FACULTY OF LAW

Lund University

Pia Friederike Bettelhäuser

AI & the Right to be Forgotten under the GDPR

JAEM01 Master Thesis

European Business Law

15 higher education credits

Supervisor: Prof. Xavier Groussot

Term: Spring 2022

Contents

Summary

The following thesis explores the interplay between Articial Intelligence and data protection under the General Data Protection Regulation. It addresses the difficulties and challenges that the use of new technologies in the digital age brings with it. The focus thereby lies firmly on the Right to be Forgotten, which was first recognised by the ECJ in 2010 and is now anchored in Art. 17 GDPR.

For this purpose, it is first explained what the term AI means and entails. It will become clear that the use of such technology is particularly dependent on large amounts of data from individuals and that the collection and processing of such personal data is at the heart of these techniques.

The European Union pursues a two-fold objective. On the one hand, the protection of fundamental rights, in particular the protection of personal data must be ensured, and on the other hand, innovation must not suffer, as it entails positive aspects and is essential for Europe's prosperity as well as its overall social welfare.

The paper further discusses the extent to which current legislation, especially the GDPR, provides sufficient safeguarding measures. The focus here is on the Right to be Forgotten. After looking at Article 17 of the GDPR, by explaining the grounds and exceptions under which an individual can in theory request erasure of his or her personal data, some technical implementation difficulties with regard to AI applications are illustrated.

The difficult question of the exact interpretation of the term personal data is also addressed. More specifically, it argues that it is currently difficult to classify training sets as personal data as such.

As it becomes clear that the GDPR contains certain weaknesses with regard to AI, some selected policy options will be presented as to how data protection can still be ensured in the future. Particular attention is paid to the draft legislation of the so-called AI Act.

It is important to emphasise that interdisciplinary research is essential in this context. If we as the European Union want to be properly positioned for the

future, this is only possible if technology and law are brought into harmony with each other. Technological progress and legislation must be aligned and compatible. They must mutually reinforce each other, rather than preclude each other.

Preface

Almost 1 1/2 years ago, when I wrote my letter of motivation for my application for a master's degree at Lund University, which I am now completing by submitting this thesis, I reflected on what the European Union means to me and why it was, and still is my personal desire and passion to study European Business Law. I wrote that I am of the opinion that the most urgent and challenging problems of our time cannot be solved without taking into account both an economic and legal perspective and that it is important to recognize and understand interrelationships and structures, to apply existing law to problematic situations and to consider how this law must develop in order to remain in line with the times and circumstances. I have confidently asserted that it is inevitable that new legal problems will arise and evolve in the future. And what is more to say, as that I have now written my master's thesis precisely on such a current topic, which raises ever more legal problems and questions in the globalised and digitalised world we live in.

I would be dishonest if I claimed that the studies now behind me, as well as the process of working on this thesis, were always easy. On the contrary, I was often stressed, felt overwhelmed and was sometimes frustrated. Either because I was not satisfied and too self-critical of myself and my work due to my honestly sometimes perhaps overly accentuated perfectionism. Or perhaps because I could not follow, grasp or understand a decision of the European Court of Justice or could not agree on an poorly presented or justified official statement of the EU on a specific topic, which is of importance to me and one that is close to my heart. But I realized that this might also be the beauty in it and what I have learned to love about my work. You don't always have to be of the same opinion, you not only can, but should have heated discussions and debates from time to time. That is the only way progress is possible. Progress and growth in a broad sense, globally, within the EU, but also on a personal level.

Sincere gratitude to all my professors and lecturers who have taught me and my fellow students this over the past year. Who encouraged us to think critically, pushed us to our limits, but also supported us with their knowledge and advice.
Special thanks in this regard to my brilliant professor and supervisor Xavier Groussot, whom I value and appreciate deeply, both personally and professionally, and who has always been there to give me advice, motivate and encourage me in what I am doing.
Last but not least, I like to thank my beloved family and my wonderful friends, who always seem to find the right words when I am - once again - stressed and desperate, who motivate and encourage me, and who believe in me in moments when I am certainly not believing in myself.
Thank you from the bottom of my heart.

Lund, 25 May 2022

Pia Bettelhäuser

Abbreviations

ADM	Automated Decision Making
AI	Artificial Intelligence
AI-HLEG	High Level Expert Group on Artificial Intelligence
APIs	Application Programmes Interfaces
CCPA	California Consumer Privacy Act
CJEU	Court of Justice of the European Union This refers to both Courts, the Court of Justice and the General Court. In the following also referred to as 'the ECJ' or the 'the Court'
DPD	Data Protection Directive (Directive 95/46/EC)
DPIA	Data Protection Impact Assessment
ECJ	European Court of Justice
EGC	European General Court
EU	European Union
GDPR	General Data Protection Regulation
MS	Member States
OECD	Organisation for Economic Co-operation and Development
SQL	Structured Query Language

1 Introduction

"*Nothing fixes a thing so intensely in memory as the wish to forget it*"[1]

At first glance, this quote by Michel De Montaigne may not appear to be very obvious and logical with regard to the Right to be Forgotten. The mentioned right, which is not only accepted by the CJEU[2] but since its introduction in 2018 also enshrined in the General Data Protection Regulation[3], takes up precisely where individuals wish to delete personal data and information concerning their person that was previously accessible to the public, thus rendering it invisible and forgotten.[4]
Yet, the reality is that we live in a world in which we are exposed to constant digital progress and in which especially Artificial Intelligence is deemed to be everywhere[5], not only affecting but also tremendously influencing and reshaping nearly every aspect of our lives.[6]

---

[1] Michel De Montaigne.

[2] The Court first acknowlged the existence of such a right in 2010 in the *Google Spain* Case. See Court of Justice of the European Union (2014) C-131/12 *Google Spain SL, Google Inc v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (*'Google Spain'*).

[3] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('*General Data Protection Regulation'*). In the following also referred to as '*GDPR*' or '*the Regulation'*.

[4] Eduard Fosch Villaronga, Peter Kieseberg, Tiffany Li,' Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) 34 Computer law & Security Review 304, 305.

[5] Sray Agarwal, Shashin Mishra, *Responsible AI: Implementing Ethical and Unbiased Algorithms* (1st ed Springer 2021) ch forword, V.

[6] Stephen Cave, Kanta Dihal, Sarah Dillon, 'Introduction: Imagining AI' In: *AI Narratives: A History of Imaginative Thinking about Intelligent Machines* (Oxford University Press; 2020:1-22) ch 1, <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198846666.001.0001/oso-9780198846666>, accessed 10.05.2022.

The notion of '*forgetting*' has fundamentally changed in the world of machine learning. It is questionable whether it is even technically feasible to be able to permanently delete data at all and whether this would not even be counterproductive in terms of stopping or at least retarding technical progress and innovation within Europe. Over-compliance in form of over-protectionism[7] may also result in the EU being left behind and unable to compete with other global powers such as the US and China in the so-called forth industrial revolution.[8]

It seems obvious that in such a technological century, known, but outdated concepts, which perhaps worked in the past, but which certainly are inadequate in regard to the nature of data flows and AI cannot succeed under the new prevailing conditions, should not and must not be sustained.[9]

Nevertheless, it must not be forgotten how essential and precious data protection is, especially in such times of constant digital progress. The use of Artificial Intelligence and automated decision-making mechanisms entails enormous risks that cannot yet be predicted and accurately estimated.[10]

Therefore it is crucial to address all associated risks and opportunities, in order to be well prepared for the future and tackle all the upcoming issues and difficulties. The overarching aim is to strike a balance between the chances and opportunities that the digital age might bring on the one hand,

---

[7] On the data protecionism debate see Alan Hervé in Shin-yi Peng, Ching-Fu Lin, Thomas Streinz (eds.), *Artificial intelligence and international economic law - disruption, regulation, and reconfiguration* (Cambridge University Press 2021) 195.

[8] M Rentzhog, 'The Fourth Industrial Revolution: Changing Trade as We Know It' (WITA 2019) <https://perma.cc/5NLX-L7VA> accessed 10.05.2022.

[9] Hervé (n 7) 197.

[10] See for example study of the EPRS (European Parliamentary Research Service, Scientific Foresight Unit (STOA)), 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020) 6; White Paper 'On artificial intelligence - A European approach to excellence and trust', Brussels, 19.2.2020 COM(2020) 65 final.

and the respect of fundamental rights on data protection and the protection of privacy on the other hand.

This paper aims to analyse the extent to which this has already been accomplished and displayed under current legislature and policy, and where remaining deficiencies still exist that the EU must address in the future.

For this purpose, the first part of the paper will clarify what is actually to be understood and covered by the concept of Artificial Intelligence and how it has developed. Followed by that, the objectives of the European Union in regard to the use of Artificial Intelligence are examined.

Subsequently, the intersection of AI and personal data and specifically with the GDPR will be outlined.

After a brief presentation of the General Data Protection Regulation, including its background and scope, and a brief overview of its content, the focus is directed to the Right to be Forgotten as one specific data subject right.

First, it will be explained how the respective right has developed. This is followed by a brief illustration of how it is now enshrined in the GDPR. The focus here will clearly be on the discussion concerning the difficulties in regard to both implementation and interpretation in relation to AI.

Finally, it is considered and examined how the Right to be Forgotten can be understood and applied in the future. In this context, some plans and upcoming initiatives of the law- and policy-makers of the European Union are outlined. An example of this is the proposal to introduce an AI Act, which is briefly presented with regard to its consequences for the RTBF.

Lastly, a brief conclusion on how it is possible to be prepared for the digital decade is drawn.

2 AI and Personal Data

2.1 What is AI?

2.1.1 Definition

In order to understand and assess the impact of Artificial Intelligence on the protection of personal data and thus achieve a satisfactory and secure handling of it, one must first understand what is meant by the term 'AI' and which applications are covered by it.

Many attempts to define the concept of AI have been made over time. Scholars, private and public organizations, as well as the European Commission, for instance, have published papers that attempt to enlighten the concept around the broad, fuzzy and vague term *'Artificial Intelligence'*. [11]

In the 1950s, John McCarthy, who is often referred to as one of the '*father[s] of Artificial Intelligence*'[12], defined AI as "*the science and engineering of making intelligent machines*"[13]. Marvin Minsky also uses the

[11] Agarwal/Mishra (n 5) ch forword, V. See also Mathias Avocats, 'Artificial Intelligence and the GDPR: how do they interact?' (2017); The European Commission´s High Level expert Group on Artificial Intelligence (*'AI-HLEG'*), 'A definition of AI: Main capabilities and scientific disciplines' (2018) 1.

[12] Artificial Solutions, 'Homage to John McCarthy, the Father of Artificial Intelligence (AI)' (2020), available at <https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence> accessed on 16.04.2022.

[13] Artificial Solutions (n 12).

term AI to describe "*the science of making machines do things that would require intelligence if done by men*"[14].[15]

Equally as the other mentioned attempts, the EU Commission's proposal for a definition[16] suggests that the concept implies the idea of technologies or systems enabling machines to perform tasks which are usually connected and performed by human intelligence. In order to analyse, and thus conceptualise and perceive its environment, these technologies rely primarily on the acquisition and processing of huge sets of personal data and derived information thereof.[17] This kind of technology is primarily used to mimic human behaviour and, in particular, the intelligent capabilities of the human brain, such as learning, reasoning, planning, problem-solving or identifying patterns. [18]

Underlying each action there is a specific goal which is to be achieved through specific measures. This may for instance involve either the interpretation of the data, the adjustment of the models further behaviour or the use of information in order to learn new things and thus change its further procedures.[19] This implies a certain degree of autonomy of the respective system.[20]

---

[14] Sibylle Peuker, 'Was ist Künstliche Intelliegnz (AI)' [engl. 'What is Artificial Intelligence (AI)?'] (zeix 2019) available at <https://zeix.com/durchdacht/2019/12/08/was-ist-kuenstliche-intelligenz-ai/#:~:text=Der%20AI%20Effekt,der%20Mensch%20Intelligenz%20brauchen%20w%C3%BCrde.%C2%BB> accessed on 22.04.2022.

[15] Agarwal/Mishra (n 5) ch forword, V.

[16] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final.

[17] These huge data sets are often referred as to 'Big Data'.

[18] Agarwal/Mishra (n 5) ch forword, V.

[19] The European Commission´s High Level expert Group on Artificial Intelligence ('*AI-HLEG'*), 'Ethical Guidelines for Trustworthy AI' (2019).

[20] COM (2018) 237 final (n 16).

Summarising, it can be seen that most definitions are based on the most prominent characteristics of Artificial Intelligence. These include concepts such as intelligence, machine-learning and the rationality of systems.[21] The reasoning module, with the aim of using the output for decision-making lies at the core of these AI systems.[22]
An revised and updated definition of the term 'AI', which attempts to represent and respect the current state of the art in the best possible way, has been proposed by the AI High Level Expert Group.[23] Looking at the corresponding definition, it is also noticeable that the scope of research in AI includes several approaches and techniques, such as machine learning, machine reasoning and robotics[24].[25] However, in regard to data protection, all of these techniques raise similar issues and problems, because all of them include the collection of personal data, which has been processed and act upon by intelligent systems[26]. Therefore, for the purposes of this paper, no distinction has to be made.

Even though, as seen above, several attempts have been made to describe and even define the notion of Artificial Intelligence, it has to be emphasized that no currently existing legislation on EU level includes a proper legal definition of the term.[27]
This can be criticised and should be changed as soon as possible as it makes the discourse around the topic enormously difficult.[28] The substantive

---

[21] Stuart Jonathan Russell, Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd edn, Prentice Hall Series, 2009); AI-HLEG, 'A definition of AI' (n 11) 3.

[22] AI-HLEG, 'A definition of AI' (n 11) 2.

[23] AI-HLEG, 'A definition of AI' (n 11) 7.

[24] The term 'robotics' is used when relating to 'AI in the physical world' or 'embodied AI'.

[25] EPRS study (n 10) 2; AI-HLEG, 'Ethical Guidelines for Trustworthy AI' (n 19) Glossary, 36.

[26] EPRS study (n 10) 3.

[27] Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts COM (2021) 206 final ('*AI Act*') 3.

[28] Agarwal/Mishra (n 5) ch forword, V.

dialogue around this topic, which tangents to all social, ethical and political issues[29], would be a more targeted one if all actors involved adopted the same definition and agreed on what was being talked about, as the term *'Artificial Intelligence'* forms the essential and central element of the discussion.

2.1.2 Development and importance of AI

"*Artificial Intelligence is everywhere*"[30] and the use of it can be considered as "*one of the most powerful drivers of the social transformation*"[31].
Artificial intelligence and automated decision making is not only omnipresent in technological societies[32], but is further changing economy, affecting politics, while reshaping citizens lives and interactions.[33] In other words, the use of AI already has great relevance in many fields of our lives and its importance and power will even continue to increase rapidly, if not exponentially, in the next few years.[34]
It is due to the current success of AI, based upon the fact that it seems to work efficiently[35], a trend towards increasingly automated decision making can be seen.[36]
Many companies are already implementing AI systems to fully take advantage of their benefits, to automate processes and optimise their

---

[29] Cave/Dihal/Dillon (n 6), ch 0.2.

[30] Agarwal/Mishra (n 5) ch forword, V.

[31] EPRS study (n 10) 1.

[32] Agarwal/Mishra (n 5) forword, p. V.

[33] EPRS study (n 10) 1 et seq.. See also Atomium European Institute for Science, Media and Democracy, 'AI4People´s 7 AI Global Frameworks' (2020) available at <https://www.eismd.eu/ai4people/> accessed on 10.05.2022.

[34] Fosch Villaronga/Kieseberg/Li (n 4) 304.

[35] EPRS study (n 10) 4.

[36] Paul De Hert, Ronan Hanon, Henrik Junklewitz, Gianclaudio Malgieri, Ignacio Sanchez,'Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making' (2022) IEEE computational intelligence magazine, 73-85, 73.

business. But also for the European Union, the increasing deployment of AI seems to be desired as it as it strives to achieve a leading position in form of 'Digital Sovereignty' in order to remain competitive, especially vis-à-vis the United States and Asia.[37]

2.1.3 EU objectives regarding the development and deployment of AI

Considering the great legal and social importance, the EU has to be aware of both risks and opportunities relating to the use of AI. Striking an appropriate balance between those, should therefore be one of its priorities and can be achieved by developing and establishing appropriate policies and regulations in this field.[38]

One of the overarching objectives can be seen in the design of an ethical and legal framework, which focuses on AI to be human-centred. [39]
As outlined in its White Paper[40], the Commission states that it pursues two parallel objectives. On the one hand the European Union aims for the promotion of the research and deployment of AI, in order to ensure its own competitiveness vis-à-vis the United States and China. On the other hand, this must be achieved in consistency and, above all, with respect for the Unions fundamental rights as well as social values. Those objectives seem to be distinct. This is why many consider the effective and fair

[37] EPRS study (n 10) 7-8.

[38] EPRS study (n 10) 1.

[39] Corinne Cath, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, Luciano Floridi, 'Artificial Intelligence and the 'Good Society': the US, EU, and UK approach' (2018) Sci Eng Ethics 24, 505–528. For a review of documents on AI ethics and policy see Anna Jobin, Marcello Ienca, Effy Vayena, 'The global landscape of AI ethics guidelines' (2019) Nat Mach Intell 1: 389–399 <https://doi.org/10.1038/s42256-019-0088-2>.

[40] COM(2020) 65 final (n 10). In this regard see also European Council, European Council meeting (19 October 2017).

administration and development as "*one of the great challenges of our time*"[41]. However, these objectives are compatible.[42]

The paper thus examines some of the current issues and attempts to show possibilities and approaches to cope with this field of tension. For meeting these legitimate interests in a fair and equitable manner and to allow sustainable success and impact, the trust in safe technology will be a key factor. The establishment of such an '*ecosystem of trust'* requires the citizens confidence to take up and use AI applications as well as legal certainty for companies and public organisations to innovate in AI.[43]

2.2 AI and Personal Data

2.2.1 Personal data as valuable commodity

Many AI applications involve the massive processing and analysis of personal data.[44] Algorithms and other AI systems strongly depend on big data sets to function and work properly.[45] If one considers this dependency, it quickly becomes clear that personal data becomes a valuable commodity, that can be used to analyse, forecast and even influence human behaviour. Hence, it becomes a valuable good, which can be traded with, gains a market value and thus becomes attractive for many tech companies.[46]

---

[41] Philipp Hacker, 'A legal framework for AI training data—from first principles to the Artificial Intelligence Act', (2021) Law Innovations and Technology vol. 13 no. 2, 257, 257 <https://doi.org/10.1080/17579961.2021.1977219>.

[42] EPRS study (n 10) 7-8.

[43] ibid.

[44] EPRS study (n 10) 1.

[45] Tuulia Karjalainen, 'All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm'(2022) EDPL 1/2022, 27; Robert Nisbet, Gary Miner and Ken Yale, *Handbook of Statistical Analysis and Data Mining Applications* (1st edn, Elsevier 2018) 39.

[46] OECD, 'Exploring Data-driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data" ' (2013) OECD Digital Economy Papers no. 222 available at < Big Data"", OECD Digital Economy Papers, No. 222

In times of big data, the processing of data can be the core of a business idea. This is a significant shift from other, more traditional data processing in a smaller context. In the latter the data processing could be seen as more of a side effect of other activities.[47]

But not only personal data of individuals are offered and sold commercially. The trade of already trained sets and algorithms[48], either in form of the licensing of application programmes interfaces or as the trading of packaged models, also offers a highly lucrative business model for many companies.[49] The observation that personal data is a valuable commodity is also strengthened by the so-called '*big data paradigm'* narrative, that promotes the processing of personal data in the interest of technological progress as its result.[50]

<http://dx.doi.org/10.1787/5k47zw3fcp43-en >; Cédric Villani, Marc Schoenauer, Yann Bonnet, Charly Berther, Anne-Charlotte Cornut, François Levin, Bertrand Rondepierre, 'Donner Un Sens a` l'Intelligence Artificielle. Pour Une Stratégie National et Européenne' [engl. 'Giving meaning to artificial intelligence: for a national and European strategy'] (2018) available at <https://perma.cc/SLC9-AMNZ> accessed on 16.05.2022; EPRS study (n 10) 22.

[47] Karjalainen (n 45) 27-28.

[48] e.g. for tasks like face recognition, emotion classification, etc.

[49] OECD, *Data-driven Innovation: Big Data for Growth and Well-being* (2015) 76; Michael Veale, Reube Binns, Lilian Edwards, 'Algorithms that remember: model inversion attacks and data protection law' (2018) Phil. Trans. R. Soc. A <https://doi.org/10.1098/rsta.2018.0083> 3-4.

[50] Joseph Alhadeff, Brendan van Alsenoy and Jos Dumortier, 'The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions' in Carla Ilten, Inga Kroener, Daniel Neyland, Hector Postigo, D Guagnin, and L Hempel (eds.) 'Managing Privacy through Accountability' (Palgrave Macmillan 2012) 49; Karjalainen (n 45) 27.

2.2.2 Opportunities and risks of AI

As mentioned briefly above, the development and use of AI systems involves both opportunities and risks at the same time.[51]

The overarching goal and probably the greatest advantage is that it is expected to be capable of contributing to an increase in general social welfare and might lead to benefits for the society as a whole.[52] Among others the development and deployment of AI may entails the enhancement of human abilities, improvement of security and efficiency, economic, social, and cultural development, energy sustainability, better health care, while also enabling and spreading universal knowledge and skills.[53]

Also in regard to the EU objective to obtain digital sovereignity, digital technologies, including AI are essential. They even have the potential to significantly contribute to the protection and promotion of fundamental rights, democracy and the rule of law."[54]

However, beside all these great opportunities and chances, the innovation and the use of AI applications, also bears serious risks and novel disruptive outcomes. According to a study initiated by the European Parliament[55], examining the impact of the GDPR on AI, these include for example the increasing opportunities for control, manipulation and discrimination, unequality, unemployment and (human) harm, which result from technological failures. Moreover, social interaction might get disrupted or possibly even worse, controlled. Artificial Intelligence may have the

[51] Gabriele Mazzini, 'A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law' in Alberto De Franceschi, Reiner Schulze (eds), *Digital Revolutions – New challenges for Law* (C.H. Beck, 2019) 3-4.

[52] De Hert et al (n 36) 73.

[53] See for example EPRS study (n 10) 6; COM (2020) 65 final (n 10).

[54] European Council, Presidency conclusions – 'The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change' 11481/20 (2020), Annex, 3, para 4.

[55] EPRS study (n 10).

consequence that individual rights and social values are completely disregarded.[56]

In this context, a striking illustration of the dangers of profiling[57] was provided by the Cambridge Analytica case.[58] The case was concerning massive processing of data, which was used in order to build a training model, which made predictions about psychology and political preferences solely based on personal information gained through a individual test paired with facebook data. With the predictions provided by the model, the available data was then extended to people, who did not even took part in the questionnaire. The attempt was to influence voting behaviour both in the US elections in 2016, as well as in the Brexit referendum, by targeting voters, who potentially are likely to change their voting behaviour, for example with personalised policial ads.[59]

The field of tension between the chances and risks, which are still difficult to assess, but within the contexts of which a lot of commercial activity, that bases on the possibility of observing every human behaviour, is already taking place and in which new models of social and economic interaction become possible, also addresses the discussion on the so-called 'surveillance capitalism' or 'surveillance state'.[60] This kind of surveillance capitalism is

---

[56] EPRS study (n 10) 7.

[57] Art. 4 (2) GDPR: *"'profiling' means 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, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"*.

[58] cf. EPRS study (n 10) 23 ff.

[59] On the problems related to disinformation and propaganda, see Judit Bayer, Natalija Bitiukova, Petra Bárd, Judit Szakács, Alberto Alemanno, Erik Uszkiewicz, 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its member states', Study, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament (2019).

[60] cf. EPRS study (n 10) 25 ff.

often referred to as the leading economic model of the present age.[61] An analysis by the historian Karl Polany[62] shows that capitalism also treats things and entities, which are initiallly not produced for the market as commodity. Human life or experience, including personal data, as a marketable opportunity to anticipate and influence human behaviour, is therefore seen as establishing a fourth 'fictional commodity'. This clearly changed the former dynamics of capitalism.[63]

In contrast to the other, earlier commodities, it is still in this sector that the produced disruptive tensions are only partially and still not adequately addressed and developed in law and other countervailing forces. This could possibly be done through political and social measures, which attempt to prevent, counteract, moderate or mitigate by additional and stronger regulation.[64] Nevertheless, a positive trend can be observed. All over the world, new legislation and standards are being passed that aim to balance those risks and opportunities, mainly by protecting personal data of individuals.[65] Examples of this are the CCPA[66] in the USA or the GDPR in Europe, which is discussed in more detail below. In the context of the latter, the aspects that are still only incompletely regulated and do not yet represent sufficient protection in relation to AI, are examined.

---

[61] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019); Julie E. Cohen, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

[62] Karl Polanyi [1944], *The Great Transformation* (Beacon Press 2001).

[63] Polanyi (n 62); Zuboff (n 61): See also EPRS study (n 10) 26.

[64] Zuboff (n 61) 507.

[65] EPRS study (n 10) 26; Zuboff (n 61).

[66] California Consumer Privacy Act (2018).

2.3 Respect of fundamental rights, legal and ethical principles

The EU, which identifies and describes itself as a '*Union of values*'[67] needs to ensure that the development and deployment of AI takes place within a sociotechnical framework, which recognises and ensures the preserving and enhancement of individual interests and social goods.[68]

Compliance with ethical standards as well existing legal norms and principles is elementary in this respect.[69] Legal principles are necessary and crucial.[70] Those principles include, in particular, fundamental rights and social values, both at an ethical and legal level.[71]

In legal terms, the Charter of Fundamental Rights[72] at EU level and national constitutions are particularly important and influential. With regard to the rights enshrined in the Charter, Art. 7 and 8, which govern the respect for private and family life and the protection of personal data[73], are certainly the most striking and noticeable provisions, which are of particular relevance in the context of AI.[74] However, also other articles and provisions have to be borne in mind, which have the protection of similar values at their core. Noteworthy are, among others Art. 1 (human dignity), Art. 10 (right to liberty, security, freedom of thought, conscience and religion), Art. 11 (freedom of

---

[67] European Council, Presidency conclusions 11481/20 (n 54) Annex, 3. See also Art. 2 TEU.

[68] EPRS study (n 10) 30, see also European Council, Presidency conclusions 11481/20 (n 54) Annex, 3.

[69] European Council, Presidency conclusions 11481/20 (n 54), Annex, 10.

[70] cf. Paul Craig, Gráinee De Búrca, *EU Law - Text, Cases, and Materials* (7th edn, Oxford University Press 2020), 414 et seq.

[71] EPRS study (n 10) 30-34.

[72] In the following also referred to as *'the Charter'* or *'CFR'*.

[73] Note also Art. 8 ECHR and Art. 16 (1) TFEU which establish the same right.

[74] European Union Agency for Fundamental Rights (FRA), 'Getting the future right – Artificial Intelligence and Fundamental Rights' (2020) 61-62.

expression and information), Art. 12 (freedom of assembly and association), Art. 21 (right to non-discrimination) and Art. 38 (consumer protection).[75]

In addition to these individual rights, social norms and values are also of great importance. These include for example democracy, welfare, peace, competition, social dialogue efficiency, advancement in science, art and culture, cooperation, civility and security.[76]

The collection, processing and use of data is tangential to many different areas of law and thus is an illustrative example of how modern technologies interfere and possibly collide with the law. [77]
Many domains such as consumer protection, competition law, labour and anti-discrimination are involved as well.[78] Nevertheless, the processing of data above all raises serious questions and problems regarding fundamental rights of privacy, personal data protection and non-discrimination.[79]
This paper focuses henceforth mainly on the relationship and interaction between AI and data protection law.

---

[75] FRA (n 74), 61.

[76] EPRS study (n 10) 31-32.

[77] Karjalainen (n 45) 27; Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*
(First Mariner Books 2015) 173-174.

[78] EPRS study (n 10) 32.

[79] Fotios Fitsilis, *Imposing Regulations on Advanced Algorithms* (Springer 2019) 13; Fabienne Ufert: 'AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?', European Papers vol. 5 no. 2 (2020) <https://www.europeanpapers.eu/en/europeanforum/ai-regulation-through-the-lens-of-fundamental-rights> accessed 16.05.2022.; Ryan Calo, 'Peeping HALs: Making Sense of Artificial Intelligence and Privacy' (2010) European Journal of Legal Studies 2, 3, The Future of... Law & Technology in the Information Society, available at <http://hdl.handle.net/1814/15123171> accessed 16.05.2022; Luisa Marin, K. Kraijciková, Deploying Drones in Policing Southern European Border: Constraints and Challenges for Data Protection and Human Rights, in A. Zavrsnik (ed.), Drones and Unmanned Aerial Systems (Springer 2016), 101.27.

Regulatory initiatives are an essential element, in order to effectively ensure the protection of citizens' rights.[80] In this respect, the Commission published a White Paper on Artificial Intelligence[81] in 2020, which forms the basis for specific regulation of techniques and applications of AI at EU level.[82]

There are also various initiatives that address this very subject. In addition, the European Commission has set up an independent group of experts to assess the impact of AI on European law and the resulting social, political and legal measures that need to be taken. [83]

According to the Ethical Guidelines for trustworthy AI[84], published by the High-Level Expert Group on Artificial Intelligence, the foundation of legal, ethical and robust AI should be grounded on fundamental rights and should reflect four ethical principles. Namely, the respect of human autonomy, the prevention of harm[85], fairness[86] and explicability, which involves the need for transparency, meaning that such systems and automated-made decisions can be communicated and explained to those affected.[87]

Beyond that, AI4People[88] has published several reports, which provide an ethical framework for trustworthy AI and guidance on how to fairly and

---

[80] EPRS study (n 10) 33.

[81] COM(2020) 65 final (n 10).

[82] Hacker (n 41) 258.

[83] The so-called High Level Expert Group on Artificial Intelligence ('AI-HLEG').

[84] AI-HLEG, 'Ethics Guidelines for Trustworthy AI' (2019).

[85] Including respect of human dignity and mental and physical integrity.

[86] Both at a substantive and procedural level.

[87] AI-HLEG, 'AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018).

[88] AI4People was initiated and launched at a Atomium – EISMD initiative in February 2018. It is a form of multi-stakeholder (with the EU Parliament with one of its first members) forum, which aims to bring together all actors interested in shaping the social impact of new applications of AI. 6 months later the AI-HLEG was established. Many of the scientifics, who were already engaged in AI4People, became part of the new expert group <https://www.eismd.eu/ai4people/> accessed on 23.04.2022.

efficiently design the development and implementation of new regulation on AI.[89]

[89] e.g. AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations (2018); Report on Good AI Governance: 14 Priority Actions, a S.M.A.R.T. Model of Governance, and a Regulatory Toolbox (2019); AI4People´s 7 AI Global Frameworks (2020); 5 AI4 People´s conversation (2022) <https://www.eismd.eu/ai4people/> accessed on 23.04.2022.

3 AI and the GDPR

The following chapter will provide an overview of the GDPR. The above-mentioned interplay between AI and the protection of personal data will then be further explored in its respective scope of application. Subsequently, potential difficulties that might arise regarding the application of the regulation in connection with the use of AI are examined. It raises the question of whether the GDPR provides sufficient safeguarding measures and thus protection for individuals in this technological era. Moreover it is to be examined whether all crucial provisions of the GDPR can be applied in the context of AI applications and unfold its full intended effect. However, conceivable possibilities of how the GDPR may influence the further development of AI will also be highlighted.

3.1 General Data Protection Regulation

3.1.1 Background

Even though the 1950 European Convention on Human Rights already referenced to some sort of right to privacy,[90] it can be said that the real beginning of Data Protection Law within the European Union dates back to the 1970s and 80s. The main reason for the upsurge in awareness was the notable technological progress during these times. First ideas and legislation were mostly concerned with technology regulation as their main objective. At first, only national laws existed to provide regulatory frameworks within this novel, rapidly-evolving field. It was not until 1995, with the introduction of

[90] "*Everyone has the right to respect for his private and family life, his home and his correspondence*."; cf GDPR.EU, 'What is GDPR, the EU's new data protection law?' available at <https://gdpr.eu/what-is-gdpr/#:~:text=The%20regulation%20was%20put%20into,tens%20of%20millions%20of%20euros.> accessed on 29.04.2022.

Directive 95/46/EC[91], that the first legislation was introduced at Union level.[92] This was accompanied by the establishment of an EU cooperation mechanism, namely the Article 29 Working Party.[93]

In 2016 after more than 20 years without any reform of the existing data protection regime, the General Data Protection Regulation was passed, repealing Directive 95/46/EC.[94] The Regulation was put into effect on, and hence applies since May 25, 2018.[95]

Forming the key act of the EU´s secondary law *acquis communautaire* regulating personal data protection[96], the GDPR regulates the protection of personal data of natural persons[97], by setting a uniform standard of data protection within the Member States of the European Union and ensures the free movement of data between MS.[98]

The novel Regulation was promoted as "*a revolution bringing EU data protection law to the 21st century through the creation of rules fit for the digital age*"[99]. This innovation was primarily motivated and based on the fact

---

[91] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ('*DPD*')

[92] Helena U. Vrabec: *Data Subject Rights under the GDPR* (Oxford Scholarship Online 2021) <DOI:10.1093/oso/9780198868422.001.0001>, 9-10.

[93] EDPB, Article 29 Working Party <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en> accessed on 10.05.2022. Since 2018: European Data Proection Board (EDPB).

[94] Krzysztofek, Mariusz, *GDPR: data protection in the European Union* (Kluwer Law International, 2021) 13.

[95] GDPR.EU (n 90).

[96] Krzysztofek (n 94) 13.

[97] It should be emphasised that the regulation does not apply to legal persons. Cf Krzysztofek (n 94) 13-14.

[98] Art. 1 GDPR.

[99] European Commission 'Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation' (2018) STATEMENT/18/3889

that new technologies and the significant development and dynamic progress of the digital age require new, modified rules and laws in order to ensure that the values and rights to be protected continue to be adequately safeguarded and that upcoming developments are sufficiently anticipated.[100] In particular, it should be ensured that the challenges of modern large-scale online processing to data protection are possible to be tackled in the future.[101] This should also regain the formerly, temporally weakened level of trust of citizens towards the massive data processing of big organizations in the online world and strengthen it for the future.[102]

The GDPR is fundamentally based on the previous model, aiming to protect equal fundamental rights as under Directive 95/46/EC, while as already mentioned, its content has been significantly updated, modernised and reinforced. It clearly addresses social and technological challenges which arise from the application of those new technologies.[103] Nevertheless, it must be emphasised that, possibly contrary to some perceptions, the GDPR has not introduced any new or more stringent measures and obligations in comparison to the Directive. In fact, some provisions have been even weakened under the GDPR.[104] The implementation of this new regulation constitutes yet a milestone in the history of data protection and is for instance also of great importance in that many rules and principles are now more clearly and unambiguously defined and addressed.[105]

<https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889)> accessed on 10.05.2022.

[100] EDPB <https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en.> accessed on 10.05.2022.

[101] Karjalainen (n 45) 19.

[102] European Commission Special Eurobarometer 431 'Data Protection' (2015) available at: <https://data.europa.eu/data/datasets/s2075_83_1_431_eng?locale=en> accessed on 10.05.2022; European Union Agency for Fundamental Rights Fundamental Rights Report, *Data protection and privacy* (2020).

[103] Krzysztofek (n 94) 13-14.

[104] Krzysztofek (n 94) 15.

[105] Krzysztofek, (n 94) 15.

The fact that data protection has become much more relevant in the EU over the past decades and has been massively strengthened is also reflected in the decisions of the ECJ. An example for this is the judgment in the *Digital Rights Ireland* case[106]. The milestone decision concerned the validity of the Data Retention Directive in light of EU law, in particular Art. 7, 8 and 11 of the Charter. In its judgment the Court held, that the respective directive violated the rights of privacy and data protection enshrined in the CFR.[107] Positively, the judgment recognises the danger of data retention and sets out that personal data has to be protected. Limitations to this are only permissible, when clear and precise safeguarding measures are included and described within the provision.[108] Therefore, the case can be seen as strongly strengthening individual data protection rights by acknowledging the risks and danger of unregulated or too extensive data retention.[109]

That the GDPR enjoys enormous global awareness and far-reaching impact beyond the borders of the Union, as the most prominent legislation in the field of data protection,[110] is demonstrated, among other things, by the fact that the uniform standard introduced by the GDPR has also been adopted by

---

[106] Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others [2014] (*'Digital Rights Ireland'*).

[107] Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States', Harvard Human Rights Journal vol. 28, 65, 65.

[108] *Digital Rights Ireland* (n 106) para. 54.

[109] Orla Lynskey, 'Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly', available at <https://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/> accesssed on 08.05.2022.

[110] Vagelis Papakonstantinou and Paul De Hert, 'Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI' (2021), available at <https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/> accessed on 10.05.2022

some third countries[111] in the form of national law.[112] This equal standard of protection[113] is, however, not shared by all major global players. The US and China, for example, set different data protection standards.[114] As this can be of major concern in a digital global world, where national borders are hardly applicable, for example, to server ranges or internet sites, it is important to be able to capture the scope of the GDPR precisely.[115]

3.1.2 Overview

The key objectives of the GDPR are laid down in Art. 1 GDPR. The Regulation lays down rules to protect individuals in regard to personal data processing and establishes the free movement of data within the Union. [116] According to Art. 3 GDPR, it applies to controllers or processors, when established within the EU (Art. 3 (1) GDPR) or when the processing relates to data subjects in the EU (Art. 3 (2) GDPR), meaning that controllers or processors outside the EU can, under certain circumstances, be subject to the GDPR too.[117]

Such an extraterritorial effect demonstrates the global significance of the statute.[118] As many processors or controllers in form of big technology firms have their company seat outside the EU´s territory, it would deem impossible for the GDPR to unfold its effects outside its borders, meaning to sufficiently protect personal data of European citizens.[119]

---

[111] Including countries like Argentina, Canada, Israel, Japan, New Zealand, Switzerland, Uruguay, etc..

[112] cf Frederik J Zuiderveen Borgesius, 'Improving Privacy Protection in the Area of Behavioural Targeting' (PhD Thesis, University of Amsterdam 2014) 88 and 133.

[113] cf. Art. 45 (1) GDPR.

[114] Krzysztofek (n 94) 16-17.

[115] See discussion concerning the geographical scope of application below under 3.1.2.

[116] Krzysztofek (n 94) 13.

[117] Veale/Binns/Edwards (n 49) 2; Interview Avocats (n 11).

[118] Art. 83 GDPR; Hervé (n 7) 203. See also Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).

[119] Paul M. Schwartz, 'Global Data Privacy: The EU Way'

The question regarding the given level of protection in third countries was for instance also subject to the *Schrems* case[120], which examined the legality of the transfer of personal data to third countries, in this case the US. The Court held, that personal data of a person in the territory of the EU may only be transferred to third countries, if they enjoy an essentially equivalent level of protection as in the EU.[121] In this respect, the Court emphasised the data exporters responsibility. Namely, the exporter must assess the level of protection that prevails in the respective third country and to which the data is to be transferred for each transfer of data.[122] Additionally he has to ensure, that appropriate safeguards for the data protection exist.[123] If this cannot be ensured, the data transfer is to be suspended or terminated.[124]

This shows that the GDPR has strong leverage even beyond European borders, especially in the big data context, which hardly knows any geographical frontiers and where data seems to flow freely across the world. The enormous scope of influence of the regulation is highly apparent in this context.

The material scope of application encompasses the processing of personal data.[125]

(2019) 94 NYU Law Review 771. For a discussion of the GDPR's limits see judgement in Case C-507/17 *Google LLC, v. Commission nationale de l'informatique et des liberte´s* [2019] ECLI:EU:C:2019:772 (*'CNIL'*).

[120] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559 ('*Schrems*').

[121] BfDI, 'Praktische Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II")'<https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html> (accessed on 08.05.2022).

[122] *Schrems* (n 122) para 134.

[123] *Schrems* (n 122) para 131.

[124] BfDI (n 121).

[125] Ufert (n 79) 1087-97.

The term '*personal data*' covers "*any information relating to an identified or identifiable natural person […]*".[126] According to Art. 4 (2) GDPR the term '*processing*' includes "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means […]*", thus also implies things like the collecting, transforming, consulting and erasing of personal data.[127]

The rules and obligations, which are imposed by the GDPR, must be complied with by the person or entity, that controls or processes the personal data. In this context a '*controller*' is defined as "a *natural or legal person, public authority agency or other body which […] determines the purposes and means of the processing of personal data […]"* in Art. 4 (7) GDPR. The person or body which "*processes personal data on behalf of the controller*", on the other hand, is referred to as '*processor*'.[128]

The corresponding definitions, as well as other definitions of terms, which are of relevance to the understanding of the regulatory framework, are to be found in Art. 4 GDPR.

Especially in relation to the use of Artificial Intelligence in some systems, these given definitions raise some uncertainties and questions in relation to their exact and appropriate interpretation, which will be addressed in the following in more detail.

3.2 AI in the conceptional framework of the GDPR

When drafting the GDPR, the legislator put the focus primarily on challenges regarding and emerging from the internet. In contrast to the previous Directive 95/46/EC, the Regulation therefore introduced and does

[126] Art. 4 (1) GDPR.

[127] Veale/Binns/Edwards (n 49) 2; note that there are further exapmples named in Art. 4 (2) GDPR.

[128] Art. 4 (8) GDPR.

now contain references to the '*internet*' and some relating terms. The topic around AI was, however, quite new and still underdeveloped at that time and only acquired social significance in the most recent years. For that reason the GDPR does not contain the term '*Artificial Intelligence'* or any other term relating to this concept.[129] Nevertheless, it can be noted, that the EU has utilised the Regulation to set out and codify its vision and objectives for the upcoming years with regard to Automated Decisions-Making[130] and AI. These must be reliable and designed in a human-centred way.[131]
Even if this may not have been intended or considered by the legislator at the time, when the regulation was drafted and released, some of the provisions of the GDPR are of tremendous relevance also with regard to AI.[132]
To what extent the use of AI creates implications to data protection and in how far the regulations of the GDPR in its current form apply, both directly and indirectly, to these situations, will be examined in more detail below. The following chapter will further discuss the interaction between those two topics.
The huge amount and volume of data, but also the way it is generated and processed, can raise various socio-technological difficulties and make it challenging to apply data protection principles in a big data context.[133] Furthermore it may bear unexpected consequences for individuals.[134] Oftentimes, the use of AI and ADM will result in high risk to individuals

---

[129] EPRS study (n 10) 35.

[130] Also referred to as *'ADM'*.

[131] Francesco Sovrano, Fabio Vitali, Monica Palmirani, 'Modelling GDPR-Compliant Explanations for Trustworthy AI' in *Electronic Government and the Information Systems Perspective* (Springer International Publishing 2020) 1.

[132] EPRS study (n 10) 35.

[133] Veale/Binns/Edwards (n 49) 12.

[134] Huntonrivacyblog, 'CIPL Submits Comments to Article 29 WP's Proposed Guidelines on ADM and Profiling' (2017) <https://www.huntonprivacyblog.com/2017/12/08/cipl-submits-comments-article-29-wps-proposed-guidelines-adm-profiling/> accessed 23.04.2022.

rights and freedoms. Companies, who work with or apply AI technologies are therefore legally required to implement some safeguarding measures. For instance, they are required to assess whether and to what extent they have to comply with GDPR provisions and implement "*appropriate technical and organizational measures*"[135] to ensure compliance with the Regulation's requirements. This may include things like encryption or pseudonymisation.[136]. The appropriateness of such measures depends on the included risks. If the processing is likely to result in high risk to individuals rights, a data protection impact assessment has to be carried out.[137] Moreover it is important to understand how data may influence the behaviour of a AI system.[138]

However, it is important to note that compliance with data protection does not only include numerous legal requirements, which could be seen as a burden to comply with by companies. Rather it brings many advantages and chances. For instance, it may encourage innovation and creativity and also have positive impacts on data quality, which is becoming increasingly crucial in the big data context.[139]

---

[135] cf. Art. 24 GDPR.

[136] Avocats (n 11).

[137] cf Art. 35 GDPR. Art 29 WP also published guidelines regarding data protection impact assessment; Interview Avocats (n 11); Clare Sellars, 'ICO launches guidance on AI and data protection', C.T.L.R. 2021, 27 (1), 1.

[138] AI-HLEG, 'A definition of AI' (n 11) 6.

[139] ICO, 'Big data, artificial intelligence, machine learning and data protection' (Version 2.2) para 212 available at <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed on 16.05.2021.

3.3 Data protection principles, legal bases and data subject rights

The GDPR provides some constraints for the processing of personal data. Exemplified, there is the need for a legal basis for any processing of personal data, obligations concerning information and transparency, limitations on profiling and automated decision-making and requirements on anonymisation and pseudonymisation.[140]

These various rules and measures, that act predominantly as safeguards, are presented below.

3.3.1 Data protection principles

The General Data Protection Regulation is fundamentally built on a set of principles that form the basis of other provisions of the Regulation. Those data protection principles are set out in Art. 5 (1) GDPR.[141] The Article specifically enshrines the principles of transparency and fairness (Art. 5 (1) (a) GDPR), purpose limitation (Art. 5 (1) (b) GDPR), data minimisation (Art. 5 (1) (c) GDPR), accuracy (Art. 5 (1) (d) GDPR), and storage limitation (Art. 5 (1) (e) GDPR).

3.3.2 AI and legal bases

As stated in Art. 6 GDPR, any processing of personal data must be based on a legal basis. At least one of the conditions listed in paragraph 1 of the respective Article must be met in order to be lawful. In total, there are six grounds of processing, which work as a legal basis.[142]

Data processing is lawful, if it is either based on the consent given by the data subject (Art. 6 (1) (a) GDPR) or if it is based on necessity. The latter is

---

[140] EPRS study (n 10) 30.

[141] EPRS, study (n 10) 44 ff.

[142] huntonprivacyblog.com (n 134).

covered by Art. 6 (1) (b) – (f) GDPR. It is permitted to process personal data if the processing is necessary in order to perform or enter into a contract (Art. 6 (1) (b) GDPR) or for *"[complying] with a legal obligation to which the controller is subject*" (Art. 6 (1) (c) GDPR). Even if necessary for *"[protecting] the vital interests of the data subject or of another natural person",* the processing may be lawful according to Art. 6 (1) (d) GDPR. Furthermore lawfulness of the processing is given, if it is based on the necessity for performing "*a task in the public interest or in the exercise of a public authority vested in the controller*" (Art. 6 (1) (e) GDPR) or if the processing purposes a "*legitimate interest pursued by the controller or by a third party*", if not overridden by other fundamental rights or interests by the data subject (Art. 6 (1) (f) GDPR).[143]

3.3.3 Data subject rights

By introducing a separate chapter on data subject rights, the GDPR transferred more control over their personal data to individuals. In terms of valuing and highlighting individual rights, the Regulation can thus be described as "*one of the most far-reaching developments*" in the modernisation of data protection law.[144]

These data subject rights are enshrined in Chapter 3 of the GDPR, and are forming the core of the data protection law.[145] Among others, these include the Right to information, the Right to object and the Right to access, which are all of great importance.

In the following, however, this paper will mainly focus on the Right to be Forgotten. Accordingly, other rights will not be explained and evaluated in detail.

---

[143] EPRS study (n 10) 49 ff.

[144] Vrabec (n 92) 105; Viviane Reding, 'Your Data, Your Rights: Safeguarding Your Privacy in a Connected World' (Speech delivered at Privacy Platform 'The Review of the EU Data Protection Framework' (Brussels 16 March 2011).

[145] Zuiderveen Borgesius (n 112) 88 and 133.

Still, because highly relevant within a machine-learning environment, Art. 22 GDPR has to be emphasised. This Article has to be interpreted as a right not to be subject solely on automated decision making, which produces legal effects or similarly significant effects. Yet this does not mean that ADM is prohibited per se. If the conditions of one of the six legal bases are fulfilled, the processing of data by machines is permitted. Nevertheless, it is noteworthy that it has to be ensured that the automated process is accurate and correct and that the decision based upon this was made fairly.[146]

[146] huntonprivacyblog.com (n 134).

4 AI and the Right to be Forgotten

4.1 Overview of the RTBF

The Right to be Forgotten is linked to the concept of '*data deletion'*. Simplified it means that individuals (data subjects) have the right to request deletion of their data, that has been collected by others (data controller).[147]

There are several fundamental values underpinning the RTBF. The right is an expression of privacy, data protection and autonomy.[148] It even reflects an important aspect of human dignity, as it addresses the protection of consumers against commercial exploitation by data processing entities, which tend to increasingly treat people as objects rather than subjects.[149]

The Right to be Forgotten, as an instrument of control[150], strongly relates to the notion of a person's autonomy and forms the "*heart of informational self-determinisation*"[151] as the active side of privacy. The individual should have

[147] Fosch Villaronga/Kieseberg/Li (n 4) 305. This definition referres to the RTBF in a narrow sense.

[148] Vrabec (n 92) 130-131.

[149] Alexander Tsesis, 'The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data' (2014) 49 Wake Forest Law Review 433, 474. This refers also to Chapter 2.2.1., which illustrates that personal data is traded as valuable commodity.

[150] Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in Erik Claes, Antony Duff, and Serge Gutwirth (eds), *Privacy and the Criminal Law* (Intersentia 2006) 69– 70; Orla Lynskey, The Foundations of EU Data Protection Law (Oxford University Press 2015) 11.', Vrabec (n 92) 130.

[151] Vrabec (n 92) 131; Giancarlo F Frosio, 'Right to Be Forgotten: Much Ado about Nothing' (2017) 15 Colorado Technology Law Journal 307, 313– 14.

the power to determine freely the dissemination and use of data concerning him or her.[152]

Especially in the digital age, where once published or used personal data may be perpetual remined and remembered,[153] personal control must be protected and guaranteed as it forms an important part of democracy. Self-determination and personal freedom hereby serve as barriers against totalitarianism.[154] As stated by the German Federal Constitutional Court data protection is crucial as forming an important, inextricable part of dignity and human worth *"[a]t the heart of constitutional order*"[155].

However, the right is not entirely uncontroversial. In the more liberate US law, for example, there is no such equivalent.[156] Instead one could describe US data collection as '*unlimited'*.[157] Furthermore, it illustrates vividly the antagonism in current EU data protection law, namely the values of privacy and transparency.[158]

These tensions are examined in more detail below. At the end of the chapter there is further an evaluation of the question to what extent the RTBF is

---

[152] Lilian Mitrou, Maria Karyda, *EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?* (5th International Conference of Information Law and Ethics, Corfu-Greece 2012) 10 available at <https://www.icsd.aegean.gr/website_files/proptyxiako/388450775.pdf > accessed 10.05.2022.

[153] Mitrou/Karyda (n 152) 10.

[154] Jed Rubenfeld, 'The Right of Privacy' (1989), 102 HARV. L. REV. 737, 802-05; Tsesis (n 150) 616.

[155] cf. Robert G. Larson III, 'Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech' (2013) 18 COMM. L. & POL'Y 91, 104 (quoting Bundesverfassungsgericht (BVerfGE) [Federal Constitutional Court] 1983, 65 BVerfGE 1 (41) (Ger.)).; note that the German concept of personal control is closely linked and related to the GDPR wording; cf. Tsesis (n 149) 616.

[156] Tsesis (n 149) 620 et seq.

[157] Ronald J. Krotoszynski, Jr., 'The Polysemy of Privacy' (2013) 88 IND. L.J. 881, 906.

[158] Fosch Villaronga/Kieseberg/Li (n 4) 304.

transferable to today's data-driven time and whether the right, in its present form, can be upheld in the future.

4.2 Right to Erasure under the GDPR

With the introduction of the GDPR in 2018, the Right to Erasure was formally introduced into European legislation. While this in itself did not constitute a substantive amendment, since the right has been even recognised and accepted by the Court before under the DPD[159], it nonetheless marked an important milestone. As one of "*the most important developments for data privacy*"[160] it contained new duties for data controllers[161] and introduced a clearer definition of the right.[162]

An explanation of the concept of the Right of Erasure, which name has formally changed, but which is often, and perhaps even most commonly, still referred to as the Right to be Forgotten, can be found in Art. 17 GDPR.[163] Accordingly, the data subject has the right to obtain erasure of his or her personal data from the controller, without undue delay. This right subsists, if the concerned data is no longer necessary in relation to the purpose which it was collected for. Further it constitutes that prior consent given by the data subject can be withdrawn anytime[164].[165]

---

[159] See for example *'Google Spain'* (n 2). Cf Krzysztofek (n 94) 15.

[160] Tsesis (n 149) 602.

[161] e.g. the duty to ensure that third parties are informed about the request for erasure (Art 17(2) GDPR).

[162] Vrabec (n 92) 141.

[163] Tsesis (n 150) 602-603; Art. 17 GDPR.

[164] Art. 7 (3) GDPR can be regarded as strenghening the RTBF. See Fosch Villaronga/Kieseberg/Li (n 4) 306; cf Factsheet on the Right to Be Forgotten ruling (C-131/12) available at <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>.

[165] Tsesis (n 149) 602-603.

An important remark is that the GDPR provisions only apply to commercial data.[166] Data collected and processed by natural persons for purely personal or household activities do not fall within the scope.[167] Another important aspect in this context is the rationale behind the Right to be Forgotten. It is not intended to erase history. Rather, it is about maintaining healthy commercial relationships.[168] Great technology firms, such as Google or Facebook strongly rely on huge amounts of personal data from individuals, which often do not have the understanding and awareness of what exactly happens to their data. There is a clear lack of transparency in regard to the processing and its dissemination.[169] This is why the GDPR, including its Art. 17, is aiming to protect data subjects privacy, where data is not essentially required.[170] This also includes the objective of making the Right to Erasure transparent.[171]

4.2.1 Article 17 (1) (a)-(f) GDPR: Grounds of Erasure

According to Art. 17 (1) GDPR data subjects have the right to obtain erasure of their personal data without undue delay. This can be based on different grounds, which are listed in Art. 17 (1) (a)-(f) GDPR.[172]

To begin with, the data subject has a right to obtain erasure of their personal data, if the processing is "*no longer necessary in relation to the purposes for which they were collected or otherwise processed*"(Art. 17 (1) (a)

---

[166] Tsesis (n 149) 604.

[167] GDPR at Art. 2 (2) (c).

[168] Tsesis (n 150) 604.

[169] Grant Arnow, 'Apple Watch-ing You: Why Wearable Technology Should Be Federally Regulated' (2016) 49 LOY. L.A. L. REV. 607, 614.

[170] Tsesis (n 149) 601-604.

[171] Art. 5 GDPR requires that personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject". See also Tsesis (n 149) 596.

[172] Vrabec (n 92) 141.

GDPR).[173] This implies in particular, that outdated and inaccurate data has to be erased. Further through this legal norm an emphasis is put on the principle of limited and specified purpose[174].[175] This principle has in particular great relevance in light of the increasing reuse of data, for instance in form of the availability to third parties.[176]

However, in some cases it may be difficult to establish that the respective data is not relevant anymore. The internet is becoming more and more personalised, which may have as a result, that any piece of personal data can be argued to be relevant.[177] Another critical aspect is the fact that the primary use of data is often based on very vague, broad definitions. Based on that, secondary use can mostly be argued to be relevant. This can result in significantly weakening the impact and effectiveness of the right, as well as challenging the idea of purpose limitation.[178]

Moreover which type of data is considered to be relevant strongly depends on the kind of controller. This can be observed, for example, in the *Google Spain* case, in which it was stated that for search engines different data could be regarded as relevant. Thus, in order to determine the relevance of the data at stake, a case-by-case analysis has to be applied, considering and taking into account all facts and circumstances of the case.[179]

---

[173] See in more detail: Vrabec (n 92) 141-142.

[174] Art. 5 (1) (b) GDPR.

[175] European Data Protection Board, 'Guidelines 5/ 2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' (2019) 7.

[176] Vrabec (n 92) 141.

[177] Hans Graux, Jeff Ausloos, and Valcke Peggy, 'The Right to Be Forgotten in the Internet Era' in Jorge Pérez, Enrique Badía, and Rosa M Sáinz Peña (eds), *The Debate on Privacy and Security over the Network: Regulation and Markets* (36 Ariel 2012) 103.

[178] Bert- Japp Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice' (2011) 8 SCRIPTed 229, 244; Vrabec (n 92) 141-142.

[179] *"[b]ecause that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.", Google Spain* (n 2) para 94.

Art. 17 (1) (b) provides the legal ground for erasure of personal data for situations, when a *"data subject withdraws consent on which the processing is based […], and where there is no other legal ground for the processing"*.

Withdrawal of consent has the effect of depriving the processing of personal data its legitimising, legal ground. This leaves a lack of a legal basis. As a consequence, the data concerned, for which consent has been withdrawn, must be deleted if no other basis exists.[180]

As reflecting the idea of free will of the data subject, Art. 17 (1) (b) GDPR enables the data subject to validly consenting to the use of personal data. Informational self-determination does not only give the right to consent to the processing of personal data in the first place, but rather also entails the right to withdraw the originally given consent for the future.[181]

However, it has to be noted that this ground of erasure might not be of particular great relevance within the big-data environment. This is because most operators of search engines or other big data firms do not seek and thus rely on the express and specific consent of data subjects before processing their personal data. Rather, processing in this field is more often based on grounds of legitimate interest.[182] This same observation is emphasised by the Court in the *Google 2* judgement.[183]

---

[180] Vrabec (n 92) 142-143.

[181] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013) 251.

[182] Vrabec (n 92) 143; Centre for Information Policy Leadership, 'CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data (Discussion draft)' (2017) 33 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf > accessed 16.05.2022.

[183] Case C-136/17, *Commission nationale de l'informatique et des libertés (CNIL) v. Google LLC* [2019] ECLI:EU:C:2019:773; EDPB, 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (2019) 8, para 24.

Pursuant to Art. 21 GDPR the data subject has the right to object to processing of his or her data. In such a case the processing will be stopped, the data however not removed from the server.[184] Due to the fact, that a complete deletion is often desired, Art. 17 (1) (c) GDPR states that such an objection may stipulate a ground of erasure.[185] This right to request erasure of the data is granted regardless of whether the processing is unlawful or not, as long as there are no overriding legitimate grounds for the processing.[186]

Compared to the former Art. 14 DPD, a reversal of the burden of proof in favour of the data subject has been carried out under the GDPR. The data controller has to erase data unless it can demonstrate overriding legitimate grounds[187].[188]

Art. 17 (d) and (e) GDPR contain two additional grounds on which the data subject might obtain erasure of its personal data, namely that erasure must take place if the processing has been unlawful (Art. 17 (1) (d) GDPR). This goes beyond the principles and provisions enshrined in the GDPR, where a valid legal basis is missing. As an illustrative example, erasure must also take place on basis of an express prohibition by a national Court order.[189]

In addition erasure might be requested for compliance with a legal obligation to which the controller is subject (Art. 17 (1) (e) GDPR). This could, for instance, be a national or European law that limits the retention of data.[190]

---

[184] cf. Art. 21 (3) GDPR.

[185] Vrabec (n 92) 144; see also Decision of the Berlin DPA (31 October 2018) https://edpb.europa.eu/sites/default/files/article-60-final-decisions/publishable_de_berlin_2019-4_reprimandtocontroller_decisionpublic.pdf accessed 16.05.2022.

[186] Recital (69) GDPR.

[187] read in conjunction with Art. 21 (1) GDPR: "*compelling legitimate grounds for the processing*".

[188] EDPB Guidelines 5/2019 (n 175) 8-9, para 30.

[189] EDPB Guidelines 5/2019 (n 175) 9.

[190] EDPB Guidelines 5/2019 (n 175) 10.

To conclude with Art. 17 (1) (f) GDPR confers a special and privileged status on children within the data protection regime.[191] If personal data of children was collected in relation to offering of information society services, the erasure of such data can be requested. This provision mainly concerns data collected in the context of social networks. The reasoning behind this special stance is that children might often not be fully aware of the risks associated with the collection and processing of their data, which is why it should be possible to delete them retrospectively. [192]

4.2.2 Art. 17 (3) GDPR: Exemptions

Exemptions to the Right to Erasure can be found in Art. 17 (3) GDPR.[193]

Art. 17 (3) (a) GDPR contains an exception to the right to erasure, on grounds of the necessity of the data processing for the exercise of the freedom of expression and information.[194] Since constituting a non-absolute right, the RTBF has to be considered "*in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality*"[195]. This is not only stated in Art. 17 (3) (a) GDPR, but was also emphasised by the ECJ in its judgment in the case *GC and Others v Commission nationale de l'informatique et des libertés (CNIL).*[196] In particular the privacy right contrasts with the freedom of expression and the right to access information in Art. 11 of the Charter as well as infringing the economic interests[197] of search engines or other companies.

A case-by-case analysis has to be undertaken, when assessing such a proportionality test.

---

[191] Recital 65 GDPR.

[192] Vrabec (n 92) 144-45.

[193] Vrabec (n 92) 145-148.

[194] Vrabec (n 92) 146. This fundamental right is enshrined in Art. 11 CFR.

[195] Case C-136/17 *CNIL* (n 183) para. 57.

[196] Case C-136/17 *CNIL* (n 183) para. 57.

[197] Possible infringement of Art. 16 CFR.

Critically, and perhaps even alarmingly, is the fact that the Court stated in the Case *Google Spain*, that: "*fundamental rights to privacy and data protection should, 'as a rule' override 'not only the economic interest of the operator but also the interest of the general public in having access to that information'*".[198]

This exemption and in particular the ruling of the Court in *Google Spain*, which clearly indicates some sort of over-compliance for many private companies, without further examination and without the application of a properly assessed and reasoned proportionality test pursuant to Art. 52 (1) CFR, seems critical particularly in regard to the internet and digitalisation. As personal data nowadays co-creates the internet, thus can be seen as shaping the world's largest news and knowledge platform, any removal of information would interfere with the freedom to access information and the freedom of speech.[199]

It seems that the Court is stretching the right to privacy and data protection to the extreme and shows what high demands the EU puts on data protection and that it is difficult for economic participants to meet them. This is also shown in the *Schrems* ruling[200], in that the Court also adopted a very strict stance with regard to the protection of personal data, by invalidating the EU-US Privacy Shield.[201]

In those judgments it seems that the Court does not sufficiently take into account the rights enshrined in Art. 11 of the Charter, which protect the freedom of expression and information and thus also the important role press plays in democracies. If one tries to translate this to possible consequences in the context of AI, the strict, protectionist stance taken by the Court here could be a source of concern, as it might be expected that the ECJ will maintain its course, which entails an incredibly far-reaching protection of individuals.

---

[198] Case C-131/12 *Google Spain* (n 2) para 99.

[199] Vrabec (n 92) 146.

[200] Case C-311/18 Schrems (n 120).

[201] BfDI (n 121).

Notable however is, that both the GDPR and the Art. 29 WP[202] address this issue and acknowledge not only the rights of the data subject, but rather also the data controller interests. Limits to the territorial scope of application to the RTBF were furthermore made in the *CNIL* case[203], where the Court clarified that a delisting request required Google only to delist search results to personal information in search engine versions corresponding to all the EU Member States. Accordingly global delisting is not required.[204]

It remains to be hoped that no such unreflective statements will be made in the future and that, above all, a proportionality test will be carried out appropriately and more reasoned. Only in doing so it is possible to protect the rights of private individuals as well as those of companies. This is the only option for us to benefit from AI without relinquishing complete control and exposing ourselves to dangers without protection.

Moreover according to Art. 17 (3) (b) GDPR the processing is justified if it is necessary for the compliance with a legal obligation or for the performance of a task carried out in the public interest or official authority. This could be a decision of a competent authority or national law to retain data for a longer period of time.[205]

Art. 17 (3) (c) GDPR concerns the retainment of data for reason of public interest in public health and Art. 17 (3) (d) GDPR addresses cases with scientific, archiving, or historical reasons, if the erasure would seriously impair the achievement of the objectives of that scientific or research

[202] Article 29 Data Protection Working Party, 'Opinion 06/ 2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/ 46/ EC' (2014) 11.

[203] Case C-507/17 *CNIL* (n 119) para 73.

[204] Case C-507/17 *CNIL* (n 119) para 73.

[205] Vrabec (n 92) 146-147.

processing.[206] The establishment, exercise or defence of legal claims constitutes another exemption under Art. 17 (3) (e) GDPR.

Exemplified, the encroachment on the RTBF is often justified based on the fact that the mass storage and transfer of personal data serves the general goal of preventing serious crime, which is a public interest offence and thus deserves special protection, although the retention of data is '*far-reaching and […] particularly serious*'.[207]" Such exemptions beyond the exceptions laid down in Art. 17 (3) GDPR on the grounds of countervailing national laws and or other European legislation concerning national security, judicial proceedings or other general public interests of MS and the protection of rights and freedoms of others, are specified in Art. 23 GDPR.[208]

4.2.3 Legal consequences

Provided that the conditions of the Right to Erasure are fulfilled, as a legal consequence, the data controller is obliged to erase the personal data concerned without undue delay.[209]

In the technological age, the right to delisting is a special, and probably most prominent form of the Right to Be Forgotten. As already seen above, most search engine cases of the recent years under Art. 17 GDPR have dealt with this important aspect of the right.[210] It has to be noted, that those cases

---

[206] Vrabec (n 92) 147-148.

[207] Cases C-293/12 and C-594/12 *Digital Rights Ireland* (n 106); Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others [2016]; Research Gate, 'European Courts Decisions Challenging Interference with Article 7 & Article 8 Rights EUCFR', 12-13 available at <https://www.researchgate.net/publication/331873330_Article_7_Article_8_Rights_EU_Charter_of_Fundamental_Rights_Case_Law_of_EUCFR_and_ECtHR_'A_Note_for_Students_of_EU_Law's_on_Data_Protection_Laws'> accessed on 16.05.2022.

[208] Vrabec (n 92) 147-148.

[209] Vrabec (n 92) 141.

[210] Vrabec (n 92). 141. See also C-131/12 *Google Spain* (n 2) where the existence of this right has been established.

oftentimes do not result in the complete erasure of data. The information concerned still remains in the archives and thus in the control of the data controller, which in general only takes down the information from its search results and websites. Thus, it is not openly accessible and visible for the public eye.[211] Nevertheless, the general obligation to erase data applies to search engine providers as well, meaning that in some cases it might be necessary to delete data completely, including all indexes and caches.[212]

If the controller who is obliged to erase the personal data pursuant to paragraph 1 has made the data public to third parties, he or she, according to Art. 17 (2) GDPR, additionally has the obligation to take reasonable steps, including technical measures, to inform other controllers which are processing the personal data of the erasure request and to delete any link or copy or replication of such personal data. In doing so, he has to take into account the state of technology and cost of implementation.[213] The increasing complexity of technical environments has led to a strengthening of the RTBF under the GDPR compared to the DPD by introducing such an obligation.[214]

4.3 The RTBF in an AI environment

Applying the Right to be Forgotten in regard to AI raises various questions and difficulties and fulfilling its legal aims can even be regarded as "*on the edge of impossibility*".[215]

This is mainly due to the fact that there are serious doubts in regard to its effectiveness and technical feasibility.[216] In order to apply the right in

---

[211] EDPB Guidelines 5/2019 (n 183) 5, para 9.

[212] EDPB Guidelines 5/2019 (n 183) 5, para 10.

[213] Fosch Villaronga/Kieseberg/Li (n 4) 306. On the meaning of 'informing third parties' see also Vrabec (n 92), 148-150.

[214] Vrabec (n 92) 148-149.

[215] Fosch Villaronga/Kieseberg/Li (n 4) 305.

[216] Brendan van Alsenoy, Aleksandra Kuczerawy, J. Ausloos, 'Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?' (2013) ICRI Research Paper 15,

modern technology environments, the concept of privacy has to be fundamentally rethought. [217]

This section discusses some potential fields of controversy. Major focus is on the precise definition and understanding of personal data, followed by an analysis of the concept of forgetting in machine learning.

4.3.1 Applicability of the GDPR: The 'personal data problem'

The prerequisite for applying the GDPR is that data must qualify as personal data pursuant to Art. 4 (1) of the Regulation.[218] Other information, that does not constitute personal data, cannot be subject to erasure under the GDPR, regardless of any harms it may cause or how desirable a removal may be.[219] The decisive element for the classification is the possibility of direct or indirect identification.[220]

Especially in relation to training sets, this can be considered problematic, because training data is often anonymised or such systems are applying powerful re-identification techniques.[221] This is why training sets are often assumed to not fall within the category of personal data.[222]

TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy, 42, available at <https://ssrn.com/abstract=2321494> acessed 16.05.2022.

[217] cf. ECP Platform for the Information Society, Artificial Intelligence Impact Assessment, The Netherlands (2019).

[218] Hacker (n 41) 265.

[219] Bonnie Kaplan, 'Selling Health Data: De- Identification, Privacy, and Speech' (2015) 24 Cambridge quarterly of healthcare ethics 256, 261.

[220] Hacker (n 41) 267.

[221] For an overview of such techniques, see El Emam, Rodgers and Malin, 'Anonymising and Sharing Individual Patient Data' (2015) 350 BMJ h1139; Cavoukian and Castro, 'Big Data and Innovation, Setting the Record Straight: De-Identification Does Work', Office of the Information and Privacy Commissioner, Ontario, 2014, 9–11.

[222] Manon Ostveen, 'Identifiability and the Applicability of Data Protection to Big Data' (2016) 6 International Data Privacy Law 299, 307; Mike Hintze, 'Viewing the GDPR

However, as several studies have shown,[223] the inferred or pseudonymised data can oftentimes still be de-anonymised under certain conditions.[224] This may be possible by using de-anonymization strategies or by relying on a link between the data and the data subject, which has been removed from the data set, but which is still accessible for the controller or a third party.[225]

In the *Breyer* case, the CJEU held that in order to be qualified as personal data, it must be reasonably likely that the controller will use the strategies available to him to carry out an identification.[226] Recital 26 GDPR further clarifies this '*reasonable likelihood'* test. However, a high degree of uncertainty relating the likelihood of re-identification remains. This is becoming especially evident, when considering the pace with which new technological possibilities evolve.[227]
Recital 9 of Regulation 2018/1807[228] provides some examples of non-personal data. Accordingly, aggregated and anonymised datasets used for big data analytics do not fall within the scope of the GDPR, if it is not

---

Through a De-identification Lens: A Tool for Compliance, Clarification, and Consistency' (2018) 8 International Data Privacy Law 86, 89; Hacker (n 41) 265.

[223] See e.g.: Latanya Sweeney, 'Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy' (2000) Working Paper LIDAP-WP4; Arvind Narayanan, Vitaly Shmatikov, 'Robust De-anonymization of Large Datasets' [2008] Proceedings of the 2008 IEEE Symposium on Security and Privacy 111; Luc Rocher, Julien M. Hendrickx, Yves-Alexandre de Montjoye, 'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models' (2019) 10 Nature Communications 3069.

[224] Hacker (n 41) 265.

[225] Hacker (n 41) 265 et seq; ICO, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection'(n 139).

[226] Case C-582/14 *Patrick Breyer v Bundesrepubblik Deutschland* [2016] (ECLI:EU:C:2016:779) paras. 45–49.

[227] Veale/Binns/Edwards (n 49) 7.

[228] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

possible to de-anonymise and thus to turn this data into personal data relying and using technological developments."[229]
Furthermore training models are highly vulnerable to cyberattacks, which could result in a breach of confidentiality as information is leaking to entities, who are not intended to get it. In analogy to Art. 4 (5) GDPR, concerning pseudonymization, such model inversion could be seen as constituting personal data.[230]

It is debatable whether it should make a difference how sensitive the respective information is. A statement made by the CJEU in the *Google Spain* ruling would suggest such a stance. Accordingly, proportionality would depend in some specific cases on the nature of the concerned data, its sensitivity for the data subject's private life and on how large the public's interest in having the personal information is.[231] However, this logic cannot be applied equally to AI cases, as models might be able to transform non-sensitive data into sensitive data.[232] When studying further case law, it appears that the CJEU imposes low requirements and thus applies a wide scope of personal data. This is supported by the *Nowak* case[233], where the Court clarified that the concept of personal data does not require the data to be particular sensitive or private, but instead encompasses '*any information'*.[234]
Article 29 WP seems to equally follow a broad concept of personal data, by endorsing inferred data as personal data.[235]

---

[229] EPRS study (n 10) 36.

[230] cf. Veale/Binns/Edwards (n 49) 4-8.

[231] C-131/12 *Google Spain*, para 81.

[232] Veale/Binns/Edwards (n 49) 3.

[233] Case C-434/16, *Nowak v Data Protection Commissioner* (ECLI:EU:C:2017:994) ('*Nowak'*).

[234] *Nowak* (n 233) 34.

[235] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data'.

Some scholars argue that the wide approach followed by the Court is too extensive and thus "*fuels undesirable data protection maximalism*".[236]

In order to find a median that protects data subjects from potential risks without going further than absolutely necessary, it might be appropriate to pursue a risk-based approach. Such an approach is generally followed throughout the GDPR, relating to data protection specific risks,[237] hereby namely the risk of re-identification.[238] This means that the applicability of the GDPR will be triggered, if a concrete re-identification risk is likely and sufficiently relevant.[239]
To summarize, strong anonymization strategies tend to exclude the applicability of the GDPR, unless there is evidence of a concrete re-identification intention, regardless of the legality or illegality of such a re-identification.[240]

Another fact, that can be criticised is that machine learning models are underlying an insufficient control regime, because they are only covered indirectly by the GDPR, as they only apply when personal data is involved in building them, throughout the process of the training or if the result is applied to other data. This means that there exist no data protection rights nor obligations for the period between the building and the use of such models. However, it can be argued that individuals want and should be able

---

[236] cf. Purtova (n 56). See also Gerrit-Jan Zwenne, 'Diluted Privacy Law' (Leiden University 2013) 9 <https://zwenneblog.weblog.leidenuniv.nl/files/2013/09/G-J.-Zwenne-Diluted-Privacy-Law-inaugural-lecture-Leiden-12-April-2013-ENG.pdf> accessed 16.05.2022.

[237] See also Recital (75) GDPR.

[238] Hacker (n 41) 266.

[239] Hacker (n 41) 266. Similar result in Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques', WP 216, 2014, 6 et seq.

[240] Hacker (n 41) 267. Note that the legality requirement is highly discussed within scholars. On this topic see specifically Jürgen Kühling, Manuel Klar, 'Speicherung von IP-Adressen beim Besuch einer Internetseite' Internetseite' [engl. 'Retention of IP addresses when accessing a website'] (2017) Zeitschrift für Datenschutz 27, 28.

to control how they are specifically read by those machines-learning systems as part of their informational self-determination.[241]

4.3.2 Concept of 'Forgetting'

As Vint Cerf, one of the so-called '*fathers of the internet'*,[242] put it once, it is impossible to *"[…] go out and remove content from everybody's computer just because you want the world to forget about something*."[243] This highlights the existence of a discrepancy between the concept of human forgetting in contrast to the one in a machine world.

What human understand as privacy and forgetting, is making information, which was previously open to the public eye, private again. However, this way of thinking does not easily translate to AI and machine learning. Big data has changed the default of forgetting fundamentally. Problematically, all current existing laws and regulations do not sufficiently recognise this discrepancy in understanding. Rather, the current rules are based solely on the concept of human memory. [244] Exemplarily, the GDPR does not specifically address AI-based processing in one of its provisions.[245]

AI does not forget in the same way as human do, as data removal in this context is much more complex. This is especially evident in large and complex systems, such as databases. It is even questionable whether real deletion is possible at all, given the current state of the art and the ever-

[241] Veale/Binns/Edwards (n 49) 3.

[242] Zeit.de, 'Interview Vinton Cerf "Das ist bestimmt nicht die Welt, die ich wollte"' [engl. Interview Vinton Cerf "This is certainly not the world I wanted"] available at <https://www.zeit.de/digital/internet/2020-01/vinton-cerf-internet-netzwerke-informatiker-usa> accessed on 03.05.2022.

[243] Matt Warman, 'Vint Cerf attacks European internet policy' (Telegraph 2012) available at: <https://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html> accessed 16.05.2022.

[244] Fosch Villaronga/Kieseberg/Li (n 4) 305-08.

[245] EPRS study (n 10) 75.

increasing complexity of systems that require diminishing human intervention. [246]

Illustrating this in a comprehensive example[247], modern database management systems nowadays are designed for the effective provision of data. By indexing data, specific data can be searched for and quickly extracted from a huge data set. However, those real-life databases have to comply with certain requirements, in order to work efficiently and be trustworthy at the same time. This raises significant implications to the problem of data removal. The so-called ACID-compliance consist of the adherence of the following prerequisites: atomicity, consistency, isolation and durability. The fact that the database always has to be restored to its previous normalized state after each finalization of an operation, and that data must be stored permanently in the database makes it considerably more difficult - if not even impossible - to actually delete data.

Beside these requirements there exist additional features of a database which are necessary to provide a usable environment. Among others, these include the necessity of intended rollbacks, as well as regular backups and replication. Thus some kind of maintenance and consistency of historical data is required, to roll back in time for a certain amount of transactions. It is both common practice and enormously important for the functioning of modern IT systems and for averting the negative effects of potential disasters that data is dynamically updated and spread across a very large geographical area. Taking into account that data is not only stored at one specific place, but rather is spread and stored at various locations inside the system or mechanism, in backups, logfiles and different replicated databases, a request of erasure in the strict sense would require the location of all of them, followed by the overwriting with random information.

In addition to those technical difficulties concerning the feasibility of the deletion of data, it is important to also consider that such a removal may

[246] Fosch Villaronga/Kieseberg/Li (n 4) 308.

[247] cf Fosch Villaronga/Kieseberg/Li (n 4) 308-10.

possibly also affect the quality of the data. In particular the overwriting endangers the consistency of the database and might have negative consequences for the performance of the database, while being both time-consuming and cost-intense.[248] Furthermore, the deletion via commonly used SQL interfaces, does not result in the immediate overwriting of the data to be forgotten. Rather, the data is first transferred to some kind of 'garbage offset' within the system. If the dataset needs space it can then easily overwrite, hence reuse the space. However, in reality this often takes a lot of time. In other words, this means that the data is not deleted, but only taken down from the active records and search index.[249]

As this example demonstrates, the answer to the question of whether deletion might become infeasible in real-life machine-learning environments operating under economic principles strongly depends on how the term deletion is interpreted. Does the term refer to the removal from search indexes, the overwriting in file systems or does it even require removal from all internal mechanisms? This must be discussed and taken up by the legislator.[250]

With regard to the unlearning of algorithms, which is another way of '*Artificial Forgetting'*,[251] it is to be said that in some cases it is possible through renewed technology, to put an extra layer between the learning algorithm and the data which it is trained upon.[252] Such a design eliminates any dependency between different layers, which means that data can

---

[248] Peter Fruhwirt, Peter Kieseberg, and EdgarWeippl, 'Using internal MySQL/InnoDB B-tree index navigation for data hiding' in: Peterson, G., Shenoi, S. (eds) *Advances in Digital Forensics XI. DigitalForensics* 2015, IFIP Advances in Information and Communication Technology vol 462, 179-94 (Springer International Publishing 2015) <https://doi.org/10.1007/978-3-319-24123-4_11>.

[249] cf Fosch Villaronga/Kieseberg/Li (n 4) 308-10.

[250] Fosch Villaronga/Kieseberg/Li (n 4) 308-10.

[251] Fosch Villaronga/Kieseberg/Li (n 4) 308.

[252] Yinzhi Cao and Junfeng Jang, 'Towards Making Systems Forget with Machine Unlearning', IEEE Symposium on Security and Privacy (2015) 483 <. DOI 10.1109/SP.2015.35>.

theoretically be removed, without resulting in the collapse of the entire model.[253]

This may be unproblematic in the case that a single person requests the deletion of his or her data. However, it may have negative consequences on the algorithmic outcome and the functioning of the trained model, if suddenly numerous individuals who share similar commodities collectively request such deletion at the same time[254], on grounds that 'group' or 'categorial' privacy is at stake. This might be supported by the argument, that groups of individuals should have an agency over their representation in models.[255]

[253] Kurzweil, 'New "Machine Unlearning" Technique Deletes Unwanted Data' (2016) available at <https://www.kurzweilai.net/new-machine-unlearning-technique-deletes-unwanted-data> accessed 16.05.2022.

[254] Vrabec (n 92) 155; Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For' (2017) 16 Duke Law and Technology Review 18, 69.

[255] Veale/Binns/Edwards (n 49) 3.

5 Policy Options/Outlook

5.1 Possible measures beyond the GDPR

As mentioned above, there are considerable uncertainties with regard to the technical implementation of the Right to Erasure in the context of AI applications, as the idea of deleting contrasts with the nature of AI.[256] However, a change of perspective may be conducive to this. The Right to be Forgotten can be understood as encompassing a broader concept than the Right to Erasure in the strict sense. Including all legal entitlements that facilitate the process of '*forgetting*', both perpetual or temporary, but also non-legal mechanisms, like down-ranking and obfuscation.[257] The underlying question for this approach is whether it is even necessary to really delete the data completely in order to achieve the objectives, when there are other methods that might lead to similar results.[258]
There exist several other options to operationalise the RTBF beyond the GDPR.

To begin with, the RTBF is not the only measure in the GDPR which can be applied to meet the named objective. Other principles like the requirements of storage limitation and purpose limitation can be applied as well.[259] Guidance documents by competent authorities could help to inform companies properly on this topic, in order to foster awareness concerning possibilities to minimize the amount of data and thus also relating risks.[260]

---

[256] Elena Esposito, 'Algorithmic Memory and the Right to Be Forgotten on the Web' (2017) 4 Big Data & Society 1,6.

[257] Vrabec (n 92) 130.

[258] Fosch Villaronga/Kieseberg/Li (n 4) 310; Vrabec (n 92) 156.

[259] Vrabec (n 92) 150; Fosch Villaronga/Kieseberg/Li (n 4) 310-311.

[260] Example: dutch regulator issued guidance paper on how to copy information from identification documents. This resulted in the minimisation of the collection of data, see Tristan Jonckheer, 'Copying ID documents – Dutch data regulator issues guidance'

When assessing possible measures beyond the GDPR, which could facilitate the forgetting of data and thus giving real control to data subjects, one should also take into account technical or other innovations which might be suitable to provide for that.

One could start with the examples of pseudonymisation and anonymisation. However, these options both have disadvantages and can therefore not to be regarded as sufficient. The GDPR treats pseudonymized data as personal data. Anonymisation might sometimes be an alternative, but does not form a strong technological solution, as re-identification might often still be possible.[261]

Another, stronger approach is the possibility of '*obfuscation*'.[262] Where classical deletion is not feasible, the "*addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects*"[263] can be suitable to reinforce the notion of forgetting in the context of AI. This approach, which consists of multiplying, instead of erasing memories, targets mainly on secondary data processing and can be seen as some form of anonymisation.[264]

Another option that seems promising, at least in theory, is the utilization of functional encryption. This implies the possibility to perform mathematical operations on encrypted data, without being able to decrypt it. Unfortunately, the current state of the art does not yet allow for this, as most algorithms are still too inefficient to apply this method to a large amount of data in a big data

---

(2012), available at <http://www.privacyandcybersecuritylaw.com/copying-id-documents-dutch-data-regulator-issues-guidance> accessed on 16.05.2022.

[261] Fosch Villaronga/Kieseberg/Li (n 4) 310.

[262] Finn Brunton and Helen Fay Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (MIT Press 2016).

[263] Vrabec (n 92) 155.

[264] Esposito (n 258) 6; Vrabec (n 92) 155-56; For instance, a decision by the French CNIL suggested that anonymisation techniques are technically equal to erasure of data and thus fulfil the purpose of art 17. Decision of the French DPA (29 August 2020) <https:// edpb.europa.eu/ sites/ edpb/ files/ article- 60- final- decisions/ summary/ publishable_ fr_2019- 09_ right_ to_ erasure_ summarypublic.pdf> accessed 17.05.2022.

environment. It is therefore desirable that further research is conducted in this area.[265]

Down-ranking, thus deliberately placing certain search results at the bottom of search engine result pages, might be a good alternative to the RTBF as well.[266] The CJEU seems to support this approach in order to improve privacy of individuals, where a delisting request could not been granted.[267]

Moreover it might be appropriate to look at the lifecycle of data processing. By introducing expiration dates on either the data or the consent for the respective processing addresses a time challenge of digital remembering.[268] Ensuring that the erasure of data becomes an inherent part of the processing by the method of '*deletion by default'* would have the effect that data use becomes circular. This would automatically ensure that data is not stored and retained for an excessively long period of time.[269]

Although the latter methods are not easy to apply to AI either, they should be named in the discussion since they are important in the overall picture around the issue of the Right to be Forgotten.

As seen, several approaches exist, but none of them seems perfect and fit enough to be used in real-life application on its own. Applying current data protection provisions to AI applications still is connected to a high degree of legal uncertainty, as the GDPR does only address some of the issues relating to machine-learning. That is why there is an additional need of different legal and regulatory approaches. Most importantly, it has to be made clear, which of the possible methods of deleting is regarded to be sufficient to comply with the GDPR. This should be complemented by the envisage of guidance documents as well as a change in legislation, which is the result of more

---

[265] Fosch Villaronga/Kieseberg/Li (n 4) 310.

[266] Vrabec (n 92) 154.

[267] e.g. Case C- 136/ 17 *GC and Others v CNIL* (n 184) para 78.

[268] cf. Viktor Mayer- Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2011) 171. Mayer-Schönberger one of the firsts argued for such expiration dates.

[269] Vrabec (n 92) 152-53.

interdisciplinary research [270] and which addresses the current deficiencies in law.[271]

5.2 AI Act

In 2020, the Commission has stated clearly in its White Paper on AI regulation[272] that it is of enormous necessity and urgency, to review the legal framework in regard to all the new technical developments.[273] Followed by that a proposal on the Artificial Intelligence Act[274], which contains some important constraints regarding AI at EU level[275], has been put forward, as the latest addition to a long series of EU Acts and other technology related regulatory initiatives. This so-called '*act-ification'* is a strong indication of the brutality with which the EU is trying to make it clear that the area around all technology-related issues falls within its competence.[276]

The AI Act aims at the creation of a coordinated European approach on the human and ethical implications of AI.[277] This should be based on the

---

[270] ICO: 'Big data, artificial intelligence, machine learning and data protection' v. 2.2, 213-214 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed on 16.05.2022.

[271] Fosch Villaronga/Kieseberg/Li (n 4) 312.

[272] COM(2020) 65 final (n 10). In this regard see also European Council, European Council meeting (19 October 2017) – Conclusion EUCO 14/17, 2017, 8.

[273] Ufert (n 79) 1087-1097.

[274] Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts COM (2021) 206 final.

[275] Hacker (n 41) 258.

[276] Vagelis Papakonstantinou and Paul De Hert,' EU lawmaking in the Artificial Intelligent Age: Act-ification, GDPR mimesis, and regulatory brutality' (2021), available at <https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/> accessed on 16.05.2022. See further on this topic: Roger Brownsword, *Law, Technology and Society Reimagining the Regulatory Environment* (Law, Science and Society 2019), 194 et seq..

[277] AI Act (n 27) 1 (Explanatory Memorandum).

ultimate goal of increasing human well-being. Ensuring the well-functioning of an internal market for AI-systems, which should be human-centric, as well as the objective to make the Union as global leader in the development of secure, trustworthy and ethical AI, competitive vis-á-vis other global players, support this main goal.[278] Above all, the proposed legislation is based on fundamental values and principles and is intended to create trust and confidence in trustworthy AI-based solutions by balancing opportunities and risks and mitigating the latter as best as possible.[279]
The proposal describes itself as being a coherent part within the Commissions overall digital strategy in its contribution to promoting technology that works for people and is crucial for ”[*s]haping Europe's digital future*”[280].[281]

When comparing to the GDPR the first significant novelty is that the AI Act wants to introduce a single definition of the term *‘Artificial Intelligence’*.[282]

Further it is worth noting that the AI Act is intended to have a much broader scope than the Data Protection Regulation, which only applies when it comes to the processing of personal data and aims primarily at personal data protection. The AI Act, on the other hand, is not limited to a specific activity and has as its objective both the protection of individuals as well as advancing the development of AI. It deals with the question of how to reconcile AI-

[278] European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020, 6; European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012 (INL).

[279] AI Act (n 27) 1.

[280] Communication from the Commission, Shaping Europe's Digital Future, COM/2020/67 final.

[281] AI Act (n 27) 5-6.

[282] AI Act (n 27) 3; for the proposed definition see Art. 3 of the proposed Regulation.

based innovation with individual rights and social values and is more entrusted with its governance.[283]

The proposed balanced and proportionate horizontal-regulatory framework follows a risk-based approach.[284] High-risk AI systems in this context are defined as posing significant risks to the health and safety or fundamental rights of persons.[285] The regulation is further differentiating between uses of AI that create an unacceptable risk, a high risk, and low or minimal risk. A list of prohibited AI is established by Title 2 of the proposed Regulation.[286] Accordingly, the obligations included should primarily affect operators of high-risk systems. Others, which represent a lower risk, will be given some kind of recommendations in the form of codes of conduct, with the aim to voluntarily apply those requirements which are mandatory for high-risk AI systems.[287]

As seen from the foregoing discussion, training data is a crucial element for the development of AI applications and raises some difficulties especially in regard to the RTBF.[288] It is therefore to be welcomed that the proposed regulation introduces with its Art. 10 a governance regime regarding such, including the training, validation and testing of such data. Three main regulatory risks are highlighted in this respect, namely quality, discrimination, as well as innovation risks.[289]

With regard to the enforcement of the regulation, a governance system at Member State level should be established, which mainly builds on existing structures. Additionally, in order to support and strengthen this, it is planned

---

[283] Papakonstantinou/De Hert EU lawmaking in the Artificial Intelligent Age: Act-ification, GDPR mimesis, and regulatory brutality' (n 276).

[284] AI Act (n 27) 3, 18; see also para 6 of the proposed Regulation.

[285] AI Act (n 27) 3.

[286] AI Act (n 27) 12.

[287] At least this is the currently preferred option by the Commission; cf. AI Act (n 27) 8-16, Title IX.

[288] Hacker (n 41) 258.

[289] Hacker (n 41) 260-262.

to establish an European Artificial Intelligence Board as forming part of a cooperation mechanism on EU level.[290]

The proposed AI Act is compatible with the GDPR and is going to complement the latter with a set of harmonised rules to the design, development and use of certain high-risk AI systems.[291]

A noticeable aspect is that some of the provisions of the drafted AI Act are very similar to the model of the GDPR. This phenomena is called '*GDPR mimesis'* and refers strong influence of the GDPR on numerous new pieces of EU law. Some argue, that the GDPR might provide some kind of acquis and can be used as a model for other legislation, which orientate on its definitions, substantial and institutional approach.[292]

Furthermore, the proposed Act is closely linked to the Data Governance Act[293], the Open Data Directive[294] and other initiatives under the EU strategy for data[295].[296]

Whether and to what extent this proposed legal act can and will really bring a change and influence the RTBF remains to be seen.

---

[290] AI Act (n 27) 3.

[291] AI Act (n 27) 4-5.

[292] Papakonstantinou/De Hert 'EU lawmaking in the Artificial Intelligent Age: Act-ification, GDPR mimesis, and regulatory brutality' (n 276). Also keep in mind the '*Brussels effect'*, which also strongly indicates the importance and extensive influence of the GDPR.

[293] Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767.

[294] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83

[295] Commission Communication, A European strategy for data COM/2020/66 final.

[296] AI Act (n 27) 5.

In any case, it is positive that the White Paper[297], the accompanying Commission report on the liability and security of AI[298] and the draft of the AI Act were developed at the interface between law and technology by collecting diverse expertise. The High Level Expert Group on AI was set up and stakeholders, for example in form and through the AI Alliance[299], were involved in the development and drafting of the Act.[300]

To be aware of, and also mention the intersection of law and AI, can clearly be seen as an important step in the right direction.[301]

However, many legal uncertainties remain. Too many indefinite legal terms still impede the effective and reliable application of existing regulation to AI systems.[302] In order to provide more legal certainty, it should be considered whether safe harbours for developers, operators and controllers of such AI applications can and should be established. Such should include both quantitative but also principle orientated elements to ensure a certain degree of certainty while remaining some flexibility, which leaves room for innovation and the ability to respond to technological changes. It is fortunate that the draft of the AI Act already contains tools for the establishment of such safe harbours in form of harmonised standards in Art. 40 or respectively in form of common specifications pursuant to Art. 41.[303]

---

[297] COM(2020) 65 final (n 10) 18 et seq.

[298] European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics', COM (2020) 64 final, 8 et seq.

[299] The AI Alliance is a multi-stakeholder forum launched in June 2018, AI Alliance <https://ec.europa.eu/digital-single-market/en/european-ai-alliance> accessed on 16.05.2022.

[300] Hacker (n 41) 298-99.

[301] Hacker (n 41) 258.

[302] Hacker (n 41) 298.

[303] Hacker (n 41) 299.

6 Conclusion

To conclude, one major finding when looking at the issue of the Right to be Forgotten in the context of AI is the huge discrepancy between legal and technical reality. As we are in the midst of a revolution in which technological progress and the application of AI systems seem inexorable, it is time that law and technology learn to speak the same language that shares a common understanding of the terms '*erasure*' and '*forgetting*'.[304]
There is a desperate need of greater interdisciplinary research in regard to application of privacy law to new technologies such as AI.[305]

Both case law and the GDPR provisions seem to indicate the existence of tendencies towards strong data protectionism.[306] The political message the GDPR is sending is the one that shows what a stringent, far-reaching stance it takes in relation to data protection.
Too extensive protectionism and overcompliance in relation to data flows should be considered cautiously, however. Critics see serious tensions between data protection and the maintainance of competitivness here, as too high standards will, in the long run, preclude the EU´s ability to keep pace with other globalplayers, in the race for digital sovereignty and technological power.[307]

Analogously to the EU's twofold objective, creating a two-folded trustworthiness and credibility should perhaps be the overarching aim for the upcoming digital decade. On the one hand, it is crucial to create a framework for trustworthy AI, including enough safeguards, which at their core are aiming to ensure individual data protection. People must be able to

[304] Fosch Villaronga/Kieseberg/Li (n 4) 313.

[305] Fosch Villaronga/Kieseberg/Li (n 4) 305.

[306] Hervé (n 7) 196-97.

[307] Hervé (n 7) 213-214.

trust AI and its development, in order to be willing to accept and embrace this transformation. On the other hand, there is need for trustworthy regulation. Companies that are progressively innovating and working with AI, need to be granted more legal certainty.

This can be achieved through addressing deficiencies in law. As it is very time-consuming and expensive to introduce new legislation, this should be preferably done in form of a collaborative approach by introducing both soft law measures[308], such as guidance documents or standards, which reflect the pace of the technology better, but also by revising and updating legislative acts, as they are of binding nature and can be relied upon more easily.[309]

Such a legal framework has to include flexible mechanisms, in order to be adapted dynamically as the technology evolves and new concerning situations emerge.[310]

It should be noted at this point that it is not expedient to simply introduce more and more rules, as this can create confusion and fragmentation. Some experts even argue that current data protection law is already quite comprehensive and sufficient. Instead of introducing new and extensive legislation, the focus should therefore be directed more towards the concretisation in specific sectors.[311]

Additional explanations, definitions and interpretations by competent authorities, such as the EDPS, which are taking into account the technical

---

[308] In comparison to regulations, directives, or decisions, soft law is not binding on the parties to whom they are addressed to. However, in some cases they might also create some legal effects. Most importantly, they can be seen as an important and useful tool and source of guidance for the interpretation of the applicable rules and laws, cf Eurofound, 'Softlaw' 2011) available at <https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/soft-law> accessed on 09.05.2022.

[309] Fosch Villaronga/Kieseberg/Li (n 4) 312.

[310] AI Act (n 27) 3, 18. See also para 6 of the proposed Regulation.

[311] European Union Agency for Fundamental Rights (FRA): 'Getting the future right – Artificial Intelligence and Fundamental Rights' (2020) 66.

side of the topic, in order to find a balance between the wording of the law and its applicability are also to be welcomed and appreciated.[312]

Summarizing, it is important to remain critical, vivid and resilient in this whole debate, which seems so wide-ranging, highly emotional and difficult to be resolved. "*Nothing fixes a thing so intensely in memory as the wish to forget it*".[313] This quote should remind us to keep reminding ourselves why the Right to be Forgotten is considered as so important and worth protecting. How much regulation do we need to efficiently safeguard individual rights but also ensure innovation and deployment of AI?
This paper, like so many before it and presumably after it, provides no concrete answer to this question. Nevertheless, it should offer some impulses, provide food of thought and highlight the need of more interdisciplinary work in this field. It remains to be seen how the topic will evolve und which stance the Court will take in upcoming cases.
Irrespective, it should be noted positively, that the issue is currently receiving so much attention in the European Union. The ECJ seems to take the protection of data very seriously. It is aware of the fact that, especially nowadays where data is omnipresent and crucial for AI applications, with the result of not having any real control over own personal data, constant further reflection, rethinking and development of law and judicial protection is necessary and pivotal.

[312] Fosch Villaronga/Kieseberg/Li (n 4) 310.

[313] Michel De Montaigne.

Bibliography

Primary sources

EU Legislation

Consolidated version of the Treaty on European Union [2016] OJ C 202 ('TEU').

Consolidated version of the Treaty on the Functioning of the European Union [2016] OJ C 202 ('TFEU').

Charter of Fundamental Rights of the European Union [2016] OJ C 2020.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ('DPD')

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, [2019] OJ L 172.

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

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303.

Legislation from other jurisdictions

California Consumer Privacy Act (2018).

EU Sources/Official Papers

European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics', COM(2020) 64 final.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM (2018) 237 final.

Communication from the Commission, Shaping Europe's Digital Future, COM/2020/67 final.

European Commission ‘Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation’ (2018) STATEMENT/18/3889 <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889)> accessed on 10.05.2022.

White Paper on Artificial Intelligence - A European approach to excellence and trust', Brussels, 19.2.2020 COM (2020) 65 final.

European Council

European Council, European Council meeting (19 October 2017) – Conclusion EUCO 14/17, 2017, 8.

European Council, Presidency conclusions – ‘The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change’ 11481/20 (2020).

European Council, Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020.

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012 (INL).

Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767.

Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts COM (2021) 206 final (’AI Act’)

Secondary sources

Books

Agarwal S, Mishra S, *Responsible AI: Implementing Ethical and Unbiased Algorithms* (1st ed Springer 2021)

Bradford A, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).

Brownsword R, *Law, Technology and Society Reimagining the Regulatory Environment* (Law, Science and Society 2019).

Brunton F, Fay Nissenbaum H, *Obfuscation: A User’s Guide for Privacy and Protest* (MIT Press 2016).

Cave S, Dihal K, Dillon S, *AI Narratives: A History of Imaginative Thinking about Intelligent Machines* (Oxford University Press; 2020:1-22) <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198846666.001.0001/oso-9780198846666> accessed 10.05.2022.

Claes E, Duff A, Gutwirth S (eds), *Privacy and the Criminal Law* (Intersentia 2006).
Cohen JE, *Between Truth and Power. The Legal Constructions of Informational Capitalism* (Oxford University Press 2019).

Craig P, De Búrca G, *EU Law - Text, Cases, and Materials* (7th edn, Oxford University Press 2020).

De Franceschi A, Schulze R (eds), *Digital Revolutions – New challenges for Law* (C.H. Beck, 2019).

Fitsilis F, *Imposing Regulations on Advanced Algorithms* (Springer 2019).

Ilten C, Kroener C, Neyland D, Postigo H, Guagnin D, Hempel L (eds.), *Managing Privacy through Accountability* (Palgrave Macmillan 2012)

Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013).

Krzysztofek M, *GDPR: data protection in the European Union* (Kluwer Law International, 2021).

Mayer- Schönberger V, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2011).

Mayer-Schönberger V, Cukier K, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (First Mariner Books 2015).

Nisbet R, Miner G, Yale K, *Handbook of Statistical Analysis and Data Mining Applications* (1st edn, Elsevier 2018).

Peng S, Lin C, Streinz T (eds.), *Artificial intelligence and international economic law - disruption, regulation, and reconfiguration* (Cambridge University Press 2021).

Pérez J, Badía E, Sáinz Peña RM (eds), *The Debate on Privacy and Security over the Network: Regulation and Markets* (36 Ariel 2012).

Polanyi P [1944], *The Great Transformation* (Beacon Press 2001)

Russell SJ, Norvig P, *Artificial Intelligence: A Modern Approach* (3rd edn, Prentice Hall Series, 2009).

Sovrano F, Vitali F, Palmirani M, *'Modelling GDPR-Compliant Explanations for Trustworthy AI'* in Electronic Government and the Information Systems Perspective (Springer International Publishing 2020).

Vrabec HU, *Data Subject Rights under the GDPR* (Oxford Scholarship Online 2021) <DOI:10.1093/oso/9780198868422.001.0001>.

Zavrsnik A (ed.), *Drones and Unmanned Aerial Systems* (Springer 2016).

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019)

Journal Articles

Arnow G, '*Apple Watch-ing You: Why Wearable Technology Should Be Federally Regulated'* (2016) 49 LOY. L.A. L. REV. 607.

Calo R, '*Peeping HALs: Making Sense of Artificial Intelligence and Privacy*' (2010) European Journal of Legal Studies 2, 3, The Future of... Law & Technology in the Information Society,<http://hdl.handle.net/1814/15123171> accessed 16.05.2022.

Cao Y, Jang J, '*Towards Making Systems Forget with Machine Unlearning',* IEEE Symposium on Security and Privacy (2015) 483 <. DOI 10.1109/SP.2015.35>.

Cath C, Wachter S, Mittelstadt B, Taddeo M, Floridi L, *'Artificial Intelligence and the 'Good Society': the US, EU, and UK approach'* (2018) Sci Eng Ethics 24, 505–528.

De Hert P, Hanon R, Junklewitz H, Malgieri G, Sanchez I, *'Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making'* (2022) IEEE computational intelligence magazine, 73-85.

de Montjoye Y-A, *'Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models'* (2019) 10 Nature Communications 3069.

Edwards L, Veale M, '*Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For'* (2017) 16 Duke Law and Technology Review 18.

El Emam, Rodgers, Malin, '*Anonymising and Sharing Individual Patient Data'* (2015) 350 BMJ h1139.

Esposito E, '*Algorithmic Memory and the Right to Be Forgotten on the Web'* (2017) 4 Big Data & Society 1.

Fabbrini F, *'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States'*, Harvard Human Rights Journal vol. 28, 65.

Fosch Villaronga E/Kieseberg P/Li T, ' Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten' (2018) 34 Computer law & Security Review 304, 305.

Frosio GF, *'Right to Be Forgotten: Much Ado about Nothing'* (2017) 15 Colorado Technology Law Journal, 307.

Fruhwirt P, Kieseberg P, Weippl E, *'Using internal MySQL/InnoDB B-tree index navigation for data hiding*' in: Peterson, G., Shenoi, S. (eds) Advances in Digital Forensics XI. DigitalForensics 2015, IFIP Advances in Information and Communication Technology vol 462, 179-94 (Springer International Publishing 2015).

Hacker P, '*A legal framework for AI training data—from first principles to the Artificial Intelligence Act'*, (2021) Law Innovations and Technology vol. 13 no. 2, 257 <https://doi.org/10.1080/17579961.2021.1977219>.

Hintze M, '*Viewing the GDPR Through a De-identification Lens: A Tool for Compliance, Clarification, and Consistency'* (2018) 8 International Data Privacy Law 86.

Jobin A, Ienca M, Vayena E, *'The global landscape of AI ethics guidelines'* (2019) Nat Mach Intell 1: 389–399 <https://doi.org/10.1038/s42256-019-0088-2>.

Kaplan B, '*Selling Health Data: De- Identification, Privacy, and Speech'* (2015) 24 Cambridge quarterly of healthcare ethics 256.

Karjalainen T, *'All Talk, No Action? The Effect of the GDPR Accountability Principle on the EU Data Protection Paradigm'* (2022) EDPL 1/2022, 27.

Koops B-J, '*Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice'* (2011) 8 SCRIPTed 229.

Krotoszynski, RJ Jr., '*The Polysemy of Privacy'* (2013) 88 IND. L.J. 881, 906.

Kühling J, Klar M, '*Speicherung von IP-Adressen beim Besuch einer Internetseite*' [engl. 'Retention of IP addresses when accessing a website'] (2017) Zeitschrift für Datenschutz 27, 28.

Larson RG, '*Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech'* (2013) 18 COMM. L. & POL'Y 91, 104

Lynskey L, *'Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly'* <https://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/> accessed 08.05.2022.

Ostveen M, '*Identifiability and the Applicability of Data Protection to Big Data'* (2016) 6 International Data Privacy Law 299.

Papakonstantinou V, De Hert P:

'EU lawmaking in the Artificial Intelligent Age: Act-ification, GDPR mimesis, and regulatory brutality' (2021), <https://europeanlawblog.eu/2021/07/08/eu-lawmaking-in-the-artificial-intelligent-age-act-ification-gdpr-mimesis-and-regulatory-brutality/> accessed 16.05.2022.

'*Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI'* (2021) <https://europeanlawblog.eu/2021/04/01/post-gdpr-eu-laws-and-their-gdpr-mimesis-dga-dsa-dma-and-the-eu-regulation-of-ai/> accessed 10.05.2022.

Rubenfeld J, '*The Right of Privacy'* (1989), 102 HARV. L. REV. 737.

Schwartz PM, *'Global Data Privacy: The EU Way'* (2019) 94 NYU Law Review 771.

Sellars C, *'ICO launches guidance on AI and data protection'*, C.T.L.R. 2021, 27 (1).

Tsesis A, '*The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data'* (2014) 49 Wake Forest Law Review 433,

Ufert F, '*AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?'* (2020) European Papers vol. 5 no. 2 <https://www.europeanpapers.eu/en/europeanforum/ai-regulation-through-the-lens-of-fundamental-rights> accessed 16.05.2022

van Alsenoy B, Kuczerawy A, Ausloos J, *'Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?'* (2013) ICRI Research Paper 15, TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy, 42, <https://ssrn.com/abstract=2321494> accessed 16.05.2022.

Veale M, Binns R, Edwards L, *'Algorithms that remember: model inversion attacks and data protection law'* (2018) Phil. Trans. R. Soc. A <https://doi.org/10.1098/rsta.2018.0083>.

Websites/Miscellaneous

AI Alliance, <https://ec.europa.eu/digital-single-market/en/european-ai-alliance> accessed on 16.05.2022.

Artificial Solutions, *'Homage to John McCarthy, the Father of Artificial Intelligence (AI)'* (2020) <https://www.artificial-solutions.com/blog/homage-to-john-mccarthy-the-father-of-artificial-intelligence> accessed 16.04.2022.

Atomium European Institute for Science, Media and Democracy, *'AI4People's 7 AI Global Frameworks'* (2020) <https://www.eismd.eu/ai4people/> accessed 10.05.2022.
Avocats M, '*Artificial Intelligence and the GDPR: how do they interact?'* (2017) <http://www.avocats-mathias.com/wp-content/uploads/wp-post-to-pdf-enhanced-cache/1/artificial-intelligence-gdpr.pdf> accessed 17.05.2022.

Bayer J, Bitiukova N, Bárd P, Szakács J, Alemanno A, Uszkiewicz E, *'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its member states'*, Study, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament (2019).

BfDI, *'Praktische Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II")'*<https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html> accessed 08.05.2022.

Cavoukian, Castro, '*Big Data and Innovation, Setting the Record Straight: De-Identification Does Work'*, Office of the Information and Privacy Commissioner, Ontario, 2014.

Centre for Information Policy Leadership, '*CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data (Discussion draft)*' (2017) 33 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf > accessed 16.05.2022.

ECP Platform for the Information Society, Artificial Intelligence Impact Assessment, The Netherlands (2019).

Eurofound, *'Softlaw'* (2011) <https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/soft-law> accessed 09.05.2022.

European Data Protection Board (EDPB); until 2018: Article 29 Working Party

Article 29 Working Party <https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en> accessed 10.05.2022.

Article 29 Working Party, *'Opinion 4/2007 on the concept of personal data'*.

Article 29 Data Protection Working Party*, 'Opinion 05/2014 on Anonymisation Techniques', WP 216* (2014)

Article 29 Working Party '*Opinion 06/ 2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/ 46/ EC'* (2014) 11.

'Guidelines 5/ 2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)' (2019).

'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (2019).

EISMD, AI4People, <https://www.eismd.eu/ai4people/> accessed on 23.04.2022.

'AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations' (2018).
Report on Good AI Governance: 14 Priority Actions, a S.M.A.R.T. Model of Governance, and a Regulatory Toolbox (2019)
'AI4People´s 7 AI Global Frameworks' (2020)
'5 AI4 People´s conversation' (2022)

European Commission´s High Level expert Group on Artificial Intelligence ('AI-HLEG'),

'A definition of AI: Main capabilities and scientific disciplines' (2018).

'Ethical Guidelines for Trustworthy AI' (2019).

European Commission Special Eurobarometer 431 'Data Protection' (2015) <https://data.europa.eu/data/datasets/s2075_83_1_431_eng?locale=en> accessed 10.05.2022.

European Union Agency for Fundamental Rights (FRA),
'Getting the future right – Artificial Intelligence and Fundamental Rights' (2020).

'Data protection and privacy' (2020).

Factsheet on the Right to Be Forgotten ruling (C-131/12) <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 17.05.2022.

GDPR.EU, *'What is GDPR, the EU's new data protection law?*' <https://gdpr.eu/what-is-gdpr/#:~:text=The%20regulation%20was%20put%20into,tens%20of%20millions%20of%20euros.> accessed 29.04.2022.

Hunton privacy Blog, *'CIPL Submits Comments to Article 29 WP's Proposed Guidelines on ADM and Profiling'* (2017) <https://www.huntonprivacyblog.com/2017/12/08/cipl-submits-comments-article-29-wps-proposed-guidelines-adm-profiling/> accessed 23.04.2022.

Information Commissioner´s Office (ICO), '*Big data, artificial intelligence, machine learning and data protection'* v2.2 <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 16.05.2021.

Joncckheer T, *'Copying ID documents – Dutch data regulator issues guidance*' (2012) <http://www.privacyandcybersecuritylaw.com/copying-id-documents-dutch-data-regulator-issues-guidance> accessed 16.05.2022.

Mitrou L, Karyda M, '*EU's Data Protection Reform and the Right to Be Forgotten: A Legal Response to a Technological Challenge?'* (5th International Conference of Information Law and Ethics, Corfu-Greece 2012) 10 available at <https://www.icsd.aegean.gr/website_files/proptyxiako/388450775.pdf > accessed 10.05.2022.

Narayanan A, Shmatikov V, '*Robust De-anonymization of Large Datasets'* (2008) Proceedings of the 2008 IEEE Symposium on Security and Privacy 111.

OECD
'Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"' (2013) OECD Digital Economy Papers, No. 222, OECD Publishing, Paris, <https://doi.org/10.1787/5k47zw3fcp43-en>.

’Data-driven Innovation: Big Data for Growth and Well-being’ (2015)

Peuker S, ’Was ist Künstliche Intelliegnz (AI)’ [engl. ’What is Artificial Intelligence (AI)?’] (zeix 2019) <https://zeix.com/durchdacht/2019/12/08/was-ist-kuenstliche-intelligenz-ai/#:~:text=Der%20AI%20Effekt,der%20Mensch%20Intelligenz%20brauchen%20w%C3%BCrde.%C2%BB> accessed 22.04.2022.

Reding V, ‘*Your Data, Your Rights: Safeguarding Your Privacy in a Connected World’* (Speech delivered at Privacy Platform ‘The Review of the EU Data Protection Framework’ (Brussels 16 March 2011).

Rentzhog M, *’The Fourth Industrial Revolution: Changing Trade as We Know It’* (WITA 2019) <https://perma.cc/5NLX-L7VA> accessed 10.05.2022.

Research Gate, *’European Courts Decisions Challenging Interference with Article 7 & Article 8 Rights EUCFR’*, 12-13 <https://www.researchgate.net/publication/331873330_Article_7_Article_8_Rights_EU_Charter_of_Fundamental_Rights_Case_Law_of_EUCFR_and_ECtHR_'A_Note_for_Students_of_EU_Law's_on_Data_Protection_Laws'> accessed 16.05.2022.

Study of the EPRS (European Parliamentary Research Service, Scientific Foresight Unit (STOA)), *’The impact of the General Data Protection Regulation (GDPR) on artificial intelligence’* (2020).

Sweeney L, ‘*Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy’* [2000] Working Paper LIDAP-WP4.

Villani C, Schoenauer M, Bonnet Y, Berther C, Cornut AC, Levin F, Rondepierre B, *’Donner Un Sens a` l’Intelligence Artificielle. Pour Une Stratégie National et Européenne’* [engl. ’Giving meaning to artificial intelligence: for a national and European strategy’] (2018) <https://perma.cc/SLC9-AMNZ> accessed on 16.05.2022.

Warman M, *’Vint Cerf attacks European internet policy’* (Telegraph 2012) <https://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html> accessed 16.05.2022.

Zeit.de, *’Interview Vinton Cerf ”Das ist bestimmt nicht die Welt, die ich wollte"*’ [engl. Interview Vinton Cerf ”This is certainly not the world I wanted”] <https://www.zeit.de/digital/internet/2020-01/vinton-cerf-internet-netzwerke-informatiker-usa> accessed 03.05.2022.

Zuiderveen Borgesius FJ, ‘*Improving Privacy Protection in the Area of Behavioural Targeting’* (PhD Thesis, University of Amsterdam 2014).

Table of Cases