

FACULTY OF LAW

LUND UNIVERSITY

Jacqueline Poucette

The Right to Be Forgotten and AI

Legal Obligations, Technical Limits, and Innovation

JURM02 Graduate thesis

Graduate thesis, Master of Laws program

30 higher education credits

Supervisor: Annegret Engel

Semester: Spring 2025

Table of contents

Summary 4
Sammanfattning 5
Preface 6
Abbreviations 7
Glossary of Terms 8
1 Introduction 9
1.1 Background 9
1.1.1 Interdisciplinary Complexity 11
1.2 Purpose and Research Questions 12
1.3 Method and Material 13
1.4 Current Research 14
1.5 Delimitations 15
1.6 Outline 16
2 The right to be forgotten under GDPR 18
2.1 The legal foundation of the RTBF 18
2.1.1 Structure and Function of Article 17 GDPR 18
2.1.2 Legal interpretation of erasure 19
2.1.3 Personal Data covered by the GDPR 22
2.2 Scope and applicability in AI models 23
2.3 Implementation Challenges 24
2.4 Doctrinal origins 26
2.4.1 The base case: Google Spain (C-131/12) 26
2.4.2 Doctrinal evolution: GC and Others, Breyer 27
2.4.3 Reflections on case law 28
2.5 Chapter Findings and Reflections 29
3 The Technical Limits of Forgetting 31
3.1 Learning and Data Embedding in AI 31
3.2 Technical barriers to enforce the RTBF 32
3.3 Technical methods for ensuring forgetfulness 33
3.3.1 Differential Privacy 33
3.3.2 Machine Unlearning - SISA 34
3.4 LEAKPRO as a compliance framework 35
3.5 Chapter Findings and Reflections 37
4 Addressing Rights and Innovation 39
4.1 Regulatory Tensions between RTBF and AI Innovation 39
4.2 The Cost of Compliance 40

4.3 Regulatory Perspectives of the GDPR in Practice 41
4.3.1 The Business Sector: Svenskt Näringsliv 42
4.3.2 The Public Institutional: Kommerskollegium and IMY . 43
4.3.3 Regulatory Strategy: The Draghi Report and EPRS 44
4.4 Chapter Findings and Reflections 45
5 The RTBF Compliance Gap 47
5.1 Balancing fundamental rights 47
5.2 Static Right in a Dynamic Setting 48
5.3 AI Act and Regulatory Synergies 49
5.4 Bridging Law and Practice 51
5.5 Chapter Findings and Reflections 52
6 Analysis 54
7 Conclusion 56
Bibliography 58

Summary

Artificial intelligence (AI) use has become more relevant in modern society, where its integration into data-driven systems raises legal issues related to the processing of personal data. These issues are particularly important as training AI models, especially machine learning, presents an insatiable appetite for data. This thesis aims to examine how the right to be forgotten (RTBF) under Article 17 of the General Data Protection Regulation (GDPR) can be applied to AI systems. The focus of this study is to examine how an AI model trained on personal data can be required to be modified, completely retrained, or otherwise influenced in order to comply with the RTBF

The analysis is based on a legal dogmatic method, which is supplemented by a legal political method and to some extent an interdisciplinary frame of reference. Central to the thesis are AI systems based on machine learning, where personal data is not stored based on traditional data records. This leads to a challenge in assessing when personal data can truly be considered deleted under Article 17 GDPR, or if the data has retained its impact even after deletion. The study also highlights the difficulties in interpreting the concept of "personal data" in the AI context, where identifiability may be probabilistic rather than direct. Technical solution to aid with deletion to come into focus, where concepts such as differential privacy and machine unlearning are analyzed. There is also a more in-depth example with the LEAKPRO framework, a Swedish research project funded by Vinnova, which is being studied to see how risk-based methods and data leakage profiling can be supportive mitgating tools. These are investigated to explore the possibility of compliance with the right to be forgotten without the need to retrain a model from the phase before the data was incorporated. Tension may arise between GDPR and AI development, which is addressed in the thesis through the views of several stakeholders, such as Svenskt Näringsliv (the Confederation of Swedish Enterprise), Kommerskollegium (the Swedish Chamber of Commerce), IMY and the EU´s institutional bodies. Their perspectives highlight the risks that the application of GDPR in AI development can stifle innovation. They call for a more flexible and technology-adapted interpretation models to address the development of AI in a sustainable way.

This Thesis concludes that there is a compliance gap in the current legal framework. To address this, the development of technical tools and legal interpretative frameworks is needed to certify that Article 17 GDPR has real impact in the AI context. An integrated approach is proposed where technical solutions, such as the LEAKPRO and SISA, can become part of the future data protection compliance architecture.

Sammanfattning

Artificiell intelligens (AI) har blivit mer alltmer aktuell i det moderna samhället och integrering i data-drivna system aktualiserar rättsliga frågor i anknytning till behandling av personuppgifter. Dessa frågor blir särskilt viktiga i samband med träning av AI-modeller som kräver mycket data. Denna uppsats ämnar därför att undersöka hur rätten att bli bortglömd (RTBF) enligt Artikel 17 i dataskyddsförordningen (GDPR) bör tillämpas vid AI-modellträning. Frågeställningen som blir central för denna uppsats är därför hur en AI-modell tränad på personuppgifter måste modifieras, tränas om från initial fasen eller på annat sätt påverkas för att uppfylla rätten till att bli glömd.

Analysen bygger på rättsdogmatisk metod, vilken kompletteras med rättspolitisk metod, med en till viss del tvärvetenskaplig referensram. Centralt för uppsatsen är AI-system baserade på maskininlärning, där personuppgifter inte lagras utifrån traditionella dataposter. Detta leder till en utmaning att bedöma när personuppgifter verkligen kan anses raderade enligt Artikel 17 GDPR, eller om persondata kan bibehållen påverkan även efter radering. Uppsatsen belyser även svårigheten kring tolkning av begreppet ”personuppgifter” i AI-sammanhang, där möjligheten att identifiera en person kan vara probabilistisk i stället för direkt. Tekniska lösningar för att möjliggöra radering hamnar i fokus, där åtgärder så som differential privacy och machine unlearning analyseras. Det finns även en utgångspunkt i LEAKPRO, ett svenskt forskningsprojekt finansierat av Vinnova, som studeras för att se hur riskbaserade metoder och data läckageprofilering kan användas som ett hjälpverktyg. Dessa undersöks för att utforska möjligheten till efterlevnad av rätten att bli glömd utan att en modell behöver tränas om från fasen innan persondata var inkorporerad. Det kan uppstå spänningar mellan GDPR och AI-utvecklingen, vilket behandlas i uppsatsen genom synpunkter från flera aktörer, såsom Svenskt Näringsliv, Kommerskollegium, IMY och EU:s institutionella organ. Deras perspektiv belyser riskerna kring GDPR´s tillämpning i AI-utveckling kan hämma innovationen. De ber om mer flexibla och teknik anpassade tolkningsmodeller för att bemöta utvecklingen av AI på ett hållbart sätt.

Uppsatsen drar slutsatsen att det finns ett påtagligt ”compliance gap” i nuvarande rättspraxis. För att lösa detta behövs en utveckling av tekniska verktyg och rättsliga tolkningsramar för att säkerställa att Artikel 17 GDPR får verklig genomslagskraft i AI sammanhang. I denna kontext föreslås en integrerad strategi där tekniska lösningar, såsom LEAKPRO och maskininlärningsanpassad radering, som kan bli en del av framtidens efterlevnadsarkitektur för dataskydd.

Preface

I would like to thank my supervisor Annegret Engel for valuable judgement and support throughout this thesis.

This project was written in collaboration with RISE as a part of their LEAKPRO initiative. I´m incredibly grateful for this opportunity to engage in research with practical relevance and societal impact. A heartfelt thank you to Emmie at RISE for her generous support, insightful ideas, and guidance.

I´m deeply grateful to my family and Christian for your encouragement and support.

Stockholm, May 2025

Jacqueline Poucette

Abbreviations

AI	Artificial intelligence
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
EDPB	European Data Protection Board
EPRS	European Parliamentary Research Service
EU	European Union
GDPR	General Data Protection Regulation
IMY	Swedish Authority for Privacy Protection (Integritets-skyddsmyndigheten)
ISO	International Organization for Standardization
RTBF	Right to Be Forgotten
SA	Supervisory Authority
SISA	Sharded, Isolated, Sliced and Aggregated
TFEU	Treaty on the Functioning of the European Union

Glossary of Terms

Anonymization	A process that removes all identifiable elements from data so that no individual can be identified, directly or indirectly.[1]
AI model	The term AI model refers to the trained part of an AI system, which means the statistical model that has learned from data during the training phase, especially for machine learning.[2]
AI system	In this thesis, the term AI system refers to machine-based systems, which operates with some level of autonomy. It uses input to generate outputs, such as content, prediction, recommendations, or decisions.[3]
Machine Learning (ML)	A type of AI where algorithms learn patterns from data to make predictions or decisions. In ML, personal data is not stored directly but becomes part of the model´s internal structure.[4]
Pseudonymization	A method where identifiable data is replaced with a code or other identifier, but the person can still be identified using additional information.[5]
Re-identification	The process of identifying a person from data that was supposed to be anonymous or pseudonymous, using additional information or technical methods.[6]
Risk-based approach	A principle in the GDPR that requires data controllers to apply stronger protection when data processing poses higher risks to individuals´ rights and freedoms.[7]

[1] 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 on the free movement of such data (GDPR) [2016] OJ L119/1, recital 26

[2] Europeans Data Protection Board (EDPB), Opinion Opinion 28/2024 on Certain Data Protection Aspects Related to the Processing of Personal Data in the Context of AI Models, (17 December 2024) para. 23

[3] Regulation (EU) 2016/679 of the European Parliament and the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations and Directives (Artificial Intelligence Act) [2024] OJ L1689/1, Article 3(1)

[4] Lucas Bourtoule et al., "Machine Unlearning" (2021) IEEE Symposium on Security and Privacy, p. 141

[5] GDPR, Article 4(5) GDPR

[6] EDPB Opinion 28/2024 (n 2) para. 43

[7] GDPR, Articles 24, 25 and 32

1 Introduction

1.1 Background

> *"Personal data is the new oil of the internet and the new currency of the digital world."*
>
> - Meglena Kuneva, European Consumer Commissioner [8]

This observation, brought forward at a 2009 roundtable on online data collection, underlined the economic and social relevance of personal data. By portraying personal data as a form currency, Kuneva urged the need to balance business interests with privacy rights.[9] These rights have its origins from the fundamental rights of the European Union for individuals to have their private life respected and their personal data protected under the Charter for Fundamental Human Rights.[10] This perspective is very relevant in the context of contemporary data-driven artificial intelligence(AI) systems, which rely on the collection, processing, and use of personal data. Where personal data is used as a resource that provides insight and supports to support evolving data-driven innovation. There is a clear incentive to use personal data for machine learning, as it requires huge amounts of data, but it also raises difficult questions on compliance with privacy law.[11]

To address such regulatory uncertainties, the European Union adopted the General Data Protection Regulation (GDPR) in 2016, which came into effect in 2018. In the way the GDPR established a comprehensive legal framework that sought to safeguard the right to privacy and informational self-determination, and at the same time make digital innovation sustainable.[12] An important provision is the right to erasure, or "right to be forgotten" (RTBF), codified in Article 17 GDPR. This article provides individuals the right to request erasure of their personal data under specific circumstances, which is important for core data protection principles that aim to achieve a high level of data protection.[13]

---

[8] Meglena Kuneva, "Roundtable on Online Data Collection, Targeting and Profiling" (Keynote Speech, Brussels, 31 March 2009)

[9] Ibid

[10] Charter of Fundamental Rights of the European Union [2000] OJ C363/1. Articles 7 and 8

[11] Daniel J. Solove, "Artificial Intelligence and Privacy" (2025), *Florida Law Review*. p. 26

[12] GDPR, Recital 2

[13] European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018) 2 nd edn, pp. 221and 223

The introduction of AI, and in particular machine learning (ML) systems, has brought new challenges to ensuring compliance with Article 17 GDPR.[14] Unlike a traditional database, which stores data in retrievable records, ML systems process data through statistical inference. Instead of storing it in conventional format, ML algorithms integrate and encode the data into the model's internal architecture and parameters.[15] This process is often performed in ways that lack transparency and reversibility.[16] The data storage function in AI systems can create a tension between the static legal right of erasure and the dynamic, probabilistic nature of AI systems. Scholars such as Tiffany Li have noted that AI models may retain influence or traces of personal data even after erasure efforts, meaning that the data can persist in the outputs, which she describes as an algorithmic shadow.[17]

The landmark case of Google Spain v. AEPD and Mario Costeja González (C-131/12) clarified, through the Court of Justice of the European Union (CJEU), the existence of the RTBF under EU law. Granting individuals, the right to request the removal of personal information under certain conditions.[18] Several cases have followed the reasoning presented in the Google Spain case. The European Data Protection Board (EDPB) has addressed the RTBF and its implications to AI, as it points out that there needs to be a careful assessment, evaluating if and where there are risks for re-identification.[19]

The geopolitical and economic landscape affects the understanding and application of data protection, particularly in the emerging fields such as AI. In the Draghi report it is found that the EU currently falls behind the United States and China in developing functional AI technologies, with over 70% of leading AI models originating in the U.S. since 2017.[20] The report has raised this as an important issue, where AI is of strategic importance for future digital competitiveness. Concerns are raised on the risks associated with strict data protection law, on the one hand it is important for protecting rights, on the other hand it runs the risk of stifling innovation and disrupt progress in critical sectors such as energy, healthcare, and defence.[21] These concerns

[14] Giovanni Sartor and Fransesca Lagioia. *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (EPRS, June 2020) pp. 74-75

[15] Michael Veale, Reuben Binns and Lilian Edwards, "Algorithms That Remember: Model Inversion Attacks and Data Protection Law", (2018) 376(2122) *Philosophical Transactions of the Royal Society A* 20180083, p. 9

[16] Sartor and Lagiola (n 14) pp. 53 and 56; Carolin Kemper, "Kafkaesque AI? Legal Decision-Making in the Era of Machine Learning". (2020) 24(2) *Intellectual Property & Technology Law Journal*. 251, p. 254-255

[17] Tiffany C. Li, "Algorithmic Destruction", (2022) 75 SMU Law Review. 479, p. 490-492

[18] Case C-131/12, *Google Spain v AEPD*, paras. 93, 97-99

[19] EDPB Opinion 28/2024 (n 2) paras. 43, 58

[20] European Commission. The Future of European Competitiveness: A Competitiveness Strategy for Europe – Part A (September 2024), p. 24

[21] Ibid. pp. 24-26

have been reflected in policy debates, when the Danish Digital Mister Caroline Stage Olsen told reporters "A lot of good things about GDPR, [and] privacy is completely necessary. But we don´t need to regulate in a stupid way. We need to make it easy for business and companies to apply".[22]

Applying the RTBF in AI systems is still not fully explored or clarified. Despite an established legal framework, technical compliance issues emerge and seek answers. This thesis aims to explore this relation between privacy and technological advancements.

1.1.1 Interdisciplinary Complexity

This thesis undertakes an in-depth analysis of the right to be forgotten in the age of AI, where it is important to understand the underlying concepts that circulate in legal and technical discourse. These terms are not always clearly defined within the legal field and can act more as clusters of interconnected meanings that can change depending on the disciplinary context. This conceptual complexity can pose a challenge for legal analysis[23], particularly with Article 17 GDPR and its application to AI models, as it is a rather new area.[24] Concepts such as "re-identification", "risk-based approach", and "anonymization" may appear legally defined, but their application within AI systems can be contested or technically difficult.[25] As a consequence, this thesis relies on a structured conceptual framework that classifies and examines the terms through four categories. First, formal concepts, which are the ones defined in the GDPR. These are formally clarified, such as personal data, processing and the RTBF.[26] Second, functional legal concepts, which depend on the concept in which they are used. These are dependent on situation, such as risk-based approach, technical and organizational measures.[27] Third, steering concepts, which constitute the technical disciples but influence legal obligations, such as re-identification, differential privacy, and machine unlearning.[28] Fourth,

[22] Ellen O´Regan, "Europe´s GDPR Privacy Law Is Headed for Red Tape Bonfire within weeks". Politico (3 April 2025)

[23] Cecilia Magnusson Sjöberg, "Legal AI from a Privacy Point of View; Data Protection and Transparancy in Focus", in Sonya Petersson (ed) *Digital Human Sciences: New Objects-New Approaches* (Stockholm University Press 2012), p. 186

[24] See EDPB Opinion 28/2024 (n 2)

[25] Zeyu Zhao, "The Application of the Right to be Forgotten in the Machine Learning Context: From the Perspective of European Laws" (2022) 31 *Catholic University of Law and Technolgy* 73, p. 85

[26] See GDPR, Article 4(1), Article 4(2) and Article 17(1)

[27] See GDPR, Articles 24, 25 and 32

[28] See EDPB Opinion 28/2024 (n 2) para. 43; Cynthia Dwork, (2006). "Differential privacy". In M. Bugulesi, B. Preneel, V. Sassone, & I. Wegener (Eds.), *Automata, languages, and programming: 33rd international colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006. Proceedings, part II* (Springer 2006). p. 2 pp. 1-2; Bourtoule et al. (n 4) p. 141

historical concepts, which has developed over time and which reflects this with legal history and doctrine.

To assist a readability, a glossary has been included after the abbreviations list. It contains short definitions and contextual notes on the key terms used throughout the study.

1.2 Purpose and Research Questions

The purpose of this thesis is to further investigate the RTBF, as codified in Article 17 of the General Data Protection Regulation (GDPR), in the context of artificial intelligence (AI) model training. The primary focus is on machine learning systems and how they process data once it has been used during training. This thesis examines the compliance challenges and legal questions that emerges between Article 17 GDPR and data-driven AI models, then it analyses if there are alternative solutions through technical and organizational safeguards.

This thesis is written within the scope of the LEAKPRO project at RISE, which is an initiative that aims to provide a scalable framework for evaluating privacy risks in AI systems.

This thesis is guided by two main research questions:

- What legal obligations exist under Article 17 GDPR when an individual requests to be forgotten from an AI model trained on personal data, and what technical and legal measures are required to verify actual compliance?

- How is the RTBF under the GDPR be interpreted, considering the technical and regulatory challenges posed by AI system, and what normative choices are needed to achieve sustainable data protection with technological innovation?

To address these overarching questions, the thesis is structured around chapter based sub-questions:

- What legal foundations and case law addresses the scope of Article 17 GDPR and its applicability to the lifecycle of AI training?

- What legal challenges does the technical structure of AI models pose to fulfilling the RTBF?

- How can Article 17 GDPR be interpreted to maintain legal certainty while allowing AI innovation to thrive?

- How can the legal and practical gap between GDPR obligations and AI system behavior be explained?

1.3 Method and Material

This thesis implements a legal doctrinal method as the primary analytical framework, which aims to examine primary legal sources. The legal doctrine of central importance for this thesis is EU data protection law, especially the RTBF under Article 17 GDPR. The doctrinal approach is applied to understand and define primary legal sources such as the GDPR, case law from the Court of Justice of the European Union (CJEU), and interpretative guidance from the European Data Protection Board (EDPB). The method corresponds to traditional legal dogmatic approach, which is applied to determine and clarify applicable law.[29]

In addition to doctrinal interpretation, this thesis incorporates a legal policy argumentation to assess the normative adequacy of the current regulatory in relation to technological realities. The legal policy perspective brings a normative evaluation by examining the balance between data protection and innovation, analyzing not only *de lege lata* (the law as it exists) but then *de lege ferenda (*with a view to the future law*).*[30]

In support of these legal methods, this thesis applies a restricted interdisciplinary approach to engage with technical concepts that are relevant to legal compliance and AI model development. This method helps to understand different concepts, terminologies, and theories together, to allow for a joint understanding of complex and interdisciplinary problems.[31] Its purpose is strictly to inform the legal discussion and to provide an understanding of the complex interdisciplinary problems that can emerge.

This thesis is built around binding legal sources within the EU legal order, with the GDPR as central normative legal frameworks and the Artificial Intelligence Act (Regulation (EU) 2024/1689) as a complementary instrument. With supplementary interpretative guidance from the EDPB, primarily their Opinion 28/2024, which clarifies the obligations under Article 17 GDPR in relation to AI systems. The EDPB´s opinions and guidelines are non-binding and are there as a provisional interpretative aid rather than law, as clarified in Article 70(1)(e)-(f) GDPR. They might be reinterpreted by courts or national authorities in the future. Preparatory legislative documents, such as impact

[29] Aleksander Peczenik, *Vad är rätt? Om demokrati, rättssäkerhet, etik och juridisk argumentation* (Norstedts Juridik 1995, republished 2021 by the Faculty of Law, Lund University) pp. 312-313

[30] Ibid pp. 93 and 173

[31] Vetenskapsrådet. *Tvärvetenskapen – en analys*. (Swedish Research Council 2005), (10) p. 14

assessments and explanatory memoranda, are included to clarify legislative intent.

To complement the legal sources some selected literature by impressive scholars in this field, primarily Daniel J. Solove, Tiffany C. Li and Z. Zhao. In addition, technical reports from applied research provide illustrative material to give insight into practical challenges. These are analyzed together with case law from the CJEU, notably Google Spain (C-131/12), to assess the RTBF and its application to AI model training. The study aims to understand these practical concerns and incorporates stakeholder reports, including from Svenskt Näringsliv and Kommerskollegium, to provide insight from the business sector concerns on GDPR and innovation.

1.4 Current Research

The right to be forgotten, as set out in Article 17 GDPR has been the topic of both academic and jurisprudential analysis. Several studies have focused on the emergence of the right through the Google Spain case, its philosophical foundations in self-determination, and the balance between the right to privacy, freedom of expression and public interest. Scholars such as Daniel J. Solove and Michael L. Rustad have contributed to framing the RTBF as a legal right grounded in the individual's privacy[32], as well as bringing forward the need to act within regulatory and technical constraints. At the time of this thesis being written, legal literature that has analyzed the RTBF have been predominantly in relation to search engine de-indexing.[33] There is still limited doctrinal studies on Article 17 and its application to machine learning models, but the topic is being touched upon in both academic and regulatory discussions.[34]

Recently, the European Data Protection Board (EDPB) published Opinion 28/2024, which is important as it acknowledges that AI-generated outputs may be within the scope of the GDPR. This would indicate legal obligations under the GDPR.[35] At the same time, there is no current step-by-step guidance for the RTBF in an AI context under the GDPR, which leaves the interpretation for erasure vague. Making some question on if there is a requirement explicitly full retraining is necessary, or if there are other acceptable compliance options[36]. The EDPB in their Opinion 28/2024, leaves out how to live up to the standard in clear measurable means, leaving a normative gap to

[32] See Solove (n 11) p. 19-20; Michael L. Rustad, and Sanna Kulevska, (2015). "Reconceptualizing the right to be forgotten to enable transatlantic data flow" (2015). 28(2) *Harvard Journal of Law & Technology* 349, p. 367

[33] See Stefan Kulk, and Frederik Zuiderveen Borgesius. "Google Spain v. Gonzales; Did the court Forget about Freedom of Expression? " European Journal of risk Regulation, 5(3), [Balancing privacy and freedom of expression in search engine indexing context] pp.391-921

[34] Veale, Binns and Edwards (n 15) p. 9; Solove (11) p. 19-20; Zhao (n 25) p. 85

[35] EDPB Opinion 28/2024 (n 2), executive summary

[36] Veale, Binns and Edwards (n 15) p. 9

understand how risk metrics could be interpreted.[37] There are some computer science researchers that explores techniques differential privacy or machine learning, as potential support measures to full retraining. These studies mostly focus on evaluating these methods through computational or statistical metrics and lack comprehensive legal analysis.[38] Some recent projects, from the Nordic, attempt to create tools for profiling and mitigating data leakage in AI systems[39], but they have not yet received regulatory approval.

1.5 Delimitations

This thesis is situated within the legal and regulatory framework of the European Union and is limited to the interpretation and application of the General Data Protection Regulation (GDPR), primary Article 17, which sets out the RTBF. The study does not undertake a comparative analysis with data protection regimes outside of the EU, such as the California Consumer Privacy Act (CCPA) or Brazil´s General Data Protection Law (LGPD), because it would extend the legal scope and purpose of this study.

Core GDPR principles, such as purpose limitation and data minimization, will be discussed to contextualize Article 17, but there will not be an exhaustive examination of other obligations under the regulation. Data Protection by Design and by Default in Article 25 GDPR is referenced to support the section on compliance strategies, but it will not primarily object of analysis. A more in-depth doctrinal analysis would have great but was not considered crucial for the analysis carried out.

The technical aspects of the thesis are limited to machine learning models and the application of the RTBF at the training stage. AI systems will be considered in this context, and will not extend to autonomous systems, real-time decision-making applications, or AI-generated outputs outside their relevance to data retention or erasure. These are interesting, but they would broaden outside a suitable scope for this study. Technical concepts such as machine unlearning and differential privacy are addressed, but these only to understand and examine the options to full retraining. The thesis will not provide a technical evaluation or performance comparison of these methods from a computer science or engineering standpoint, since it would require a technical methodology beyond this thesis.

An ethical, philosophical, or socio-political discussion are not the subject of this thesis as it lies outside the scope of this legal analysis. These perspectives

[37] EDPB Opinion 28/2024 (n 2), executive summary

[38] See for example Bourtoule et al. (n 4)

[39] See AI Sweden, "LeakPro: Leakage Profiling and Risk Oversight for machine Learning models" (AI Sweden, 2024); Project Report; R. Brännvall et al., *Technical Report for the Forgotten-by-Design Project: Targeted Obfuscation for Machine Learning*, (RISE Research Institutes of Sweden, December 2024)

will only be briefly acknowledged when they assist on framing broader implications.

Finally, the regulatory framework analyzed in this study reflects the status as of May 2025, including the adoption of the AI Act (Regulation (EU) 2024/1689) and recent interpretive development, such as the EDPB 28/2024 Opinion.

1.6 Outline

This thesis consists of seven chapters, with each exploring a layer and dimension of RTBF under the GDPR, in the context of artificial intelligence (AI) models, from training stage to deployment. The structure is designed around the core research questions, where each chapter answers a sub-question to examine the compatibility of AI development with legal obligations under Article 17 GDPR and understanding the application of the RTBF in AI model training.

Chapter 2 introduces the legal foundations of the RTBF, studying the doctrinal origins, legal scope, and normative structure. It examines the right´s first appearance in EU jurisprudence through to the later codification in Article 17 GDPR. The chapter analyses the legal conditions for lawful erasure, relevant case law, and considers the interpretative issues that AI systems may contribute with. It aims to answer the sub-question: What legal foundations and case law addresses the scope of Article 17 GDPR and its applicability to the lifecycle of AI training?

Chapter 3 provides the technical background to understand the implementation challenges of the RTBF in AI models. It explores the issue of retaining and processing training data in AI models and looks into why deleting personal data proves difficult. It than studies potential technical solutions, and how these can comply with the current GDPR. The chapter bridges the regulatory and the technical dimensions and tries to meet the sub-question: What legal challenges does the technical structure of AI models pose to fulfilling the RTBF?

Chapter 4 evaluates the tension between data protection and advancement in AI. It assesses the impact of safeguarding fundamental rights on the development of AI systems, and the potential trade-off between data protection and model performance. This chapter incorporates stakeholder perspectives and regulatory commentary, with special attention on the LEAKPRO project to explore compliance mechanism. Therefore, this chapter discusses sub-question: How should Article 17 GDPR be interpreted to maintain legal certainty while allowing AI innovation to thrive?

Chapter 5 examines the current European regulatory and analyses the GDPR’s interplay with the Artificial Intelligence Act (AI Act), relevant

EDPB guidance. It assesses theses instruments and how they can operate in a balanced way, and if they can support the RTBF in AI development, or if they risk stifling it. It further discusses sub-question: How can the legal and practical gap between GDPR obligations and AI system behavior be explained?

Chapter 6 builds on the legal and technical foundations provided by the thesis and provides a comprehensive analysis. It assesses the compliance with Article 17, considers legal interpretations, explores normative developments necessary to bridge law with practice and explores future technical alternatives.

Chapter 7 concludes the thesis and summarizes the key findings. It reflects on how the RTBF should be interpreted in the context of AI model training and proposes potential development and policy recommendations.

2 The right to be forgotten under GDPR

2.1 The legal foundation of the RTBF

The right to erasure, more commonly referred to as the right to be forgotten (RTBF) in this thesis, is an important entitlement under the GDPR. It provides individuals with the fundamental right to privacy[40] and empowers them to request deletion of their personal data under certain conditions. This chapter interprets the legal basis for the right by examining the structure and function of the right to be forgotten. Focusing on clarifying the structure and function of Article 17, the legal interpretation of erasures and the definition of personal data. These components provide legal entitlement, interpretative scope, and definitional clarity to understand the right and how it may apply to artificial intelligence systems.

2.1.1 Structure and Function of Article 17 GDPR

Article 17 GDPR, covered as the Right to erasure ("right to be forgotten"), provides a legal entitlement for individuals to request the removal of their personal data under certain circumstances. The article states:

> "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
>
> (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
>
> (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
>
> (d) the personal data have been unlawfully processed;
>
> (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
>
> (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)." [41]

[40] Charter of Fundamental Rights of the European Union [2000] OJ C363/1. Articles. 7-8

[41] GDPR, Article 17(a)-(f)

Article 17 GDPR functions as a safeguard mechanism that enforces several foundational principles of the GDPR, especially the purpose limitation principle and the storage limitation principle. Its aim is to make certain that personal data is not retained or processed longer than is deemed necessary, lawful or with consent.[42] This provides data subjects with a right over their personal data, reinforcing the principle of self-determination, which is a central part of the GDPR.[43] Despite this, the right is not absolute. Article 17(3) outlines exceptions, and these include where the continued processing is necessary for exercising the right to freedom of expression, compliance with legal obligations, or for archiving purposes in the public interest, scientific, historical, or statistical purposes under appropriate safeguards.[44] This balance of competing rights was reflected in the CJEU´s decision for Google Spain v. AEPD and Costeja (C-131/12), which required careful consideration of the public´s freedom of information against privacy and data protection.[45]

The application of Article 17 on AI can become difficult, as machine learning models embed data rather than store it in discrete records. This creates uncertainty in how the concept of erasure should be interpreted in technical terms, since the GDPR does not clearly state what erasure constitutes in the AI context.[46] Although it provides a timespan in which erasure must occur "without undue delay" when a legal ground applies.[47] Here, the proportionality principle, under Article 52 the Charter of Fundamental Human Rights, becomes important. This highlights that limitations on fundamental rights are permitted when necessary, lawful, and proportionate in relation to legitimate objectives. Recital 4 GDPR similarly frames data protection in relation to broader societal needs.[48]

To comply with the RTBF, it follows that the data must no longer be retrievable or inferable, either by the controller or by third parties with reasonable means.[49] In cases where the data has been shared, the controller should follow reasonable steps to inform other controllers of the erasure request.[50] The erasure must be completed in the specified period of time of one month, unless specific circumstances apply, if so, the controller must inform the data subject and justify the delay.[51]

2.1.2 Legal interpretation of erasure

[42] GDPR, Article 5(1)(b) and 5(1)(e)
[43] Rustad and Kulevska (n 29) pp. 356 and 359
[44] Article 17(3)(a-d) GDPR
[45] Case C-131/12, *Google Spain v AEPD* , para. 81
[46] Veale, Binns and Edwards (n 15) p. 9
[47] GDPR, Article 12(3)
[48] See also Charter of Fundamental Rights of the European Union [2000] OJ C363/1; Article 52: GDPR, Recital 4
[49] GDPR, Recital 26
[50] GDPR, Article 17(2), Article 19, and Recital 66
[51] GDPR, Article 12(3) and Recital 59

The GDPR provides data subjects with the right to request the erasure of personal data under Article 17, but the legal meaning of erasure remains imprecise. The Regulation sets out the legal grounds that trigger the right to erasure, but the precise scope and procedural expectations lack detailed clarification. For an AI model it can be expected that compliance with the right to erasure requires deletion of the personal data that was used as an input and the influence of those specific data points in the trained model.[52] Erasure is not defined as a stand-alone act, but as a form of processing. Where Article 4(2) GDPR clarifies that processing includes "any operation or set of operations performed on personal data or sets of personal data". The classification of erasure as an active form of processing demonstrates its status as a controlled and accountable legal obligation, not just a technical measure.[53] This follows the framework of fundamental GDPR principles such as purpose limitation, storage limitation, and accountability.[54]

It is Article 17(1) GDPR that sets out the conditions under which erasure should be granted. These grounds determine when erasure is required but does not cover how this procedure should be executed.[55] Then Article 12(3) GDPR adds that request must be carried out "without undue delay", which introduces a procedural dimension. Where applicable, the controller should on top of that take the reasonable steps to inform other controllers processing the same data, creating a relational obligation outside of internal erasure.[56]

The lawfulness of processing is outlined in Article 6 GDPR. Where AI developers may seek to rely legitimate interest for their data processing under Article 6(1)(f), which requires the use of a three-part balancing test. This test first part looks towards the pursuit of a legitimate interest by the controller or a third-party or to whom the data in question is disclosed to. The second part turns towards if the processing is in the purpose of the legitimate interest, and the third part takes fundamental rights and freedoms of the data subject in consideration, as it can take precedence over initial interest.[57] Applying this test to AI is complex due to the lack of transparency in model behavior and the difficulty in assessing if personal data continues to have residual influence within the model´s parameters. The EDPB, in Opinion 28/2024, clarifies that the balancing test under Article 6(1)(f) does not only apply to the initial stage of data collection. The test should be considered in all steps throughout the

[52] Kris Shrishak, *AI–Complex Algorithms and Effective Data Protection Supervision: Effective implementation of data subjects' rights*. (EDPB, March 2024), p. 4; Veale, Binns and Edwards (n 15) pp. 1-2 and 9

[53] Luca Tosoni and Lee A. Bygrave., "Article 4(2): Processing", in C Kuner., L. A. Bygrave, an C Docksey, (eds), *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update*, pp. 31-32

[54] GDPR, Article 5(1)(b), Article 5(1)(e) and Article 5(2)

[55] Ibid, Article 17(1)

[56] Ibid, Article 12(3), Recital 59 and Recital 66

[57] Case C-708/18, TK v. Asociatia de Proprietari bloc M5A-ScaraA, para. 40; Herke Kranenborg, "*Article 17: Right to erasure", in Kuner, C., Bygrave, L. A. & Docksey, C. (eds), The EU General Data Protection Regulation (GDPR): A Commentary – 2021 update*, p. 74

data lifecycle, to safeguard in relation to the risks for long term usage.[58] To invoke legitimate interest, an AI developer must conduct a thorough data protection impact assessment, demonstrating the necessity, proportionally and the implementation of appropriate safeguards, possibly including an effective erasure mechanism.

The GDPR addresses two related concepts that are crucial for the interpretation of erasure, and these are pseudonymization and anonymization. Pseudonymization, defined in Article 4(5), refers to a concept where personal data is processed in such a way that it cannot be attributed to a specific data subject without additional information. Though, pseudonymized data still qualifies as personal data and remains within the scope of the GDPR.[59] Anonymization is defined by Recital 26, as data where identifiability is eliminated entirely by any means reasonably likely to be used. If data is anonymized in a manner that aligns with irreversibility and no longer constitute identifiable personal data, it falls outside the material scope of the GDPR.[60] There is no concrete harmonized technical standard to verify a successful anonymization from the GDPR, and author Z. Zhao has raised concerns if anonymization could even act as a proportionate tool to establish a practical and sustainable approach for machine learning.[61] Further raising the topic of real-world reliability of anonymization and pseudonymization, arguing that the RTBF should not rely solely on data deletion. Instead proposing stratified technical standards specifically made for the different phases of data processing, from collection to retention and archiving.[62]

Erasure requires a structured legal interpretation to demonstrate compliance with the RTBF. The starting point is the requirement that the data is no longer accessible in a way that could lead to identification, both direct and indirect.[63] Once the RTBF is invoked, the controller is obligated to erase that data, which includes avoiding further use and influence of that data. This aligns with the principles of purpose of limitation and storage limitation.[64] In practice, the controller needs to trace all the relevant data, then evaluate what should be erased, and then establish that deletion is within a reasonable period of time. If the statistical traces remain in the model and makes inferences possible on the data subject it would be unlikely to comply with the RTBF.[65] In accordance with Recital 59, where it is made clear that deletion must take place "without undue delay". In concrete terms, Article 12(3) requires the controller to act within one month of the erasure request, unless there are justifiable

[58] EDPB Opinion 28/2024 (n 2) para. 76

[59] Thomas Zerdick "Pseudonymous Data: Processing Personal Data While Mitigating Risks" [blog] (EDPS, 21 December 2021); GDPR, Article 4(5)

[60] EDPB Opinion 28/2024 (n 2) para. 134; GDPR, Recital 26

[61] Zhao (n 25) pp. 88 and 93

[62] Ibid, p. 106

[63] GDPR, Article 4(1) and Recital 26

[64] GDPR, Article 5(1)(b) and (e)

[65] Zhao (n 25) p. 94

reasons for an extension. The reasons for extension should be provided to the data subject and the extension should only be allowed for up to two additional months.[66]

Understanding the legal definition of erasure forms the foundation to understand how the RTBF can or cannot be realized in the context of machine learning systems. This will be further examined in later chapters, where it is important to understand that erasure under the GDPR requires more than mere deletion.[67] The right requires the elimination of identifiability, guided by the principles of necessity, proportionality, and accountability.[68]

2.1.3 Personal Data covered by the GDPR

The central question in assessing the applicability of the GDPR to AI systems is in case the data involved qualifies as personal data under the regulation. Article 4(1) GDPR defines personal data broadly as "any information relating to an identified or identifiable natural person (i.e. data subject)". This definition cover not only directly identifying information, such as names or national identification numbers. In addition, it covers information that when combined with other accessible data, could be used re-identify an individual.[69] The Article 29 Working Party (now the EDPB) introduced in their Opinion 4/2007 on the Concept of Personal Data that identifiability needs to be assess with "all the means reasonably likely to be used" by any party, not only the data controller.[70] This interpretation is supported with Recital 26 GDPR, which further clarifies the meaning of identifiability, by addressing that is with regard to the cost, time, and technology available at the time of the processing and future technological developments.[71] This approach and contextual understanding have been confirmed through the Court of Justice of the European Union (CJEU) in the Breyer judgment (C-582/14). In which the court found that IP address could be classified as personal data in the disposal of a website operator, if third parties (e.g. internet service providers) could reasonably be used to identify and individual. This solidified personal data to be approached in both relational and contextual terms, and not only by direct identifiers.[72] Another significant ruling on the broad definition of personal data Is Nowak (C-434/16), where it concluded that exam answers and examiner´s comments would constitute as personal data. The CJEU then reinforced that personal data is data which can be linked to an identifiable individual from that person's knowledge, abilities to reason and their achievements.[73] In case C-

[66] GDPR, Article 12(3)

[67] Veale, Binns and Edwards (n 15) p. 9

[68] EDPB Opinion 28/2024 (n 2) para. 34

[69] GDPR, Article 4(1)

[70] Article 29 Working Party, Opinion 4/2007 on the concept of personal data (EP 136, 20 June 2007), Section 2.2

[71] GDPR, Recital 26

[72] Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, para. 49

[73] Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, ECLI:EU:C:2017:994, paras 34-39, 53-56

319/22, a vehicles VIN number was recognized as personal data under Article 4(1), and this showed that even a car number, that does not constitute a personal data in itself, could combined with other data be seen as such.[74]

Applying this to an AI context has raised debate on the possibility that trained AI models themselves contain or process personal data. Following the risk-based approach from Recital 26 and the reasoning from relevant case law, a functional and contextual analysis is necessary. This analysis would need to consider not only what data initially used, but in addition examine risk of re-identification through model outputs or adversarial techniques[75] (e.g. membership inference attacks, which can extract or reconstruct personal data from AI models).[76]

2.2 Scope and applicability in AI models

Recent regulatory interpretation has clarified that the scope of the GDPR can go beyond systems that store personal data in a traditionally retrievable format. For example, the Hamburg Data protection Authority (DPA) understood large language models (LLMs) to not store personal data in such traditionally retriable format, for the reason that they operate through data embedding and statistical inferences instead of conventional records. In this regard LLMs were not seen as data bases, but if outputs of such AI systems could contain or resemble personal data, it would then be within inside the scope of the GDPR.[77] As the Hamburg DPA saw it "AI systems that process personal data, particularly in their output, must fulfill data subject rights".[78] Their view reflects a regulatory focus not only on storage to generation, but they recognized the probabilistic nature of AI systems. There seems to be a debated shift from static record deletion to output accountability, not only input-based compliance but a move towards functional privacy oversight throughout the AI lifecycle.[79] There are potential risks through this AI lifecycle, and the Swedish Authority for Privacy Protection (IMY) identifies some issues linked to LLMs. One risk they bring up occurs at the output stage, where there is a possibility of hallucination, which is factually inaccurate but still personally attributable information.[80] Risks such as misattribution raise concerns on

[74] Case C-319/22 *Gesamverband Autoteile-Handel v. Scania* EU:C:2023:837, paras. 46-49, and see the analysis under 2.4.2

[75] Veale, Binns and Edwards (n 15) pp. 1-2 and 9

[76] Reza Shokri et al., "Membership Inference Attacks Against Machine Learning Models" in *Proceedings of the 2017 IEEE Symposium on Security and Privacy* (IEEE 2017) 3 pp. 5-6

[77] Theodore Christakis. "AI Hallucinations and Data Subject Rights under the GDPR: Regulatory Perspectives and Industry Responses" (2024) pp. 3-4

[78] Hamburg Commissioner for Data Protection and Freedom of Information, *Discussion Paper: on Large Language Models and Personal Data*, (July 2024) , p. 9

[79] Christakis (n 77) pp. 3-4

[80] Integritetsskyddsmyndigheten (IMY), *Integritet och ny Teknik: Integritetsrisker kopplade till stora språkmodeller 2020-2024* (IMY 2025), p. 15

compliance, both to the principle of accuracy under Article 5(1)(d) and the outcome and product of Articles 15-17 GDPR.[81]

The legal background for data processing was built around structured datasets, AI brings another type of processing model. The new generation of machine learning models processing, which uses personal data during training, instead absorbed that data into the model.[82] The EDPB seems to share this view by bringing forward that even a probabilistically generated output may fall within the scope of the GDPR if the risk is more than insignificant.[83] Therefore, data controllers should be responsible for ensuring that outputs that are hallucinated or statistically inferred comply with relevant data protection obligations.[84] Special categories of personal data, under Article 9 GDPR, puts a heightened regulatory burden on AI systems that could infer or reproduce such data. Janssen et al. draws attention to the continuous obligation, when processing such sensitive information, to comply with transparency and erasure requirements.[85] Controllers must implement appropriate measures to correctly identify and regulate such outputs, with heightened attention on the high-risk sector.

The difficulties around implementation of traditional erasure methods[86] have gained recognition, with some turning their attention towards complementary technical safeguards. Alternative techniques, such as differential privacy or model fine-tuning, offer partial mitigation, but they still lack explicit legal recognition.[87] Bridging the gap between GDPR´s demands and AI practices should come from deploying technical safeguards together with core principles like data minimization and purpose limitation.[88] Resolving the difficulties will on top of that need the application of Article 25 GDPR, implementing Data Protection by Design and by Default to connect abstract legal norms and technical implementation options.

2.3 Implementation Challenges

Implementation of the RTBF in the context of AI present both legal and technical challenges. One primary challenge that AI models face is the difference between the traditional data storage systems for which the GDPR was designed, and the current machine learning models parameter weights. Tiffany C. Li observation is that even personal data is no longer in a directly identifiable format, instead the data has been transformed and absorbed in a way that

[81] See GDPR, Article 5(1)(d) and Article 15-17

[82] Christakis (n 77) p. 4

[83] EDPB Opinion 28/2024 (n 2) para. 43

[84] See GDPR, Article 5(1)(d) Recital 78

[85] Heleen Janssen et al. "Decentralised Data Prcessing: Personal Data Stores and the GDPR". (2020). *Computer Law & Security Review*, 36(1), p. 51

[86] See Case C-131/12, *Google Spain v AEPD*

[87] Shrishak (n 52) p. 5-6

[88] Sartor and Lagiola (n 14) p. 6-7

it still can leave influence of traces which affect the behavior of a model.[89] Following a RTBF request, the controller needs to check that there has been effective legal erasure under Article 17 GDPR of the personal data in question.[90] Even so, the GDPR lacks procedural specification to guide a controller on how this could be achieved when applied to a complex algorithmic system.[91] However, the GDPR claims a technology neutral status, where it aims to encourage development of technology, such as AI.[92]

To achieve complete erasure in AI models, there might be a risk that removing a single data point requires retraining of the entire mode, which would be an extensive and costly process.[93] The Swedish Authority for Privacy Protection (IMY) has highlighted this difficulty of removing data. They studied the integrity risks in large language models, in particular the meaning and relation to the data being completely absorbed.[94] The European Parliamentary Research Service (EPRS) has attempted to address these legal concerns by suggesting alternatives such as pseudonymization and risk-based minimization, which could be potential options compliance mechanism.[95] Still, it is important pay attention to that these options have not been formally certified in a clear way, which means they do not necessarily neutralize and fulfill the obligations under Articles 5(1)(e) and Article 17 GDPR. Both the EPRS and scholar Els. J. Kindt and Smuha argue that technical measures like pseudonymization and privacy-preserving design are important, but they are insufficient by their own do in depth meet the fundamental rights embedded in data protection law.[96]

RTBF claims are regularly encountered by national data protection authorities (DPAs) across the European Union, but the field is without a comprehensively harmonized legal interpretation.[97] The EDPB, in its Opinion 28/2024, seems to present that an "insignificant" risk of re-identification can place AI generated outputs outside the GDPR´s scope[98], but there is an evident lack of a regulatory threshold for re-identification or any harmonized metric for assessing what should qualify as insignificant. Controllers might find this difficult to interpret, which risks resulting in fragmentation and inconsistent

[89] Li (n 17) pp. 489-490

[90] GDPR, Article 17(1), supported by Article 5(2) and Article 24(1)

[91] Veale, Binns and Edwards (n 15) p. 9

[92] European Data Protection Supervisor (EDPS), *Opinion 4(2020 on the European Commission´s White Paper on Artificial Intelligence – A European approach to excellence and trust,* (29 June 2020) para. 16; GDPR, Recital 6

[93] Ananth Mahdevan and Michael Mathioudakis, ´Cost-aware retraining for machine learning´, (2024) 293 *Knowledge-Based Systems* 111610, p. 1

[94] IMY (n 80) p. 15

[95] Sartor and Lagiola (n 14) p. 6-7

[96] See EPRS (2020), "Reasoning with Personal Data and AI: A Normative Framework", pp. 6-7; N. A. Smuha, "Beyond Data: Artificial Intelligence, Data Protection and the GDPR", in *The Cambridge Handbook of the Law , Ethics and Policy of Artificial Intelligence*, (2020), (Cambridge University Press), pp. 319&321

[97] Christakis (n 77) p. 4

[98] EDPB Opinion 28/2024 (n 2) para. 43 and executive summary

enforcements from controllers. A legal tension is created as the *de jure* requirements of Article 17 collide with the *de facto* structure of modern AI models. The GDPR does not favor one technique for removing data influence, and the legal compliance demands are unclear if full retraining is necessary or the possibility that non-identifiability assurance is enough. There is a need for clarification, both of normative and technical nature, to confirm meaningful implementation of Article 17.[99]

2.4 Doctrinal origins

The RTBF, as formally codified in Article 17 of the GDPR, is traceable by its roots in the jurisprudence of the Court of Justice of the European Union (CJEU). In the EU legal order there has been a strong foundation in self-determination when applying the right to privacy, both in the private and the public sector data processor.[100] Data protection has evolved over the past decade from foundation in consent driven framework.[101] The progress has culminated in several landmark decisions from the CJEU, in which the RTBF was both articulated and bit by bit modelled into a legal right. The jurisprudential articulation of RTBF initially came with the Google Spain v. AEPD and Costeja case (C-131/12).

2.4.1 The base case: Google Spain (C-131/12)

The CJEU laid the legal groundwork for RTBF in the judgment Google Spain SL and Google Inc v. AEPD and Mario Costeja González (2014). The case concerned Mr. Costeja Gonzales and a complaint over continued indexing on outdated information.[102] The Court stated that search engines themselves were to be considered data controllers under Article 2(d) of Directive 95/46/EC, and that the indexing constituted processing of personal data, according to Article 2(b) of Directive 95/46/EC.[103]

Search engine operators would be in charge of removing such data, if it was inadequate, irrelevant, no longer relevant, or excessive.[104] This case strengthened data privacy by introducing a balancing test that weighed Articles 7 and 8 from the Charter of Fundamental Rights of the European Union (the rights to privacy and data protection) against the publics legitimate interest in access to information under Article 11(freedom of expression and information). There was no introduction of an absolute RTBF, but the judgment introduced

[99] Zhao (n 25) p. 85; See also EDPB Opinion 28/2024 (n 2) para. 43
[100] Rustad and Kulevska (n 29) p. 356
[101] Solove (11) p. 20
[102] Case C-131/12, *Google Spain v AEPD*, para. 14
[103] Ibid paras. 28-33
[104] Ibid paras. 93-94

a mechanism through which individuals could reclaim control over their personal data.[105]

2.4.2 Doctrinal evolution: GC and Others, Breyer

The CJEU further developed the RTBF in several subsequent rulings. One relevant case was the one of GC and Others v. CNIL (C-136/17, 2019), which addressed the question on sensitive categories as covered under personal data, under Article 9 GDPR, fall within the scope of the RTBF. The court held search engine operators, as data controllers, must assess request for erasure on case-by-case basis, and provide extra care for sensitive personal data. Sensitive data which can reveal ethnic origin, political opinions, religious beliefs, or sexual orientation must be de-references if they do not meet the legal framework, even without court order.[106]

Another case of importance was Patrick Breyer v. Bundesrepublik Deutschland (C-582/14, 2016). In this case, the CJEU examined if a dynamic IP address, that had been gathered by a website operator, could be placed in the category of "personal data" under Directive 95/46/EC.[107] The court concluded that a dynamic IP address can indeed be personal data. In the occurrence that a data controller could reasonably access additional data held by a third party (e.g. an internet service provider) that would allow to identify the individual behind the IP address.[108] This ruling was significant since it increased the scope on what actually qualifies as personal data under EU law. The CJEU adopted an approach where identification would not be limited only to direct identification, but also to include situations in which identification is possible or reasonably likely.[109] Personal data was thus recognized as context dependent and relational, as opposed to static and absolute, shifting the legal concept in evolving technological environments. In 2023 another case touched upon the scope of personal data in case C-319/22, in which a vehicles VIN number could constitute personal data under Article 4(1). As the VIN together with someone with the reasonable means to enable it, could be associated with a specific person, which supports that objects or number that does not constitute a personal data in itself could together with other data be seen as such.[110] The case supported a contextual reading of identifiability, which clarified where

[105] Ibid. paras. 81-82 and 97; Charter of Fundamental Rights of the European Union [2000] OJ C363/1, Articles. 7-8 and 11; See 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, Articles 2(d) and 2€

[106] Case C-136/17, *GC and Other v. Commission nationale de línformatique et des libertés (CNIL)* ECLI:EU:C:2019:773, Judgment of the Court (Grand Chamber), 24 September 2019, paras. 39 and 66-68

[107] Directive 95/46/EC, [1995] OJ L281/31, Article 2(a)

[108] Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, Judgment of the Court (second Chamber), 19 October 2016. paras. 39–49

[109] Ibid, para. 49

[110] Case C-319/22 *Gesamverband Autoteile-Handel v. Scania*, paras. 46-49

there is a reasonably possible way for indirect re-identification, particularly with publicly or accessible data it could fall within the scope of the GDPR.[111]

A later case that is important is Google C-460/20, where the CJEU in 2022 clarified that data subjects who wants to make referrals based on alleged inaccuracies does not first need to win a case against the content provider, if the data subject can provide sufficient evidence that demonstrates the conditions under Article 17(1) GDPR to apply the RTBF. Reinforcing the RTBF even in absence of initial proof the search engine must oblige to the erasure request where it meets the evidentiary threshold.[112]

2.4.3 Reflections on case law

The CJEU has shaped the development of the RTBF in EU law over the years. Through its decisions, the meaning and regulatory frameworks for data subjects´ rights under Article 17 GDPR have been progressively defined. With the base case Google Spain (C-131/12), the Court established that search engine operators qualify as data controllers and, as such, may be required to remove links to personal data when that data either becomes inadequate, irrelevant, or no longer necessary.[113] The need to balance the data subject´s right to privacy and data protection with the public´s right to access information under Article 11 was central to the judgment.[114] This decision was based in a context of static and easily identifiable data, which could be delisted or erased through traditional methods.[115]

Complementing this development is the judgment in GC and Others v. CNIL (C-136/17), which addresses the application of the RTBF in relation to sensitive data under Article 9 GDPR.[116] The court held that erasure requests impose an obligation on the controller, to be assessed on a case-by-case basis.[117] This reinforced the principle of proportionality and highlighted the importance of weighing competing fundamental rights.[118] The case of Breyer v. Bundesrepublik Deutchland (C-582/14) brought further clarity by expanding the scope of what qualifies as personal data. Where the CJEU found that a dynamic IP address could constitute personal data when combined with additional information that could reasonably lead to the identification of a data subject.[119] This judgment established a foundation for a relational and context-dependent approach to identifiability. Personal data is not limited to directly identifiable information, it extends to data that can be used to identify

[111] Case C-319/22 *Gesamverband Autoteile-Handel v. Scania*, paras. 48-49

[112] Court of Justice of the European Union, *TU and RE v. Google LLC* (judgment)Case C-460/20 ECLI:EU:C:2022:962, paras. 68, 72

[113] Case C-131/12, *Google Spain v AEPD*, paras. 81-99, especially para. 93

[114] Ibid, paras. 81 and 97

[115] Ibid, paras. 93-95

[116] Case C-136/17, *GC and Other v. CNIL*, paras. 53-55

[117] Ibid, paras. 66-68

[118] Ibid, paras. 72-74

[119] Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, para. 49

an individual by reasonable means.[120] The Google (C-460/20) case further extended the scope of the RTBF, by clarifying the context where it could be applied.[121]

These cases represent doctrinal advancements that have shaped the framework on privacy, accountability, and fundamental right. These cases are important guidelines, but they do not offer concrete guidance on the application of these obligation in an AI environment. Unlike the search engines and databases[122], AI models based on machine learning stores data in a different way.[123] The European Data Protection Board (EDPB) has raised this issue in its recent Opinion 28/2024, where they underscore that AI models trained on personal data cannot be presumed anonymous. Controller must demonstrate, through appropriate technical and organizational measures, that risk of reidentification is on an "insignificant" level.[124] The jurisprudence leads the way for interpretations, but they have not yet covered the latest movements. AI systems challenge traditional legal assumptions and further clarification could be useful.

2.5 Chapter Findings and Reflections

The central motive for this chapter has been to clarify the doctrinal, interpretative, and practical scope of the RTBF under Article 17 GDPR, especially in regard to its application to AI systems trained on personal data. The RTBF is rooted in traditional data protection law and jurisprudence but faces challenges when applied to the dynamic technologies based on data embedding, such as machine learning models.[125] The rights legal foundation in Article 17 belongs to a broader constitutional framework of the EU, including the principles of proportionality, accountability, and self-determination.[126] From the Article 17 GDPR there are six grounds where erasure must be granted, but the technical meaning of erasure remains vague in the AI context.[127] Erasure is defined as a form of processing under the GDPR, which reinforces its procedural and accountable character[128], but it is still surrounded with uncertainty, when applied in complex technological environments.

[120] Ibid, para. 49; EDPB Opinion 28/2024 (n 2) paras 29-24
[121] Case C-460/20 *TU and RE v. Google LLC*, para. 77
[122] Case C-131/12, *Google Spain v AEPD,* paras. 93-95
[123] Li (n 17) p. 485
[124] EDPB Opinion 28/2024 (n 2) paras. 29-34
[125] Veale, Binns and Edwards (n 15) pp. 1-2 and 9
[126] See Charter of Fundamental Rights of the European Union [2000] OJ C363/1, Articles 7-8 and 11; GDPR, Article 5(1)(a)-(f)
[127] See GDPR, Article 17(1)
[128] See Luca Tosoni and Lee A. Bygrave., "Article 4(2): Processing", in C Kuner., L. A. Bygrave, an C Docksey, (eds), *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update*, pp. 31-32

Personal data under Article 4(1) GDPR should be interpreted with a broad, contextual, and risk-based manner, as clarified in the Breyer case. The broad definition is crucial in the AI context, as identifiability may be probabilistic or based on indirect indicators instead of direct identifiers. The CJEU has over time endorsed this flexible interpretation, where the RTBF covers cases of indirect or inferred personal data processing, further reaffirmed by the EDPB in its 2024 Opinion.[129]

The jurisprudence has proved important for the RTBF as the Google Spain case solidified it as a balancing right, weighing privacy and data protection freedom of expression and information. Cases that followed such as GC and Others v CNIL and Breyer expanded the scope to include sensitive data and probabilistic identifiability. In the light of these insightful decisions, there is none of these cases that can provide clear guidance on AI training models.[130] This structural difference creates a challenge to provide effective erasure under the GDPR, particularly when it might necessitate retraining or technically complex procedures.[131] The EDPB´s introduction of "insignificant risk" as the measurement for re-identification may shift the focus from input erasure to output accountability.[132] One issue remains unsolved, how the threshold for acceptable residual risk is to be measured to comply with insignificant. Data controllers need to meet the RTBF with a proportionality-based approach that is built upon technical and organizational safeguards, as the GDPR remain technologically neutral but functionally strained in an AI context.

To conclude, there are legal foundations for applying the RTBF to AI model training through legislation and CJEU jurisprudence, but the absence of procedural standards for the architecture of AI systems creates a compliance gap. To address this gap, it would be required to understand the legal and technical and combine a strategy. This constitutes the foundation for the thesis as the following chapters will explore the technical limits of forgetting and the tensions that arises when privacy and innovation needs to coexist.

[129] See Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, EDPB Opinion 28/2024

[130] See Chapter 2.4

[131] See Veale, Binns and Edwards (n 15) pp. 9-10

[132] EDPB Opinion 28/2024, para. 443

3 The Technical Limits of Forgetting

3.1 Learning and Data Embedding in AI

Artificial intelligence models in the modern sense, particularly those based on machine learning, are vastly different from the traditional databases. Most AI models do not store data in retrievable and concrete records, instead they embed data in the AI models learned parameters during the training process. This technical architecture has direct legal implications when data subjects exercise rights such as the right to be forgotten (RTBF) under Article 17 GDPR.[133] When training an AI model, data is put input to adjust internal parameters through a process known as iterative learning[134](iterative means that a specific procedure is repeated over multiple times[135]). The model then "learns" when it extracts patterns from the training data, which are then encoded as numerical values within the network of parameters that constitute the model. The parameters are later used to guide the model in its predictions or generated outputs.[136] As long as these parameters stay immersed in the architecture of the model code, personal data can influence and affect the outputs and behavior, which could constitute processing under 4(1) GDPR.[137]

AI models, such as large language models (LLMs) are usually trained on enormous and diverse sets of data, which can come from different sources such as web scraping of publicly available text or images.[138] Within these massive datasets, developers may struggle to confirm what personal data is included, or if special categories of data under Article 9 GDPR have been processed.[139] It is important to understand that personal data does not only consist of direct identifiers (e.g. names, addresses), it besides that covers subtle indirect identifiers, such as writing style and other unique traits that can be linked to an individual.[140] Once this data is processed and incorporated into a model, it becomes intertwined within the general parameter space. From that point on removing or "forgetting" a single individuals data point retroactively becomes a significant technical challenge.[141]

---

[133] GDPR, Article 17(1). See also Zhao (n 25), pp. 85-86

[134] Kemper (n 16), p. 254

[135] Nivratti Kasture, "Machine Learning: Why It Is an Iterative Process" (Medium, 1 June 2020)

[136] Ian Goodfellow, Yoshua Bengio and Aron Courville, *Deep Learning* (MIT Press 2016), p. 95

[137] Solove (n 11) p. 66

[138] IMY (n 80) pp. 15&17

[139] GDPR, Article. 9; see also Stefano De Luca, and Marina Federico, *Algoritmic Discrimination under the AI Act and the GDPR*. (EPRS, European Parlimentary Research Service, February 2025) p. 2

[140] Paul M. Schwartz, and Daniel J. Solove, (2011), "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York Law Review* 86(6), p. 1841

[141] Zhao (n 25) pp. 85-86

3.2 Technical barriers to enforce the RTBF

Article 17 of the GDPR provides data subjects right to request erasure of personal data, and it is the duty of the data controller to fulfill this obligation. The technical architecture of many AI models poses a significant barrier to fulfill the obligations for legal compliance. In machine learning system, large datasets are incorporated during the training stage, and the data is then split into multiple datapoints. These are then weighted and incorporated into parameter adjustments through iterative updates and spread across interconnected parameters.[142] For that reason, performing technical removal or "forgetting" of a single data subject's personal data is far more complex than merely deleting a file. This challenge stems from that AI models embed data across parameters, making *ad hoc* erasure technically demanding. The issue is then reinforced by the fact that data remnants may still influence a model´s parameters, even after the original dataset has been purged.[143] In practice, many AI systems have additional training rounds, such as reinforcement learning or fine-tuning, which can spread the traces of personal data in different layers of a model. Making targeted erasure both technically complex and expensive. Where full retraining is necessary, or if specialized machine unlearning techniques are needed, the costs of compliance can be heavy.[144]

Even data that has been to all intents and purposes erased may still be found in a models learned internal patterns. One way of detecting this is thorough membership inference attacks, which involves sending carefully designed queries to a model and analyzing its response patterns, by metrics such as confidence scores and output probabilities, to determine if a particular record was likely used in the training process.[145] The membership inference attacks can occur in both white-box setting (where an attacker has direct access to the model´s parameters) and black-box scenarios (typically the customer version, where only input-output behavior is visible).[146] In both scenarios, a successful retrieval of personal data suggests that effective erasure under Article 17 of the GDPR has not been effectively complied with. This seems to be a shared position with the EDPB Opinion 28/2024, as this Opinion highlighted the need for controllers to show that the risk for residual re-identification cannot be higher insignificant.[147]

There are some difficulties with the technical aspects, which can be described as three separate issues. The first issue is that AI systems distributes encoded data over numerous parameters. The deletion of a single data point asks for far more elaborated technical effort than standard practice on data erasing.[148]

[142] Ibid, P. 79
[143] Li (n 17) p. 490
[144] Bourtoule et al. (n 4) p. 143
[145] Shokri et al., (n 76) p. 5
[146] Ibid, p. 3
[147] EDPB Opinion 28/2024 (n 2) para. 43
[148] Li (n 17) p. 490

The second problem is the persistence of re-identification risks, as demonstrated by membership inference attack. The re-identification risk seems to persist even when the data points that where about the data subject has been removed from the dataset.[149] Then, the third technical issue is regarding the GDPR's accountability principle[150], because organizations need to document how they aim to mitigate risks related to personal data leakage and demonstrate ability to secure legal erasure of personal data upon request.[151] Such assurance is difficult without tools like machine unlearning or differential privacy, both of which require thorough verification to verify that no hidden data traces remain.[152] Membership inference attacks could themselves be used to test if the legal requirements are complied with, and failure to comply could expose controllers to regulatory liability.[153] The process in AI systems seems to complicate compliance to Article 17 GDPR, seeking measures that goes beyond simple deletion.

3.3 Technical methods for ensuring forgetfulness

A key aspect of complying with Article 17 GDPR and implementing the right to erasure is defining how to personal data can either be technically remove or reduce its residual influence, once it has been embedded into an AI model´s parameters.[154] To address this issue, several technical methods have been proposed to verify genuine erasure, or "forgetfulness", in AI systems. A preliminary measure already incorporated in the GDPR under Article 5(1)(c), is to strictly follow data minimization. Where the model only process what is necessary for their specific purpose. The risk of re-identification is inherently reduced by limiting the volume and level of detail of the personal data used.[155] In the context of machine learning models, where data is absorbed into the internal parameters, traditional data deletion methods, such as file-level removal, risk being insufficient to achieving legal erasure. The influence of data points may remain embedded in the model's behavior even after an attempt to deletion has been made.[156]

3.3.1 Differential Privacy

Differential privacy involves introducing calibrated "noise" into the training process of a machine learning model. The goal is to prevent the model´s output to not reveal whether or not a specific individual´s data was in the dataset from the original training dataset.[157] This can be achieved through ensuring that each individual´s data only influences the model´s parameters as

[149] Li (n 17) p. 493; Shokri et al., (n 76) p. 1
[150] See GDPR Article 5(2)
[151] EDPB Opinion 28/2024 (n 2) para. 58
[152] Bourtoule et al. (n 4) p. 141
[153] Shokri et al., (n 76) p. 3
[154] Li (n 17) p. 493
[155] EDPB Opinion 28/2024 (n 2) paras. 73 and 97
[156] Bourtoule et al. (n 4), p. 141
[157] Shrishak (n 52) p. 7

imperceptible as possible, thereby mitigate the residual presence of personal data in the model's parameters.[158] By fine-tuning the level of noise at various stages of a models training, the general risk of re-identification becomes lesser. This technique aims to prevent an external observer from confidently determining if a particular individual's personal data was used for the model.[159] It is important to recognize that differential privacy reduces the risk, but it does not disappear fully, as the record of personal data still contributes, even if marginally, to the model's learned parameters. A single data erasure request might not mandate full retraining, but several requests that are met by removing a "bounded but not zero" method could eventually necessitate a more invasive update to the model´s decision making structure.[160]

The EDPB acknowledges that there are techniques which can significantly reduce or eliminate identifiability, and that these provide some appropriate privacy-preserving and their example for such a methodological choice is differential privacy. It is a that aligns with the GDPR´s principle of privacy by design under Article 25 GDPR, as it can act as supporting evidence of efforts made to meet compliance obligations.[161]

3.3.2 Machine Unlearning - SISA

When traditional deletion methods are not enough, other technical solutions have been proposed, one promising being machine unlearning. Machine unlearning introduces methods to selectively remove or neutralize the influence of specific personal data points, without requiring full model retraining of the entire system. One framework that does this is the SISA training framework, which stands for Sharded, Isolated, Sliced and Aggregated. The method divides datasets into segments (shards), to then train separate models on each different shard. Allowing for removal of those segments which contained the personal data that request. Only a smaller part of the modeled needs retraining, providing a resource-efficient methods.[162] This should align with the accountability principle incorporated in the GDPR, as it promotes transparency and traceability.[163] In opinion 28/2024 from the EDPB clarifies that an AI model trained on personal data is not automatically regarded as anonymous, even if the data has been changed *ad hoc.*[164] The effectiveness of machine unlearning is still heavily dependent on its verifiability.

It is important to tell apart machine unlearning from differential privacy. Differential privacy attempts to reduce the influence of a single data point by adding noise in the training phase, which only minimizes the influence and does not remove it entirely. Machine unlearning seeks for reversibility or

[158] Dwork (n 28) p. 2
[159] Ibid, pp. 8-9
[160] Bourtoule et al. (n 4) p. 141
[161] See for example EDPB Opinion 28/2024 (n 2) paras. 52 and 43
[162] Bourtoule et al. (n 4) pp. 142 and 145
[163] EDPB, Guidelines 4/2019 on Article 25, §§86-88
[164] EDPB Opinion 28/2024 (n 2) paras. 43 and 58

complete removal of the data´s influence altogether[165], and that might be even closer to the legal requirement of erasure under Article 17 GDPR.

3.4 LEAKPRO as a compliance framework

AI models are increasingly used in the processing of personal data. Ensuring compliance with GDPR is not only a legal necessity, but as well presents practical challenges.[166] Traditionally, data protection focused on approaching static databases, where traditional deletion or anonymization was enough to fulfill meet the criteria for the RTBF.[167] Modern AI systems are not static databases in the same manner, instead they embed their training data into the model, which challenges traditional deletion methods.[168] There are new methods and projects to address this issue, but if full retraining of a model is needed to comply with the GDPR it could become both technically intensive and costly.[169]

One project attempting the resolve this is LEAKPRO, which is being developed as a risk assessment framework intended to assist organization in profiling privacy leakage in machine learning models. It is an ongoing project coordinated by RISE, funded by Vinnova (project ID 2023-03000).[170] The tools provided by LEAKPRO could support assessments of privacy risks. The objective of the project is to provide an open-source platform, specifically made to assess issues on information leakage in machine learning models, with focus on scalability and relevance.[171] Threats such as sensitive data being extracted through membership-inference or data-reconstruction attacks are central to the project´s scope.[172] As it attempts to systematically test models against different attack styles to help organizations identify vulnerabilities and create risk profiles to provide mitigation advice, enabling the development of mitigation strategies. Vulnerability testing involves testing if a model´s parameters inadvertently could reveal training data, which directly concerns compliance under Article 17 and Article 25 GDPR.[173] The resulting risk profiles assess the likelihood of personal data being reconstructed or inferred, which is crucial to make certain of compliance with data protection requirements.[174] Following a leakage test, organizations could hopefully identify and implement appropriate mitigation strategies, for example using completely anonymized data or to include pseudonymized data. Such

[165] Dwork (n 28) pp. 1-2; Bourtoule et al. (n 4) p. 141

[166] De Luca and Federico (n 117) pp. 1-2

[167] See Zhao (n 25) p. 89

[168] Veale, Binns and Edwards (n 15) p. 9

[169] Mahdevan and Mathioudakis (n 84) p. 1

[170] Vetenskapsrådet, "LEAKPRO: Leakage Profiling and Risk Oversight for Machine Learning Models" (Forskning.se, 2023-2025), funded by Vinnova, Project ID 2023-03000

[171] Ibid

[172] AI Sweden (n 39)

[173] Ibid

[174] GDPR, Recital 26; Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, para. 43

adjustments may reduce exposure of personal data, which could reinforce the organization´s their privacy position.[175]

The EDPB, in its Opinion 28/2024, implies that controllers must systematically assess the residual identifiability in AI models trained on personal data.[176] GDPR brings forward the importance on the obligation of data controllers to implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing.[177] From the EDPB Opinion several state-of-the-arts attacks are mentioned as methods to that can provide successful testing, such as attribute and membership inference, exfiltration, training data regurgitation, model inversion and reconstruction attacks.[178] A membership inference attack can reveal real and tangible personal data that was used to train the model, that data would still be considered embedded in the model's internal parameters.[179] The LEAKPRO tool could expose scenarios in which personal data remain inferable.[180] As clarified in by the EDPB in Opinion 28/2024, data inferred from an AI model´s parameters may constitute personal data, where the residual risk of identification has not been effectively eliminated.[181] For data controllers these risk assessments can potentially assist data controllers in demonstrating compliance with GDPR´s principles, particularly the RTBF under Article 17 and Data Protection by Design and Default under Article 25.[182] Addressing security vulnerabilities early on in the development cycle could be a critical step for any organization to credibly claim compliance with GDPR.[183]

The comprehensive approach from LEAKPRO spans from development to deployment and aims to find a balance between innovative data usage and a robust privacy framework.[184] Within this framework, LEAKPRO attempts to detect information leakage throughout the AI lifecycle. The information from the analysis can provide structured assessment of the residual identifiability risk.[185] Where successful, such technical interventions could potentially reduce the need for full retraining. This could minimize the operational burden of retraining, along with maintaining a high standard of data protection by design.[186]

[175] See GDPR, Article 25(1) and Recital 78
[176] EDPB Opinion 28/2024 (n 2) para. 43
[177] GDPR, Article 25
[178] EDPB Opinion 28/2024 (n 2) para. 55
[179] Solove (n 11). p. 5
[180] AI Sweden (n 39)
[181] EDPB Opinion 28/2024 (n 2) para. 31; GDPR, Recital 26
[182] GDPR, Article 25 and Article 24(1); AI Sweden (n 39)
[183] EDPB Opinion 28/2024 (n 2) para. 43
[184] AI Sweden (n 39)
[185] Ibid
[186] GDPR, Article 25(1) and Recital 78; and Veale, Binns and Edwards (n 15) p. 9; AI Sweden (n 39)

3.5 Chapter Findings and Reflections

In this chapter the focus revolved around the structural and technical features of AI which may insinuate difficulties to compliance with the RTBF. Instead of the traditional data bases that the GDPR was intentionally made for machine learning models rather absorb personal data. This data is embedded in the model's internal parameters through a statistical learning process, which makes retroactive removal of specific data far more difficult to extract.[187] The option of full retraining is resource-intensive and could risk the systems functionality. The legal requirement of erasure implies more than simple deletion, but the elimination of identifiability, which is difficult in systems built to generalize from the training data.[188] When applying the time frame under Article 12(3) GDPR to AI-systems, could the removal of the data be postponed until the next model retraining cycle?

There are technical methods designed to meet the challenges posed by AI systems. One being differential privacy, which introduces calibrated noise during training to reduce the likelihood that a single data point could be reverse engineered and identified. This approach can improve privacy during model use, but it does not offer a retrospective solution for data already embedded in the model. Then machine unlearning could be an alternative, as it seeks to selectively remove the influence of individual data points without the model requiring full retraining. It uses techniques such as the SISA framework to provide scalable strategies to fulfill erasure requests. Still, differential privacy and available machine unlearning methods face issues on verifiability and standardization.[189] There are other options that try to meet the demands for solutions, with the LEAKPRO framework being one. It attempts to provide a leakage risk profiling tool with techniques like membership inference attacks. They evaluate if personal data can be inferred from the outputs of a model, and this should align with the GDPR´s insistence for accountability and privacy by design.[190] For LEAKPRO to become a legally meaningful tool to address the RTBF it needs to meet some requirements. First, it would have to detect continues use of personal data from the AI´s outputs in a reliably way, either directly or with statistical association. This first step is important to establish processing in accordance with Article 4(2) GDPR. Second, there needs to be a supporting course of action, which can demonstrate that the influence has been erased or reduced. Third, these actions must be traceable to comply with Article 5(2) and its accountability obligation. Fourth, the tool must be employed under the procedural framework set out by the GDPR, such as the timespan of one month where the data must be erased under Articles 12(3) and 17(1). LEAKPRO does not make legal compliance itself, but it could assist as an enabler of risk-based and proportionate erasure for AI.

[187] See Zhao (n 25) pp. 85-86
[188] See Veale, Binns and Edwards (n 15) p. 9
[189] See Dwork (n 28) pp. 1-2; and Bourtoule et al. (n 4) p. 141
[190] See Vetenskaps rådet (n 170); and AI Sweden (n 39)

Emerging techniques are promising, but the GDPR provides limited guidance on if they are sufficient to meet the erasure standard. The EDPB with Opinion 28/2024 provides the concept of “insignificant risk” for re-identification but does not clarify how to measure this. The result is a compliance environment where controllers must find their way without clear approved technical standards, risking inconsistent legal enforcement. To bridge this compliance gap there needs to be a closer integration of legal interpretation and technical design to support regulatory clarity. This will be further discussed in the next chapter on privacy, innovation, and regulatory strategy.

4 Addressing Rights and Innovation

4.1 Regulatory Tensions between RTBF and AI Innovation

The right to be forgotten (RTBF) as codified in Article 17 the General Data Protection Regulation (GDPR), aims to empower data subjects to exercise control information by providing a legal right to request the erasure of personal data.[191] This right is a logical connection from the broader right to privacy in Article 8 of the Charter of Fundamental Right of the European Union.[192] The rise of Artificial intelligence development has brought with it some concerns with the RTBF, as this regulation requires implementation that might hinder innovation. AI models, especially those that are based on machine learning, are built, and trained on big amounts of data to work as intended. Once the personal data is introduced into the model, it is not only stored but more so transformed and statistically absorbed into the model's structure.[193] If a developer is forced by legislation to remove residual impact of specific data points retrospectively, both the legal and technical reality can become a challenge. In some cases, such a requirement could lead to a regulatory need to completely retraining the model, a scenario like this would mean significant uncertainty as there is no clear legal or technical standards on acceptable methods. In AI large datasets are generally used for machine learning to generate aggregated insights at a group level, and not to inspect or map out specific individuals, they still fall under the strict GDPR requirements. There is uncertainty on how to meet the purpose limitation principle, the necessity of valid legal basis for processing, and special rules covering sensitive personal data. This creates a regulatory environment which could be perceived as excessively restrictive for AI innovation.[194] The GDPR does not offer a clear or robust definition to understand "erasure" in the context of AI. It has not provided precision on how to measure level of residual data influence or what level could constitute ongoing processing.[195]

The RTBF is not an absolute right. Data subject must state their request on the grounds listed in Article 17(1). There are then certain exemptions under Article 17(3) that can allow for further data processing. The RTBF might not apply when necessary for exercising freedom of expression and information, fulfilling a legal obligation, performing a public task, or protecting public health. this specific establishment, exercise, or defense of legal claims. Further exceptions include processing for scientific and historical research

[191] GDPR, Recital 65

[192] See Charter of Fundamental Rights of the European Union [2000] OJ C363/1, Article 8

[193] Bourtoule et al. (n 4) p. 141

[194] Martin Brinnen and Daniel Westman, Vad är fortfarande fel med GDPR? (Svenskt Näringsliv, November (2022) pp.11-12

[195] Zhao (n 25) pp. 85-86; Shrishak (n 53) pp. 5-6

purposes, which requires certain safeguards in accordance with Article 89(1), such as pseudonymization.[196] The Swedish National Board of Trade puts significance on the need to find a balance between regulatory compliance and the innovation, particularly as the GDPR may have measurable impact on the EU´s economic productivity.[197]

4.2 The Cost of Compliance

The practical application of RTBF under Article 17 GDPR to AI model training introduces not only legal uncertainties, but some significant practical and financial burdens for developers as well. One option is full model retraining, in which the personal data removed, and model erased and then needs to be retrained from the initial stage. This is a comprehensive method of fulfilling data subjects right to erasure, it is both costly and often impractical, especially for large-scale AI systems built on vast amounts of data.[198] Whereas smaller models might face fewer challenges with less data to inspect, but as a model's complexity increases or the number of erasure request grows, the resource demands of full retraining risks becoming huge. This assumes the controller still has access to the original training dataset, which is not always the case.[199] Small and medium-sized enterprises risks finding themselves with a high-cost burden, with some evidence suggesting that GDPR compliance introduces fixed costs (e.g. hiring a data protection officer or updates to the technical infrastructure) that disproportionally impact emerging and smaller developers.[200] Companies of a substantial size can spread the costs over several products or services, making it more profitable, compared to smaller developers that might only have one product or service. This asymmetry could impact the reward of the work and discourage innovation, especially in projects that needs to rely on processing personal data.[201] Retraining requires time and labour cost, in addition to energy cost, with data centers being responsible for between 1.1%-1.5% of the global power consumption.[202] The international aspects of the GDPR´s influence could place a strain on cross-border data flows, if there is any uncertainty this can affect the trade and cooperation.[203]

The GDPR´s principles of accountability and risk-based regulation aims to encourage innovation through accommodating compliance. This aim turns into a burden of interpretation and technical implementation onto the controller. The regulation forces developers to be conscious about every stage of their process, anticipate uncertainties, balance the risks, and implement

[196] GDPR, Article 17(1) and 17(3), Article 89(1)

[197] Hannes Berggren, *The GDPR and International Trade: Evidence and Implications for EU Policy* (National Board of Trade Sweden March 2025) p.10

[198] Veale, Binns and Edwards (n 15) p. 9

[199] Shrishak (n 52) p. 5

[200] Rebecca Janßen, Reinhold Kesler, Michael E. Kummer and Joel Waldfoge. ´GDPR and the lost generation of innovative apps´ (2022) NBER Working Paper No. 30028. p. 45

[201] Ibid, p. 45

[202] Veale, Binns and Edwards (n 15) p. 9

[203] Berggren (n 197) pp.12-13

solutions. The complexity of understanding and achieving compliance increases, with the fear of fines under Article 83 GDPR, can increase the experienced burden.[204]

The cost of compliance with the GDPR for AI developers is not only about the legal, but it also includes technical, economic, and this being unevenly distributed across the industry. There is a need to acknowledge the importance of harmonization and providing companies with a clear regulatory framework to provide legal certainty to further compliance and innovation.[205]

4.3 Regulatory Perspectives of the GDPR in Practice

As artificial intelligence becomes more central to Europe´s digital and economic future, the role of the GDPR in guiding that future has become under increasing inspection.[206] The Regulation was designed to protect fundamental rights, in accordance with Article 8 of the EU Charter. Its application in data-intensive contexts such as AI development has raised concerns about legal uncertainty, high compliance costs and the risk of stifling innovation. With several stakeholders from different sectors calling for a more proportionate and technically adapted approach. Svenskt Näringsliv (The Confederation of Swedish Enterprise) has discussed in their rapport that the current interpretation of the GDPR creates unnecessary obstacles to machine learning and data-driven innovation.[207] Following a similar thought process is IMY (Swedish Authority for Privacy Protection), highlighting how regulatory rigidity, especially in low-risk contexts, can damage both legitimacy and effectiveness, and for that reason calls for a review of the GDPR, and guidance driven application of the law.[208]

These concerns are reflected at the European Union level. The Draghi report, released in 2024, identified GDPR as a potential constraint on Europe´s ability to lead the field on AI and digital competitiveness.[209] Furthermore, Kommerskollegium (The Swedish Chamber of Commerce) analyzed the GDPR and found that, while globally influential, the regulation risks hindering international data flows, and disproportionally burden smaller business.[210]

Following sections examines these perspectives and discussion further to frame the RTBF in an AI context and examines what they suggest for the future balance between data protection and innovation.

[204] Sartor and Lagiola (n 14) p. 78
[205] Berggren (n 197) pp. 16-17
[206] Brinnen and Westman (n 194) p. 12
[207] Ibid, p. 12
[208] IMY (n 80) pp. 7 and 11
[209] European Commission (n 20) p. 69
[210] Berggren (n 197) p. 10

4.3.1 The Business Sector: Svenskt Näringsliv

The GDPR has raised concerns from the business sector over how to interpret and enforce the legislation in practice, particularly in the context of AI systems and the use of personal data in machine learning. In 2022 Svenskt Näringsliv published a report called "What is still wrong with the GDPR", where it is argued that even if the regulation is normatively sound, it risks being applied in a manner that can stifle innovation and undermine competitiveness, particularly for companies relying on machine learning and advanced data analytics.[211]

The report raises a technical concern regarding the application of the GDPR to machine learning (ML) development, as it depends and needs vast amount of data. In ML projects personal data is mostly processed to generate insight on a group level, and not to target individuals. Examples for this could be data to use for autonomous systems or security. The report highlights that data which is handled in a correct manner should not result in any adverse effects for the individuals whose data may have been involved. This approach is sound, except the broad definition of personal data under Article 4(1) covers these data processing activities, even when individuals are not directly identifiable.[212]

Svenskt Näringsliv points out that the regulation is complex and could present a bureaucratic burden, disproportionately affecting small and medium-sized enterprises (SMEs) or companies where the risks associated with personal data only are minimal.[213] This point of view is shared by Kommerskollegiums analysis "The GDPR and International Trade: Evidence and Implications for EU Policy". Which followed with that GDPR compliance could generate high fixed costs and legal uncertainty for smaller actors, especially when engaging with developing data-intensive technologies.[214]

The report is positive to alternative technical approaches but approaches this with caution as they find no "solve-all" solution. Even data initially thought as anonymized may turn out to be classifies as personal data. In the light of the Breyer judgment, which highlighted the difficulty in excluding the risks of re-identifications that other parties might identify with their resources.[215]

The conclusion from Svenskt Näringsliv was a call for a proportionate and risk-based approach to enforcement. Suggesting data protection authorities (DPAs) to focus their efforts on high-risk processing activities and follow a

[211] Brinnen and Westman (n 194) pp. 12-13
[212] Ibid pp. 12-13
[213] Ibid, p. 20
[214] Berggren (n 197) p. 11
[215] Brinnen and Westman (n 194) p. 13

more practical and reasonable guidance approach towards low-risk use cases, such as aggregated or anonymized AI training data. The authors of the report further asked for a clarification on acceptable anonymization techniques and for a possible way to establish safe harbours or presumptive compliance mechanisms for data controllers who follow safeguards of industry-standards.[216] They underscored the need for clarified interpretative standards and a regulatory guidance that both preserves important rights and supports innovation.

4.3.2 The Public Institutional: Kommerskollegium and IMY

Innovation and international competitiveness in relation to legal certainty with GDPR has issued concerns from public institutions in Sweden. In above mentioned report by Kommerskollegium it was highlighted that the regulation, intended to safeguard fundamental rights, could risk disproportionate burdens for both public and private actors who operate within international data flows. They stressed that the challenges presented by the GDPR where especially burdensome on SMEs who operate in international digital markets, where the compliance complexity of the GDPR could risk innovation of getting through.[217] In the report it was stressed that these chilling effects on data driven markets could potentially complicate the EU´s digital competitiveness. It could be a predicament, as a lack of clear global standards and a strict EU regulatory could be risk friction in the digital trade, with increased legal uncertainty. Effectively complicating the international deployment of AI based services.[218] According to Kommerskollegium, structural problems like these do not only affect private actors, as the structural barriers provide difficulties for public actors who use data for research and international digital governance.[219]

Integritestskyddsmyndigheten (IMY, The Swedish Authority for Privacy Protection) released research on this topic with its 2024 government report on integrity and technology from 2020-2024. In the report they called for a legislative review of the GDPR, citing the perception that the Regulation is difficult to apply and that it could lead to a heavy administrative burden, even for low-risk situations. They warned that the Regulation is perceived as disproportionate or difficult to understand, could potentially risk legitimacy erosion of the Regulation over time.[220]

In line with Svenskt Näringslivs report, IMY pressed for a clarified and more practical guidance on the Regulation. Finding that uncertainty could act as a barrier for public and private innovation. They proposed a more practical

[216] Ibid, pp. 3-5
[217] Berggren (n 197) pp. 10-11
[218] Ibid, pp. 14-15
[219] IMY (n 80) p. 11
[220] Ibid, p. 10

approach, with forward thinking interpretations in dialogue with affected sectors, particularly to guidance for emerging technologies such as AI.[221]

These two public actors provide insight with a trade-oriented approach from Kommerskollegium and institutional approach from IMY. Revealing that the challenges of the GDPR covers both public and private actor alike. It challenges innovations, collaboration across borders and data-driven services in line with European digital ambitions.

4.3.3 Regulatory Strategy: The Draghi Report and EPRS

The European Union has released strategic documents on the disconnect between GDPR´s current format and the demands of the digital evolution, particularly in relation to AI. The Draghi Report (from the former European Central Bank (ECB) president Mario Draghi) with "the future of European Competitiveness" and from the European Parliamentary Research Service (EPRS) "The Impact of The General Data Protection Regulation (GDPR) on artificial intelligence". These have contributed with strong recommendations to adapt GDPR´s application to make technical innovation possible, and at the same time respect and preserve the fundamental rights in the Regulation.

The Draghi Report lifts forward the issue of fragmentation in enforcement from national Data Protection Authorities (DPAs), arguing that different approaches lead to legal uncertainty and unequal compliance assurance. A more harmonized approach is proposed to not risk hindering the EU´s digital innovation. With a more harmonized data protection law the EU could gain both the scale and thrust needed to create a competitive digital market.[222] The EPRS report focuses more on technical alignment of the Regulation. In the report they bring forward that AI systems present challenges to important GDPR principles such as purpose limitation, data minimization, and lawful processing. As a result, they find that the GDPR should be interpreted as compatible with AI, as these principles can be understood in a way that reconcile at both ends.[223] They argue for layered, and risk-based approaches compliance models meet the probabilistic and non-deterministic nature of machine learning models.[224] Such risk-based approaches include privacy-enhancing technologies such as pseudonymization and others that align with "data protection by design and by default", under Article 25 GDPR. The EPRS on top of that brings forward importance of procedures that can identify and counter risks in an AI context.[225] In particular, the EPRS report critiques the lack of direction to understand what an acceptable residual risk is. Guidance without measurable thresholds or technical standards become problematic as it creates vagueness that can lead to compliance friction. Developers, especially in

[221] Ibid, p. 10
[222] European Commission (n 20) pp. 30 and 69
[223] Sartor and Lagiola (n 14) pp. 76-77
[224] Ibid, p. 77
[225] Ibid, pp. 75-76

smaller companies, need to know how the GDPR applies and should be used.[226]

Both of these sources seem to agree that innovation and privacy need legal clarity and regulatory foresight to work with each other. They focus their attention on proportionality, interpretability, and scalability to not stifle innovation.

4.4 Chapter Findings and Reflections

This chapter examined Article 17 GDPR interpretation in relation to sustainable innovation in the development of AI. Data-intensive technologies are becoming increasingly central to the EU digital strategy, but the strict data protections in the GDPR raises concerns whether the legal framework is fit for purpose in the AI context.[227] The RTBF was founded as a to give individuals control over their digital footprint but did not foresee the future application, to machine learning systems. This has created a difficult balancing situation where personal data may be embedded in AI systems, where it continues to influence outputs as long as it has at one time affected the model. The structural features of AI system, which depend on large data sets and probabilistic outputs, could complicate compliance and model functionality.[228] This problem is particularly burdensome for smaller developers that lack the resources to retrain models or implement a harsh privacy-preserving infrastructure. The compliance burdens seem to be unevenly distributed, as legal uncertainty and high compliance costs may discourage innovation, especially in lower-risk context.[229]

Article 17 establishes a right to erasure, but this right is not absolute as there are provisions providing exemptions for processions, such as public interest, scientific research, or on the bases of legitimate interest. These exemptions require an assessment based on contextual proportionality, where the data controller need to weigh the interests of innovation and societal benefit against the data subject´s right to informational self-determinations. This balancing test could prove complicated as the unpredictability and lack of clarity in machine learning systems.[230]

The stakeholder commentary, from Svenskt Näringsliv, Kommerskollegium and IMY, revels a discussion about how the GDPR supports innovation accordingly. Together their commentary seems to land on the need for a more flexible interpretation of the regulation, with clear guidance on techniques, and a risk-based compliance mechanism that allow for scalable application.[231]

[226] Ibid, pp. 77-78
[227] See Sartor and Lagiola (n 14) pp. 76-77
[228] See Bourtoule et al. (n 4) p. 141; Zhao (n 25) pp. 85-86; Shrishak (n 52) pp. 5-6
[229] See Berggren (n 197) pp. 16-17; Brinnen and Westman (n 194) p. 12
[230] See Zhao (n 25) pp. 85-86; Shrishak (n 52) pp. 5-6
[231] See Berggren (n 197) pp. 16-17; Brinnen and Westman (n 194) p. 12

From the EU level, with the Draghi Report and the EPRS, it is argued that there is a need for a the GDPR´s principles to be interpreted with proportionality, scalability, and technological neutrality. The EPRS then proposes that privacy-enhancing technologies that incorporate the correct privacy-by-design measures could assist with lawful innovation if integrated into the early phases of development.[232]

To conclude this chapter, the RTBF is still important to comply with the fundamental rights in a digital environment, but it needs a more nuanced and adaptable regulatory approach. The findings from the chapter proposes that innovation and the RTBF can coexist if operationalized through proportionate, risk-based frameworks that work together with technical safeguards, such as pseudonymization, machine unlearning, and structured data governance. The next chapter further addresses the compliance gap and how there is a need for both doctrinal development and systemic alignment to allow sustainable AI development.

[232] See European Commission (n 20) pp. 30 and 69; Sartor and Lagiola (n 14) pp. 76-77

5 The RTBF Compliance Gap

5.1 Balancing fundamental rights

The Right to Be Forgotten (RTBF) needs to be interpreted and understood in accordance with the broader framework of fundamental rights set out in the Charter of Fundamental Rights of the European Union (the Charter).[233] The Charter provides the right to protection of personal data under Article 8, which includes fair data processes, based on consent for specific purposes or another legitimate legal ground, and provides for the right to both access and have the data rectified. At the same time the Charter protects freedom of expression and information under Article 11, in which everyone should be able to receive and impart information, which grants individuals the right to receive and impart information.[234] These rights are not absolute, and can at times be in conflict of one another, which means that a controller need to carefully exercise a balance based on the principle of proportionality when handling these rights.[235] As established in Google Spain(C-131/12) the balancing exercise proved central to the Court of Justice of the European Union (CJEU).[236] Where they clarified this obligation must be proportional to the public´s interest in accessing the information.[237] In the same manner the CJEU in the GC and Others(C-136/17) contributed with that the RTBF must be assessed on a case-by-case basis, where specific context and proportionality of each request must be considered[238]. Applying this to AI makes the balancing more difficult, as the AI model's outputs are probabilistic and context dependent. The information is not directly attributable to specific individuals at all times, and not accessible in the same way as a search engine. Understanding the privacy harm and corresponding personal interest becomes more complex by this.[239]

The definition on the proportionality principle is found in EU law and requires that fundamental rights in conflict should follow necessity, be suitable and proportionate in the strict sense.[240] In the case of Google (C-460/20), the CJEU clarified that the RTBF claims should be assessed against both privacy rights and freedom of information. Where slighter inaccuracies in the could swing the pendulum towards the rights to private life and protection of data,

[233] Charter of Fundamental Rights of the European Union [2000] OJ C363/1, Preamble and Article 8

[234] Ibid, Article 8, Article 11

[235] Case C-131/12, *Google Spain v AEPD* , paras. 74-85; Case C-136/17, *GC and Other v. CNIL*, paras. 66-74

[236] Case C-131/12, *Google Spain v AEPD*, para. 93

[237] Ibid, paras. 81-85

[238] Case C-136/17, *GC and Other v. CNIL*, paras. 66-74

[239] EDPB Opinion 28/2024 (n 2) paras. 29-34; Li (n 17) p. 485

[240] Charter of Fundamental Rights of the European Union [2000] OJ C363/1. Article 52

and obligation to delete the personal data. Seeing that data which is wrong or inaccurate should not fall under the right to information, as it does not cover the right to disseminate such information.[241] Applying this principle to the RTBF in for AI model needs correct measures, assessing actual privacy gains for data subject, model functionality and achievability. Technical alternatives, such as machine unlearning or differential privacy could possibly aid as protective measures to support the steps to compliance.[242]

The application of the RTBF in AI systems is not only a technical challenge, but equally a test for legal data protection. For the RTBF to be effective and lawful it needs to be interpreted with the Charter, to assure compliance with Article 8 and Article 11 in a meaningful way.[243] The CJEU has consistently brought forward case law clearly based on the proportionality principle, requiring a balance assessment on case-by-case.[244] Implementing the RTBF in an AI context needs to balance technical reality and follow the constitutional framework of the European Union.

5.2 Static Right in a Dynamic Setting

The relationship between static legal rights and AI systems of a dynamic character creates a rigid and sometimes incompatible regulatory space. Even so, there is potential for the AI system´s architecture to act as a regulatory modality. Professor Lawrence Lessing had a famous quote on this, "code is law", meaning that regulation is not the exclusive domain of law. By the system´s inherent ability to either facilitate or constrain behavior, through code, protocols, and design, in ways that could be comparable to legal norms.[245] Lessing identifies four forces that over time shape behavior. First law, then social norms, followed by market incentives and the last one being the architecture consisting of code, protocols and the technical design.[246] In the context of AI governance, the architecture becomes relevant as traditional tools fall short attempting to work with the inner parts of machine learning systems.

Some data controllers are opting for system-level configurations that can hinder access to personal data, through geographic and role-based restrictions. A

[241] Case C-460/20 *TU and RE v. Google LLC*, para. 65; See Christakis (n 77) pp. 3-4, which highlights hallucinations, which should be inaccurate data as presented in the Case C-460/20

[242] Bjorn A. Juliussen, Jon P. Rui and Dag Johansen, "Algorithms That Forget: Machine Unlearning and the Right to Erasure" (2023) 51 *Computer Law & Security Review*, p. 7

[243] Charter of Fundamental Rights of the European Union [2000] OJ C363/1. Articles 8 and 11

[244] Case C-131/12, *Google Spain v AEPD*, paras. 74-85; Case C-136/17, *GC and Other v. CNIL* paras. 66-74

[245] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (2013) p. 96

[246] Elettra Bietti, ´Assessing principles for the regulation of online content: Lessig´s modalities of regulation´, (Law and Media Working Paper Series, No. 1/2017) p. 2

company with connections to multiple nations could routinely design IT systems to geofence access, meaning that personal data from one jurisdiction cannot be accessed from another.[247] This is an example of preemptive compliance measures, reflecting both data minimization, the principle of purpose limitation, and data protection by design.[248] Introducing technical and organizational measures are in line with Article 25(1) GDPR, which implies that the controller needs to be aware of what and how to apply measures that establish protection of data.[249]

The central issue lies in the discrepancy between the legal assumptions of GDPR and the actual structure of machine learning systems.[250] Machine learning models spread their data across parameters, encoding data in patterns rather than storing individual records in accessible formats.[251] This can create a structural problem, where data continues to influence outputs even after formal removal.[252] This phenomenon is captured in the concept of the algorithmic shadow, where the personal data´s influence has been technically deleted but remains statistically present in the behavior and output.[253] There appears to be a philosophical and legal mismatch as Article 17 GDPR is predicated on a static law and traditional logic on deletion and withdrawal of consent. AI systems are instead probabilistic and non-deterministic, generalizing patterns more than collecting and individually storing data, but may still be able to give out characteristics of personal data in their outputs.[254]

5.3 AI Act and Regulatory Synergies

To understand the RTBF on AI models further, it is important to consider the broader regulatory context. The European Union has taken a significant step by implementing a comprehensive regulatory framework on artificial intelligence with the Artificial Intelligence Act (Regulation (EU) 2024/1689). Its objective is to promote human-centric, trustworthy innovation at the same time as making sure fundamental rights are protected, particularly under the Charter.[255] The European data protection framework is built around a technology neutral language and should apply in an AI context[256]. Even so, there are tensions for AI systems regarding traditional data protection principles and the data-intensive nature for AI. There are some interpretations that can be beneficial for AI uses, one is the purpose limitation principle, that can

[247] Kuner (n 254) pp. 96-97
[248] FRA and Council of Europe, Handbook (n 13) p. 356
[249] EDPB, Guidelines 4/2019 on Article 25, §§7-10
[250] Zhao (n 25) p. 85
[251] Li (n 17), p. 490
[252] Ibid, pp. 490-491
[253] Ibid, p. 494
[254] Christakis (n 77) p. 4
[255] AI Act (n 3) Recital 1-2
[256] EDPB Opinion 4/2020 (n 83) para. 16

accommodate secondary uses for statistical purposes, if not presenting an unacceptable risk to the data subjects.[257] In a similar way, the data minimization principle does not in all cases strictly imply a reduction in data quantity, instead it aims to reduce the identifiability, often through techniques like pseudonymization. The architecture of the GDPR makes it possible to apply proportional safeguards into the AI system, such as privacy by design and by default principle.[258]

The AI Act addresses AI specific risks by introducing a classifying system, based on risk levels, which places stricter obligations on the high-risk systems.[259] Under Article 16 of the Treaty on the Functioning of the European Union (TFEU), such systems need to respect the right to data protection, especially when it is about biometric or sensitive personal data. The AI Act require several transparency measures, including documentation, logging, and human oversight.[260] The provisions in the AI Act align accordingly to the GDPR's Recital 60, making it clear that data subjects must be informed of the processing practices affecting their personal data.[261] AI developers, such as OpenAI and Google, have introduced several support mechanisms like disclaimers, correction forms, and transparency portals to comply with obligations related to data subject´s rights. These measures are supportive, but they do not guarantee full compliance with RTBF. For example, OpenAI acknowledges that due to the complexity of AI models, full correction or deletion is not always attainable, and instead offers partial remedies such as removal of personal data from future outputs.[262]

The AI Act does not impose a direct requirement for machine unlearning, but it does put significant weight on data governance and lifecycle documentation, both of which supports implementation erasure mechanisms.[263] Article 9 of the AI Act reinforces this by requiring high-risk systems to implement ongoing risk management procedures to assess and mitigate privacy risks over time.[264] Another important provision from the AI Act is the requirement to include clear instructions for data subjects regarding foreseeable misuses and their impact on fundamental rights. This could possibly serve as a foundation for integrating RTBF-aware design strategies starting at the training phase.[265]

[257] Sartor and Lagiola (n 14) p. II
[258] Ibid, p. II
[259] AI Act (n 3) Recitals 46-48
[260] Ibid, Articles. 13-15
[261] GDPR, Recital 60
[262] Christakis (n 77) pp. 9-10
[263] AI Act (n 3) Articles. 9, 17, 18
[264] See Ibid, Recital 65
[265] AI Act (n 3), Article. 13

Even with these synergies, the AI Act does not specify what actually constitutes an acceptable amount of residual personal data post-training. The EDPB Opinion 28/2024 refers to the concept of "insignificant" likelihood of re-identification but does not provide any measurable means.[266] The AI Act governance framework includes national market surveillance authorities and a European AI board. It is valuable to understand that the AI Act is an important step it is complementary to the GDPR and is not a replacement. The EDPB has proposed enhanced cooperation between national DPA´s and AI supervisory authorities, that together can work to assess re-identification risks and track erasure obligations.[267]

5.4 Bridging Law and Practice

The RTBF presents a unique challenge in the age of AI models, since attaining legal erasure through retraining or technical unlearning is often technically complex and resource intensive.[268] This contributes to a regulatory ambiguity, but there is a chance for proxy mechanisms, like auditing, certification, and traceability, to demonstrate GDPR compliance without compromising on innovation.

Model audits creates a compliance route that is concrete and possible to follow, exemplified by initiatives such as the LEAKPRO project. In the LEAKPRO project there are systematical tests on the AI models to locate data leakage, by testing vulnerability to membership inference and data reconstruction attacks.[269] Attacks like these can give important indication on the status of personal data. Discovering if the data resides, even residually, and if so then there is a breach of Article 17 GDPR.[270] Audit-based can offer technical security and additionally propose auditable standards of risk awareness. Periodic leakage audits might serve as substitute evidence to demonstrate that re-identification risks are on an "insignificant" level, as referred to in EDPB Opinion 28/2024.[271] It is important to understand that as long as a model is susceptible to meaningful inference attacks, the audit function acts as mitigating control and not as proof of data erasure. Even so, it could be a layer of risk-based accountability, aligned with Article 5(2) GDPR.[272]

A third-party certification could as aid as a compliance mechanism. There are two relevant standards that attempt to cover this, to a certain degree. Firstly ISO/IEC 42001:2023, which contains guidelines on establishing,

[266] EDPB Opinion 28/2024 (n 2) para. 43
[267] Ibid, para. 76
[268] Zhao (n 25) p. 85
[269] AI Sweden (n 39)
[270] Solove (n 11) p. 5; Shokri et al., (n 76) p. 3
[271] EDPB Opinion 28/2024 (n 2) para. 43
[272] Ibid, para. 58

implementing, maintaining, and continual AI management improvement systems within organizations. It covers lifecycle controls, governance mechanism and role accountability[273], which aligns with the privacy by design principle under Article 25 GDPR.[274] ISO/IEC 23894 focuses on the framework and methodologies for identification, assessment, and mitigation risks for AI systems, and acts as a complementary risk management standard, specific for AI systems, where it provides tools for technical and socio-ethical risk evaluation through the AI lifecycle.[275] These standards do not cover RTBF explicitly, but they do offer options for risk mitigation tools. Applying these to standards together could potentially provide AI developers and actors options to systemize their compliance strategies, by offering verifiable risk mitigation and demonstrable due diligence. These are still voluntary frameworks, and as a consequence not legally binding, but they could potentially be persuasive.

5.5 Chapter Findings and Reflections

This chapter revealed the disconnect between the legal framework of the GDPR, particularly Article 17, and the practical reality of implementing the RTBF in modern AI systems. The GDPR provides clear obligations for data controllers to respond erasure request, even so the architecture of machine learning models creates difficulties for compliance. The RTBF can be hard to apply as it's rooted in static legal concepts, as AI works as a dynamic technical system. AI models work in an output driven environment where personal data is influential, but no longer directly accessible.[276] The EDPB in its Opinion 28/2024, proposed "insignificant" risk of re-identification as the threshold where AI model outputs would fall outside the scope of the GDPR. Nevertheless, they did not provide measurable standards for what would qualify as insignificant, which may undermine predictability and contribute to fragmented enforcement.[277]

There are developers and institutions exploring alternative strategies to bridge the gap and bring clarity. One approach is to embed the regulatory principles into the design of AI systems, from "law-on-paper" to "law-by-architecture". This draws from Lessig´s concept that code is law, which means design features that can initiate data minimization and privacy by design at the system level.[278] These do not directly fulfill the requirements under Article 17 GDPR

[273] ISO, ISO/IEC42001:2023, Artificial Intelligence, Management System, Geneva: International Organization for Standardization, (ISO 2023). See in particular Clauses 5.2 and 5.3 on governance and accountability, Clause 8 on lifecycle operational controls

[274] See GDPR Article 25

[275] ISO, ISO/IEC23894:2023, Information Technology, Artificial Intelligence, Guidance on risk management, Geneva: International Organization for Standardization, (ISO 2023). See in particular Clause 5 and Annex A

[276] See Zhao (n 25) p. 85; Li (n 17), p. 490

[277] See EPBD 28/2024 para. 43

[278] See Kuner (n 254) p. 96

they could represent a design feature of risk mitigation. The chapter further proposed a layered compliance framework where audit and certification could assist in operationalizing the RTBF. Incorporating tools like LEAKPRO could help to assess when personal data remains inferable in AI outputs, and certifications from ISO standards could assist with externally verifiable evidence of compliance.[279]

The synergy between the GDPR and the AI Act was explored, as the AI Act offers structural tools such as risk classification, lifecycle governance and documentation requirements. The Act does not explicitly codify the RTBF, but it provides a foundation of transparency, human oversight, and post-deployment monitoring.[280] These can help bridge the legal norms and AI-specific technical practices. The chapter finds that there is a need to understand the RTBF in a dynamic setting, where legal reasoning, technical design and innovation assist each other.

[279] See Chapter 5.4
[280] See AI Act

6 Analysis

This chapter analyses the findings from the previous chapters together, to examine the central research questions together with their sub-questions. This will systematically assess Article 17 GDPR´s legal obligations to AI systems and their technological structure and explore the balance between privacy and innovation.

In Chapter 2.1 it is established that Article 17(1) GDPR provides individuals with the possibility to request erasure of their personal data, which is derived from the Charter of Fundamental Rights of the European Union.[281] The RTBF, as codified in Article 17(1), provides six grounds for erasure under which the controller must fulfill the request. The concept of controller is to pe interpreted broadly, as even one in control over the dissemination and access of the data is covered by Article 4(7) GDPR.[282] This creates the foundation of erasure, which AI systems challenge with their data structure. A machine learning system rather integrates the data into the model's core, or parameters, which both complicates what constitutes processing and how to reach erasure. The sub-question for chapter two concerns the scope and applicability of Article 17 in relation to AI models, where it is important to understand personal data and its role. Article 4(1) GDPR is the foundation of the definition, and chapter 2.1.3 and 5.1 highlights the Breyer Case(C-582/14) as it expands the scope personal data to indirect identifiability.[283] It is further reinforced by the Nowak case, where even traces of knowledge and abilities can result in identification of an individual.[284] This approach is followed by the EDPB in their Opinion 28/2024, where AI outputs are expressly covered if they can be subject to re-identification of personal data.[285] Read together these sources support a view, in which the residual data's influence in an AI model could constitute personal data. In the event of an erasure request a data controller obligation might have to extend to locate even embedded traces of residual data. To address this chapter 3.2 and 3.3 focuses on the technical aspect of fulfilling erasure, and they underline the effects of full retraining for smaller organizations due to both labour and cost intensive. Some techniques are proposed to aid as mitigating tools[286], such as differential privacy and machine unlearning in the framework of SISA[287], though they are not complete effective legal substitutes for all situations but could be applied where necessary or appropriate. Chapter 3.4 examines data leakage risks and focuses on

[281] Charter of Fundamental Rights of the European Union [2000] OJ C363/1, Articles 7 and 8; See Chapter 2.1

[282] See Google Spain (C-131/12); Case C-460/20 *TU and RE v. Google LLC;* Directive 95/46/EC, on controller; now codified as 4(7) GDPR

[283] See Case C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland; GDPR, Article 4(1)*

[284] See Case C-434/16, *Peter Nowak v. Data Protection Commissioner*

[285] See EDPB Opinion 28/2024 (n 2) paras. 43, 58

[286] See EDPB Opinion 28/2024 (n 2) para. 52

[287] See Dwork (n 28) pp. 1-2; Bourtoule et al. (n 4) p. 141

the LEAKPRO framework, which can help assess residual identifiability. This could potentially align with the accountability principle in Article 5(2) GDPR, as it provides an opportunity to locate data and maybe the possibility to verify that the residual influence data no longer is there.[288] In the same line as differential privacy and SISA, the LEAKPRO frameworks future potential is hard to assess as determining its effective application to the fulfilment of erasure obligations remains.

The legal burden of Article 17 GDPR is examined in Chapter 2.2 and reinforced in Chapter 5.2, with much of the analysis based on the proportionality principle. The threshold of "insignificant" risk of re-identification is introduced in the EDPB´s Opinion 28/2024, which could imply that safeguarding measures that can turn the data into unidentifiable information reduces the obligation of full retraining. Chapter 5.5 highlights concern on the absence of measurable metrics for insignificant, which leaves the interpretation of other viable alternatives uncertain. Chapter 4 had a sub-question on the impact and interpretation of GDPR to innovation. There were reports from Svenskt Näringsliv (2022), Kommerskollegium (2025), and the Draghi Report (2024) to get a status on the subject of innovation and the GDPR. These reports mentioned in different ways that the GDPR present high compliance costs, which risks chilling the digital market. These concerns bring up the difficulties of providing free movement of data and information, which should align with the aims of the GDPR under Recital 4 and 6.[289] There seems to be a regulatory environment which lacks clear guidance, although there are intentions to balance the right, the reality is more challenging. Chapter 4.3 investigates more flexible compliance mechanisms to meet the lack of clear guidance, with certification frameworks and model audits to support data minimization and lifecycle documentation.[290] This practical gap between legal obligation of erasure and AI systems is covered by the last sub-question, where it is concluded that the theoretical and practical do not quite agree. The GDPR does not provide clear guidance on the RTBF, and the introduction of the AI Act brought few guidelines on unlearning and leakage testing. The Act does provide some helpful tools such as risk classification of AI systems and the introduction of human oversight. Still, the need for guidance and an understanding of technical concepts seems important to meet.

[288] See AI Sweden (n 39); Brännvall (n 39)

[289] See GDPR, Recital 4, which states "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality" and Recital 6, which states "…technology has transformed both economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third counties and international organisations…"

[290] See Chapter 5.4

7 Conclusion

This thesis examined the right to be forgotten (RTBF) in relation to the emerging AI sector, with specific interest in the data intensive nature of machine learning models. It follows the origins of the right and explores how it translates to AI models in a modern sense. This reveals a path through an evolving technical field, with legal uncertainty, complexity, and normative tensions.

As demonstrated in this study, AI systems absorb personal data through probabilistic learning processes, in which the data becomes embedded in the architecture of the models. Removing personal data seems to mean all traces that could potentially reveal an individual, which is difficult in an AI system trained on huge amounts of data. The thesis consequently finds that there is a structural compliance gap between the technical reality of machine learning and the standard of erasure under the GDPR. To address this the study explores emerging approaches to the issue, such as machine unlearning, differential privacy, and leakage risk profiling through frameworks like LEAKPRO. These techniques could potentially contribute with supporting technical measure for erasure, and evidentiary material through assessments. It remains uncharted territory, and new techniques would require verifiability, proportionality, and legal validity to assist in compliance matters.

To address the current field of innovation and AI the thesis incorporates stakeholders from both business and public governance to assess their view of the application of GDPR. They are worried that fragmented application, uncertain guidelines, strict data protection rules and high costs might leave the EU behind in the digital market. Clear guidelines and a review of the GDPR seems important to meet the needs for technological advancement. For AI especially the vagueness of terms in the GDPR provides uncertainty. The goal with these is to provide a technology neutral framework, but the practical application could prove difficult as the interpretive and operational broadness of the Regulation has not yet been clarified through standards, jurisprudential or legal cases. One case which highlights an attempt for standard is the introduction of "insignificant" from the EDPB in Opinion 28/2024, but in spite of that its application and measurable metrics are vague and could lack enforceability.

This thesis does not provide clear answers to the questions asked, but it does explore the layered and conditional understanding of the RTBF in relation to AI systems. Erasure in a machine learning model is not performed with a single action, it requires a new approach to fully grasp the continuous and technical function throughout the AI lifecycle. The subject seems to require more of an interdisciplinary process, where legal experts, engineers, regulators, and industry actors combine their knowledge. Innovation needs to meet

fundamental rights not only in the theoretical but in the practical to see change. To conclude this thesis, the current legal framework on the RTBF would require a review to align its principles with the dynamic structure of AI systems, with a realistic approach. Guidelines from the EDPB can offer some advice to the Regulation, but there needs to be guidance with firm legal ground. Some suggestions might be to distinctly provide measurable erasure standards, with recommended techniques. The EU data protection laws need to harmonize the digital field to counteract fragmentation and to serve the best practices for mankind.

Bibliography

LEGAL INSTRUMENTS

Charter of Fundamental Rights of the European Union [2000]. OJ C364/1

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 L 281/31

Regulation (EU) 2016/679 of the European Parliament and of 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 (General Data Protection Regulation, GDPR) [2016]. OJ L 119/1

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 March 2024 laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts. OJ, L1689/1, 2024

CASE LAW

Court of Justice of the European Union /Grand Chamber), Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. ECLI:EU:C2014:317, judgment of 13 May 2014.

Court of Justice of the European Union, Case C-708/18, TK v Asociatia de Proprietari bloc M5A-ScaraA. ECLI:EU:C:2019:1064, judgment of 11 December 2019

Court of Justice of the European Union, Case C-583/14, Breyer v. Bundesrepublik Deutchland. ECLI:EU:C:2016:779, judgment of 19 October 2016

Court of Justice of the European Union, Case C-434/16, Peter Nowak v. Data Protection Commissioner. ECLI:EU:C:2017:994, judgment of 20 December 2017

Court of Justice of the European Union, Case C-136/17, GC and Others v. CNIL. ECLI:EU:C:2019:773, judgment of 24 September 2019

Court of Justice of the European Union, TU and RE v. Google LLC, C-460/20. ECLI:EU:C:2022:962, judgment on 8 December 2022

Court of Justice of the European Union, Case C-319/22 Gesamverband Autoteile-Handel v. Scania. EU:C:2023:837, judgment of 9 November 2023*

OFFICIAL PUBLICATIONS

Article 29 Working Party, Opinion 4/2007 *on the concept of personal data*, adoped (WP 136, 20 June 2007). Brussels.

De Luca, S., and Federico, M. (2025). *Algorithmic Discrimination under the AI Act and the GDPR*. European Parliamentary Research Service (EPRS), PE 769.509. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)769509 [accessed 5 April 2025]

European Data Protection Board (2024). *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, Adopted 17 December 2024. Brussels: EDPB

European Data Protection Supervisor (2020). *Opinion 4(2020 on the European Commission´s White Paper on Artificial Intelligence – A European approach to excellence and trust.* Adopted 29 June 2020

European Union Agency for Fundamental Rights and Council of Europe (2018) *Handbook on European data protection law*, 2 nd edn. Luxembourg: Publications Office of the European Union. Available at: https://data.europa.eu/doi/10.2811/58814. [accessed 11 February 2025]

European Commission (2024). *The Future of European Competitiveness: A Competitiveness Strategy for Europe – Part A*. Brussels: European Commission. Available at: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf [accessed 23 February 2025]

Integritetsskyddsmyndigheten (IMY), *Integritet och ny Teknik: Integritetsrisker kopplade till stora språkmodeller 2020-2024.* Diarienummer IMY-2024-*2570.* Stockholm: IMY. Available at: https://www.imy.se/globalassets/dokument/rapporter/imy_rapport_integritet-och-ny-teknik.pdf [accessed 11 April 2025]

International Organization for Standardization (ISO), ISO/IEC42001:2023 — Artificial Intelligence — Management System, Geneva: ISO

ISO, ISO/IEC23894:2023 — Information Technology — Artificial Intelligence — Guidance on risk management, Geneva: International Organization for Standardization, 2023. See in particular Clause 5 and Annex A

Berggren, H. *The GDPR and International Trade: Evidence and Implications for EU Policy*. Stockholm: National Board of Trade Sweden 2025. Available

at: https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2025/gdpr-and-international-trade.pdf [accessed 8 April 2025]

Sartor, G., and Lagiola, F., (2020), *The impact of the Genereal Data Protection Regulation (GDPR) on artificial intelligence*. European Parliamentary Research Service(EPRS), Scientific Foresight Unit (STOA). PE 641.530, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf [accessed 15 March 2025]

REPORTS AND WORKING PAPERS

Bietti, E. (2017). "Assessing principles for the regulation of online content: Lessig´s Modalities of Regulation", *Law and Media Working Paper Series*, No. 1/2017, Available at: https://www.medialaws.eu/wp-content/uploads/2017/01/1.2017-Bietti.pdf [accessed 15 February 2025]

Brinnen, M. and Westman, D. (2022). *Vad är fortfarande fel med GDPR?* Stockholm: Svenskt Näringsliv. Available at: https://www.svensktnaringsliv.se/bilder_och_dokument/rapporter/xq29h7_vad-ar-fortfarande-fel-med-gdprpdf_1193101.html/Vad+%25C3%25A4r+fortfarande+fel+med+GDPR%253F.pdf [accessed 10 April 2025]

Brännvall, R., Adomaitis, L., Görnerup, O., and Sedrati, A. (2024). *Technical Report for the Forgotten-by-Design Project: Targeted Obfuscation for Machine Learning.* Stockholm: RISE Research Institutes of Sweden, Available at: https://arxiv.org/pdf/2501.11525 [Accessed 12 April 2025]

Christakis, T. (2024). "*AI Hallucinations and Data Subject Rights under the GDPR: Regulatory Perspectives and Industry Response´s"*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5042191 [accessed 24 April 2025]

Janßen, R., Kesler, R., Kummer, M. E., and Waldfogel, J., (2022). "GDPR and the lost generation of innovative apps". NBER Working Paper No. 30028. Available at: https://www.nber.org/papers/w30028, [accessed 23 March 2025]

Shrishak, K. (2024). *Effective Implementation of Data Subjects´ Rights*. Support Pool of Experts Programme. European Data Protection Board (EDPB). Available at: https://www.edpb.europa.eu/system/files/2025-01/d2-ai-effective-implementation-of-data-subjects-rights_en.pdf [accessed 26 April 2025]

Vetenskapsrådet (2005). Tvärvetenskapen – en analys. Stockholm: Swedish Research Council (10). Available at:

https://www.vr.se/download/18.2412c5311624176023d25be6/1529480529282/Tvaervetenskap-en-analys_VR_2005.pdf [accessed 14 February 2025]

ACADEMIC LITERATURE

Dwork, C. (2006). "Differential privacy". In M. Bugulesi, B. Preneel, V. Sassone, & I. Wegener, Eds., *Automata, languages, and programming: 33rd international colloquium*, *ICALP 2006, Venice, Italy, July 10-14, 2006. Proceedings, part II.* Lecture Notes in Computer Science, Vol. 4052. Berlin: Springer, Available at: https://link.springer.com/chapter/10.1007/11787006_1 [accessed 23 April 2025]

Goodfellow, I., Bengio, Y., and Courville, A. (2016). *Deep Learning*. Cambridge, MA: MIT Press 2016

Janssen, H., Cobbe, J., Norval, C. and Singh, J. (2020). "Decentralised Data Prcessing: Personal Data Stores and the GDPR". Available at: https://doi.org/10/1016/j.clsr.2019.105384 [accessed 25 April 2025]

Juliussen, B. A., Rui, J. P., and Johansen, D. (2023). "Algorithms that forget: Machine unlearning and the right to erasure". *Computer Law & Security Review*, 51. Available at: https://doi.org/10.1016/j.clsr.2023.105885 [accessed 23 April 2025]

Kemper, C. (2020). "Kafkaesque AI? Legal Decision-Making in the Era of Machine Learning", *Intellectual Property & Technology Law Journal*, 24(2), pp. 251- 275. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3744199 [accessed 18 April 2025]

Kranenborg, H. (2021). Article 17: Right to erasure, In C. Kuner, L.A Bygrave and C. Docksey, eds., *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford: Oxford University Press, pp. 85-96

Kulk, S., and Zuiderveen Borgesius, F. Z. (2014). ′Google Spain v. Gonzales; Did the court Forget about Freedom of Expression?′ 5(3) *European Journal of Risk Regulation*, pp. 389-398. Available at: https://www.jstor.org/stable/pdf/24323469.pdf?refreqid=fastly-default%3A888217b0292c78b53efd2237da7375ff&ab_segments=&initiator=&acceptTC=1 [accessed 17 April 2025]

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press; online edn, Oxford Academic, 26 Sept. 2013, Available at: https://doi-org.ludwig.lub.lu.se/10.1093/acprof:oso/9780199674619.001.0001 [accessed 15 April 2025]

Li, T.C., (2022). 75 “Algorithmic Destruction”. SMU Law Review 479 , pp. 479-502 available at: https://scholar.smu.edu/smulr/vol75/iss3/2 [accessed 23 April 2025]

Magnusson Sjöberg, C., (2012). Legal AI from a Privacy Point of View: Data Protection and Transparency in Focus. In: S. Petersson,, ed., Digital Human Sciences. Stockholm : Stockholm Univsersity Press

Peczenik, A. (1995). *Vad är rätt? Om demokrati, rättsäkerhet, etik och juridisk argumentation*. Norstedts Juridik. Republished digitally by the Faculty of Law, Lund University(2021 [eBook] Available at: https://doi.org/10.37852/oblu.106 [accessed 23 April 2025]

Rustad, M.L., and Kulevska, S. (2015). “Reconceptualizing the right to be forgotten to enable transatlantic data flow”. 28(2) *Harvard Journal of Law & Technology*, pp. 349-416. Available at: https://ssrn.com/abstract=2627383 [accessed 2 April 2025]

Schwartz, P.M., and Solove, D.J. (2011). “The PII Problem: Privacy and a New Concept of personally identifiable Information”. New York University Law Review, 86(6), pp. 1814-1894. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366 [accessed 2 March 2025]

Smuha, N. A. (2020), “Beyond Data: Artificial Intelligence, Data Protection and the GDP”`, In: M. Dubber, F. Pasquale and S. Das, eds. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge: Cambridge University Press, pp. 317-332

Solove, D.J. (2025). “Artificial Intelligence and Privacy”, Florida Law Review, 77, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4716545 [accessed 14 April 2025]

Tosoni, L. and Bygrave, L.A. (2021). “Article 4(2): Processing”, in C Kuner., L. A. Bygrave, an C Docksey, (eds), *The EU General Data Protection Regulation (GDPR): A Commentary – 2021 Update,* Oxford: Oxford University Press. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839645 [accessed 13 April 2025]

Veale, M., Binns, R. and Edwards, L. (2018). “Algorithms That Remember: Model Inversion Attacks on Data Protection Law”. (2018) 376(2133) Philosophical Transactions of the Royal Society A, Article 20180083. Available at: https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0083 [accessed 12 April 2025]

Zhao, Z. "The Application of the Right to be Forgotten in the Machine Learning Context: From the Perspective of European Laws" (2022) 31(1) *Catholic University Journal of Law and Technology*, 73, pp. 73-98. Available at: < https://scholarship.law.edu/jlt/vol31/iss1/5 > [accessed 14 February 2025]

ELECTRONIC SOURCES AND ONLINE SOURCES

AI Sweden, (2024). "LEAKPRO - Leakage Profiling and Risk Oversight for Machine Learning Models". Stockholm: AI Sweden. Available at: https://www.ai.se/en/project/leakpro-leakage-profiling-and-risk-oversight-machine-learning-models#:~:text=The%20primary%20objective%20is%20to,collaborative%20training%2C%20and%20synthethich%20data [accessed 17 mars 2025]

Bourtoule, L., Chandrasekaran, V., Choquette-Choo, C. A., Jia, H., Travers, A., Zhang, B., Lie, D., and Papernot, N., 2021. "Machine Unlearning. In: Proceedings of the 2021 IEEE Symposium on Security and Privacy". (SP), 23-27 May 2021. *IEEE Symposium on Security and Privacy*, pp. 141– 159.Available at: https://doi.org/10.1109/SP40001.2021.00019 [accessed 17 mars 2025]

Zerdick T, "Pseudonymous data: processing personal data while mitigating risks" [blog]. (European Data Protection Supervisor (EDPS) 21 December 2021) Available at: https://www.edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en [accessed 3 May 2025]

Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI), 2024. *Discussion Paper on Large Language Models and Personal Data* [online] (15 July 2024). Available at: https://datenschutx-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Inforamtionen/247015_Discussion_Paper_Hamburg_DPA_KI_Models.pdf [accessed 20 May 2025]

Kasture, N., "Machine Learning: Why It Is an Iterative Process", Medium – Analytics Vidhya. Available at: https://medium.com/analytics-vidhya/machine-learning-why-it-is-an-iterative-process-bf709e3b69f2 [accessed 21 Mars 2025]

Kuneva M, "Roundtable on Online Data Collection, Targeting and Profiling Keynote Speech". Keynote Speech, Brussels, 31 March 2009. European Commission. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_09_156/SPEECH_09_156_EN.pdf [accessed 20 February 2025]

Mhadevan. A. and Mathioudakis. M. (2024), “Cost-aware retraining for machine learning”. *Knowledge-Based Systems*, 293, Article 111610. Available at: https://doi.org/10.1016/j.knosys.2024.111610 [accessed 10 April. 2025]

O´Regan, E. (2025) “Europe´s GDPR Privacy Law Is Headed for Red Tape Bonfire within weeks”. *Politico*, 3 April. Available at: https://www.politico.eu/article/eu-gdpr-privacy-law-europe-president-ursula-von-der-leyen/ [accessed 15 April 2025]

Shokri, R., Stronati, M., Song, C., and Shmatikov, V. (2017). “Membership Inference Attacks Against Machine Learning Models”. In: *Proceedings of the 2017 IEEE Symposium on Security and Privacy,* 22-24 May 2017, San Jose, California. IEEE, pp. 3-18. Available at: https://doi.org/10.1109/SP.2017.41 [accessed 2 April 2025]

Vetenskapsrådet (2023), “LEAKPRO: Leakage Profiling and Risk Oversight for Machine Learning Models”. Project period: 1 November 2023 – 1 November 2025. Funded by Vinnova, Project ID 2023-03000. Available at: https://www.vr.se/swecris.html?project=2023-03000_Vinnova#/ [accessed 2 Febuary 2025]