one of the requirements enshrined in Article 22 (1) GDPR is not met. This leads to a Type 3 legal problem for the same reasons as outlined in the cumulativeness problem. Article 22 (1) GDPR is not fit for purpose to strengthen the rights of data subjects and ensure that they are effective.[2121] It also fails to facilitate that data subjects can exercise control[2122] regarding the processing of their personal data processed by AI systems. As outlined in Section 4.4.3, enforceable rights are one of the main mechanisms for data subjects to exercise control over the processing of their personal data. Due to the narrow scope and cumulative criterion enshrined in Article 22 GDPR, this right is in many cases not applicable to personal data automatedly processed by means of AI systems. This is in stark contrast to what Article 22 GDPR aims to achieve according to the CJEU: *effective protection* against risks associated with the automated processing of personal data.[2123] Article 22 (1) GDPR further restricts the already limited means for data subjects to exercise control[2124] concerning the automated processing by means of AI systems and therefore fails to achieve the GDPR's legislative goal. Because one of the cumulative requirements enshrined in Article 22 (1) GDPR is not met, data subjects cannot obtain meaningful information about processing concerning ADM when enforcing their right of access. Therefore, they have no effective means to exercise control, for example, enforcing other data subject

[2115] See <https://www.iborderctrl.eu/Technical-Framework/> accessed 8 February 2024.
[2116] See <https://www.iborderctrl.eu/Frequently-Asked-Questions/> accessed 8 February 2024.
[2117] If the border guard does not blindly follow the system and 'rubber-stamp' its decision.
[2118] Tim Lewis, 'AI can read your emotions. Should it?' *The Guardian* (London 17 August 2019) <https://www.theguardian.com/technology/2019/aug/17/emotion-ai-artificial-intelligence-mood-realeyes-amazon-facebook-emotient> accessed 8 February 2024.
[2119] See <https://www.iborderctrl.eu/Technical-Framework/> accessed 8 February 2024.
[2120] Commission, 'White Paper on Artificial Intelligence - A European approach to excellence and trust' COM (2020) 65 final 12 <https://commission.europa.eu/document/d2ec4039-c5be-423a-81ef-b9e44e79825b_en> accessed 8 February 2024.
[2121] Recital 11 GDPR; Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42; Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[2122] Recital 7 GDPR.
[2123] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 60.
[2124] Case C-300/21 *UI* [2022] ECR I-756 Opinion AG Manuel Campos Sánchez-Bordona para 72.

rights, regarding decisions supported and enabled by AI that may negatively affect them. This Type 3 legal problem occurs regardless of which AI discipline has been used for ADM because it is caused by the cumulativeness requirement enshrined in Article 22 GDPR. It is therefore a general problem and potentially relates potentially to all AI disciplines as introduced in Chapter 2.

The opaque ADM problem (Type 3)

The cumulativeness problem renders Article 22 GDPR inapplicable to many decisions taken by or generated with the support of AI. Consequently, data subjects cannot obtain meaningful information about the logic involved in decisions taken by or generated with the support of AI. Data subjects are not effectively protected and have no means to exercise control regarding decisions supported and enabled by AI that may negatively affect them.

Contesting to ADM

In case all the cumulative requirements enshrined in Article 22 (1) GDPR are indeed met, the right to contest the ADM as enshrined in Article 22 (3) GDPR provides the data subject with an effective remedy with respect to ADM,[2125] at least from a preliminary point of view. The scarce literature in academia suggests that the term 'contest' means a right of appeal and therefore more than simply a right to object or oppose to ADM. To be meaningful, the right to contest shall at least oblige the controller to hear and consider the merits of an appeal made by the data subject. To be fair, the appeal process shall carry a qualified obligation to provide the data subject with reasons for the ADM.[2126]

Although these claims are valid, it seems that the right to contest ADM mostly offers a procedural safeguard rather than meaningful protection against ADM and personal data automatedly processed by AI systems. In fact, it is unlikely that a company deploying ADM will actually revise such decisions when an individual invokes her right to contest under Article 22 (3) GDPR unless sector-specific decision-making standards or other provisions of data protection law are violated.[2127]

This holds particularly true for types of ADM which determine whether to conclude a contract with the data subject. The freedom of contract is a cornerstone of EU contract law and grants parties the legal freedom to enter into a contract (or not) and agree on its content.[2128] According to the CJEU, freedom of contract is covered by the freedom to conduct a business enshrined in Article 16

[2125] 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) 93.
[2126] Ibid 93-94.
[2127] 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 570, 571.
[2128] 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.

EUCFR.[2129] A company may decide on its own discretion whether and how to conclude a contract with the data subject, provided that this complies with EU and MS law. Consider, for example, a data subject who applies for a loan at a bank. The bank has a highly sophisticated AI system in place that automatically decides whether the loan will be granted. The system deploys approaches from the AI disciplines ML and DL in particular and analyses all personal data provided by the data subject, including behaviour related to mobile phone usage, to determine the creditworthiness of the data subject. The AI system decides to not grant the loan to the data subject because the likelihood of repayment was predicted negatively due to behavioural features derived from the data subject's mobile phone usage[2130] (see Section 4.4.3).

In this scenario, all requirements enshrined in Article 22 (1) GDPR are met: There is a decision (i) which is fully automated (ii) and significantly affects the data subject (iii) because the latter will not receive the loan to buy its own apartment. In addition, the prohibition on ADM is lifted because it is necessary to assess and determine the creditworthiness of the data subject, from the bank's perspective, to enter a contract with the data subject. The data subject may very well invoke its right to contest the ADM, but the bank is by no means obliged to revert its decision. The freedom of contract grants the bank legal freedom not to enter into a contract with the data subject. Imagine a second scenario, in which an employer relies on the AC-powered HireVue software to analyse the emotions a job candidate portrays during the video assessment,[2131] automatically assigns an average score and selects the candidate with the highest score. Here as well, candidates who have been rejected may invoke their right to contest the ADM, but the employer is under no requirement to change the decision.

The right to contest to ADM is a procedural safeguard rather than a right which allows data subjects to exercise real influence over ADM that legally or significantly affect them. This leads to a Type 3 legal problem. The right not to be subject to ADM is not fit for purpose to strengthen the rights of data subjects and ensure that they are effective.[2132] This is in stark contrast to what Article 22 GDPR aims to achieve according to the CJEU: *effective protection* against risks associated with the automated processing of personal data.[2133] A right that merely provides procedural safeguards but no meaningful influence on the ADM facilitated or supported by AI systems cannot be effective, nor can it strengthen the rights of data subjects.

[2129] Case C-426/11, *Alemo-Herron* [2013] ECR I-521 para 32; Case C-283/11, *Sky Österreich* [2013] ECR-28 paras 42, 43.
[2130] Daniel Björkegren, Darrell Grissen, 'Behavior Revealed in Mobile Phone Usage Predicts Credit Repayment' (2020) Vol 34 Iss 3 The World Bank Economic Review 618, 623.
[2131] 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.
[2132] Recital 11 GDPR; Case C-132/21 *Nemzeti* [2023] ECR I-2 para 42; Case C-154/21 *Österreichische Post AG* [2023] ECR I-3 para 39.
[2133] Case C-634/21, *SCHUFA Holding AG* [2023] ECR I-957 para 60.

The ability to influence ADM is intertwined with the GDPR's goal that 'natural persons should have control of their own personal data'.[2134] As outlined in Section 4.4.3, enforceable rights are one of the main mechanisms for data subjects to exercise control. Because the right to contest is only a procedural safeguard, it fails to achieve the GDPR's goal that data subjects be able to control the processing of their personal data related to ADM. The right to contest will not really change the controller's ADM, as it is in many cases not obliged to revert its decision due to the freedom of contract. This Type 3 legal problem occurs regardless of which AI discipline has been used for ADM because it is caused by the fact that the right to contest according to Article 22 (3) GDPR is solely a procedural safeguard. It is therefore a general problem and potentially relates to all AI disciplines introduced in Chapter 2.

The procedural safeguard problem (Type 3)

The right to contest ADM as enshrined in Article 22 (3) GDPR is a procedural safeguard rather than a right that allows data subjects to exercise influence over ADM that significantly affects them. If a data subject contests ADM generated by means of AI and based on Article 22 (2) lit a GDPR, the controller is by no means required to change the outcome of the decision due to the freedom of contract. The right to contest fails to provide data subjects with effective protection and meaningful influence over ADM based on personal data.

5.12 Conclusions

This chapter addressed Subquestion 4, i.e. what legal problems arise or may arise when the enforceable rights enshrined in the current legal framework are applied to AI. I have outlined that all AI disciplines as described in Section 2.2 may raise legal problems when they are applied to the enforceable rights enshrined in the current legal framework discussed in Chapter 3. Three types of legal problems were identified, i.e. that (1) legal provisions are violated, (2) that legal provisions cannot be enforced and (3) that legal provisions are not fit for purpose to protect the fundamental right at stake. These legal problems may be caused by the AI disciplines *or* by the enforceable rights themselves when applied in the context of AI. Table 5.2 provides an overview of the legal problems identified in this chapter. The table illustrates the broad range of legal problems that arise or may arise in the context of AI. In total, twenty-five problems are identified.

[2134] Recital 7 GDPR.

Problem	Right	Type	AI Disciplines
Control	Informational privacy	1	ML, NLP, CV, AC, AR
Bodily information	Bodily privacy	1	ML (DL), AC
Mental information	Mental privacy	1, (3)	ML (DL), NLP, CV, AC
Speech analysis	Communicational privacy	1	ML, NLP, AC
Interception and identification	Communicational privacy	1	NLP
Keyword	Communicational privacy	1	NLP
Meaningless information	Access	1	ML (DL)
Information restriction	Access	2	ML, NLP, CV, AC, AR
Trade secrets	Access	2, 3	ML, NLP, CV, AC, AR
Logic and causal explanation	Access	3	ML, NLP, CV, AC, AR
Procedural autonomy	Rectification	1	ML, AC
Unverifiable data	Rectification	2	ML
Subjectivity	Rectification	2	AC
Verifiability standard	Rectification	3	ML, AC
Training data	Erasure	1, 2	ML
Erasure	Erasure	2	ML, AC
Transmission	Portability	2	ML, NLP, CV, AC, AR
Restricted scope	Portability	3	ML, NLP, CV, AC, AR
Continuance problem	Object	1	ML, NLP, CV, AC, AR
Erasure after objection	Object	3	ML, NLP, CV, AC, AR
Autonomous ADM	Automated decision-making	1	ML, NLP, CV, AC, AR
Intervention	Automated decision-making	2	ML (DL)
Cumulativeness	Automated decision-making	3	ML, NLP, CV, AC, AR
Opaque ADM	Automated decision-making	3	ML, NLP, CV, AC, AR
Procedural safeguard	Automated decision-making	3	ML, NLP, CV, AC, AR

Table 5.2 Overview of legal problems, enforceable rights concerned, type of legal problem (1, 2, 3) and AI disciplines concerned. The brackets surrounding DL indicate that this *specific kind* of ML causes the legal problem.

Regarding the *right to informational privacy*, I have identified one Type 1 legal problem when applied to AI. This problem constitutes an overarching issue. *All AI disciplines* introduced in Chapter 2 process various types of information beyond the control of the individuals concerned. It thus attacks the core of informational privacy which is to provide individuals with a form of informational self-determination, allowing them to exercise control over the collection, dissemination and use of their information. No Type 2 or 3 legal problems arise due to the broad scope of the fundamental right to privacy and the living instrument doctrine adopted by the ECtHR, which considers technological developments such as AI and the issues to which they may give rise.

Regarding the *right to bodily privacy*, I have identified one Type 1 legal problem when applied to AI. This problem relates to the AI disciplines *ML (particularly DL)* and *AC* which are highly dependent on bodily information, including its functions and either gain physical access to the body (e.g., implants) or derive information from it through non-invasive means (e.g., wearables sensing neural activity in the brain). Due to the broad scope of the fundamental right to privacy and the living instrument doctrine adopted by the ECtHR, no Type 2 or 3 legal problems arise.

Regarding the *right to mental privacy*, I have identified one Type 1 legal problem when applied to AI. This problem constitutes a major issue. *All AI disciplines (*except AR) facilitate access to mental states and information that might be derived from this, which means that the mind is no longer insusceptible to interferences. As such, the right to mental privacy is not yet recognised as a specific element falling under the notion of private life as enshrined in the fundamental right to privacy. However, the existence of the right to mental privacy could be derived from existing case law or developed in future ECtHR jurisprudence due to the broad scope of this right and the doctrine of living instruments. If not, there will also be a Type 3 legal problem which is indicated by the brackets surrounding the Type 3 problem as illustrated in Table 5.2.

Regarding the *right to communicational privacy*, I have identified three Type 1 legal problems when applied to AI. *NLP* is the main driver: All three legal problems relate to this AI discipline. This is not surprising because *NLP* aims to give machines the ability to process human language, which unavoidably involves the processing of communications. Two other AI disciplines, i.e. *ML* and *AC*, give rise to one Type 1 legal problem. Due to the broad scope of the fundamental right to privacy and the living instrument doctrine adopted by the ECtHR, no Type 2 or 3 legal problems arise.

Regarding the *right of access*, I have identified four legal problems of either Type 1, 2 or 3 when applied to AI. Table 5.2 shows that *all AI disciplines* are associated with these legal problems. This is mainly caused by the non-absolute nature of the right of access and trade secret protection for AI under the EU trade secrets directive (TSD). The broad scope of protection for AI under the TSD and restrictions to the right of access have severe effects on the entire data protection law regime because this right constitutes a conditio sine qua non for exercising other data subject rights.

Regarding the *right to rectification*, I have identified four legal problems of Type 1, 2 or 3 when applied to AI. All these problems relate to the AI disciplines ML and/or AC. This is mainly due to the unverifiable and subjective nature of the personal data generated by these two AI disciplines and the close connection with the right to rectification. Both ML and AC can generate inaccurate personal data, and the right to rectification grants data subjects the right to rectify inaccurate personal data.

Regarding the *right to erasure*, I have identified two Type 1 and/or 2 legal problems when applied to AI. ML is the main driver: All three legal problems relate to this AI discipline. As such, no Type 3 legal problems arise when the right to erasure is applied to the AI disciplines. This is mainly due to the broad wording contained in Article 17 (1) lit d GDPR[2135] which allows data subjects to request the erasure of personal data that 'have been unlawfully processed'.

Regarding the right to *data portability*, I have identified two legal problems when applied to AI: Types 2 and 3. Table 5.2 shows that *all AI disciplines* are associated with these legal problems. Both legal problems occur regardless of which *AI discipline* is applied to the right to data portability because the problems relate to the broad scope of protection for AI under the TSD and the restricted scope of this right. As such, no Type 1 legal problems arise when the right to data portability is applied to AI.

Regarding the *right to object*, I have identifed two legal problems when applied to AI: Types 1 and 3. Both legal problems occur regardless of which *AI discipline* is applied to the right to object. No Type 2 legal problems arise because data subjects can easily enforce their right to object, and the burden of proof is imposed on the controller if the latter intends to continue processing.

Regarding the *right not to be subject to ADM*, I have identified five legal problems when applied to AI: either Type 1, 2 or 3. Table 5.2 shows that *all AI disciplines* are associated with these legal problems, except for the Type 2 legal problem, which only relates to ML or, more specifically, to *DL*. All other legal problems are not caused by AI, but rather by the right itself: The right not to be subject to ADM suffers from significant flaws. The ambiguity and complexity of this right make it difficult to apply in practice.

In terms of the *types of legal problems* identified in this chapter, Table 5.2 shows that the total number of legal problems per type is almost evenly distributed. In total, there are eleven Type 1 legal problems, eight Type 2 legal problems and nine Type 3 legal problems. The almost equal distribution per type of legal problem underscores that the problems caused by AI are diverse, leading to situations in which the fundamental rights to privacy and data protection are violated, cannot be enforced or are not fit for purpose.

In terms of the *fundamental right to privacy*, a clear trend can be observed regarding the types of legal problem identified within this chapter: Only Type 1 legal problems occur. The fundamental right to privacy appears to be well equipped to protect privacy from the challenges and risks posed by AI.

[2135] Herke Kranenborg, Commentary of Article 17 in Christopher Kuner, Lee A. Bygrave, Christopher Docksey (eds), *The EU General Data Protection Regulation: A Commentary* (OUP 2020) 481.

This is mainly due to the broad scope of the right and the living instrument doctrine adopted by the ECtHR.

In terms of the *fundamental right to data protection* and the enforceable rights enshrined in the GDPR, no clear trend can be observed regarding the types of legal problems. There are five Type 1 legal problems, eight Type 2 legal problems and eight Type 3 legal problems. However, the finding that Types 2 and 3 legal problems occur just as often indicates two things: that there is an enforcement problem and that legislative measures and judicial action are needed to overcome the shortcomings of the current legal framework.

In terms of which AI disciplines cause *how many legal problems* when applied to the enforceable rights enshrined in the current legal framework, Table 5.2 shows that ML leads to twenty-two, NLP sixteen, CV thirteen, AC nineteen and AR twelve legal problems. The prominent role of ML is not surprising, as this AI discipline is the most widely used and often combined with other AI disciplines. In addition, AC seems to be the main driver of legal problems, as it causes only slightly less legal problems than ML. The total amount of legal problems associated to the AI disciplines NLP, CV and AR are almost evenly distributed.